Performance Analysis: Unified Virtual Infrastructure Backup

Dell AppAssure 5
Backup, Replication, and Recovery Software
vs.
Veeam Backup & Replication v6.1
Performance Analysis: Unified Virtual Infrastructure Backup

*Dell AppAssure 5*
*Backup, Replication, and Recovery Software*
*vs.*
*Veeam Backup & Replication v6.1*

Author: Jack Fegreus, Ph.D.
Managing Director
openBench Labs
http://www.openBench.com
August 21, 2012
Table of Contents

Executive Summary 04
Building Business Continuity 07
Backup Performance 14
Recovery & Replication Performance 21
Test Summary 29
Executive Summary

“Smart Agents challenge the fundamental rationale for agentless backup: You can’t do more by knowing less.”

**WHY READ THIS DOCUMENT?**

If you’re currently using or considering either Veeam Backup & Replication or Dell AppAssure software to protect your vSphere or Hyper-V Virtual Infrastructure (VI) environment, you may already be aware that both products were reintroduced in June of 2012 in significantly enhanced forms.

openBench Labs is pleased to be the first independent test organization to compare them so you can make an informed purchase decision. We pitted the performance of Veeam Backup & Replication v6.1 software versus AppAssure 5 in a well-appointed VI lab environment. We found that while each offering has focused on ease-of-use through the addition of a new interface and has substantially enhanced its capabilities over its previous version, customers will judge these products primarily by how well they answer three time-tested questions:

- **How easy is it to use?**
- **How fast can it complete a backup, with all the functionality you need for recovery?**
- **What does it take to recover when you need it most?**

Nonetheless, there is another important question that needs to be examined, especially in the light of the growing emphasis on private and public cloud computing:

- **How well will the application architecture adapt to future needs?**

It is with respect to this last question that openBench Labs found AppAssure 5 to be unique among data protection products that we have tested for small to medium sized businesses (SMBs). Driven by the exponential growth in storage resources across the spectrum of all businesses, AppAssure 5 introduces a number of key technologies for scalability, integration, and performance to the SMB market that were previously limited to products targeting global enterprises. More importantly these capabilities are uniquely integrated around two critical constructs, which underpin the rapidly increasing AppAssure 5 value proposition:

- **Universal Changed Block Tracking for all protected machines through the use of Smart Agents**
- **A repository storing a unified space of data blocks for all protected machines built on an object-oriented file system in place of traditional independent sets of backup files**
Smart agents change the dynamics of backup and restore operations by analyzing protected machines and then monitoring and optimizing all data transfer operations—down to on-demand reordering of queued disk blocks during recovery—using fast TCP-based connections. Smart Agents challenge the fundamental rationale for agentless backup: You can't do more by knowing less. Complimenting Smart Agent operations, a unified, deduplicated, multi-dimensional representation of the entire storage space of all protected machines is a much more synergistic platform for advanced operations than independent collections of backup files.

Synergies between Changed Block Tracking metadata on protected machines collected by Smart Agents and an object-oriented repository of data blocks provides a ready environment for incremental forever backups. More importantly, that same metadata can create Delta Change Rollbacks that restore only the data changed since the last incremental backup. In addition, this environment enables data protection operations to be decoupled and run as asynchronous event-driven processes requiring minimal data-synchronization points. As a result, sophisticated data protection operations that include backup and Disaster Recovery (DR) operations can be configured as pipeline processes that will not stall.

**FINDINGS & BENEFITS**

In testing, we found AppAssure 5 offered significant advantages in ease-of-use, backup speed, and recovery time. Here are several key takeaway findings and their impact on IT operations:

- **Finding: More backups mean more recovery point choices.**
  AppAssure's incremental forever image-level backup technology can be set to execute every five minutes for 288 recovery points a day. More importantly, data transfer optimizations automatically applied by AppAssure Smart Agents™ make this a potential level of performance even for many transaction processing applications.

  **Benefit:** IT operations managers can practically eliminate the potential for even minor data loss by creating very closely spaced recovery points for frequently updated mission-critical applications like Exchange, SQL and SharePoint.

- **Finding: Backup processing time for VMs hosted on vSphere was consistently faster.**
  With True Global Deduplication and Recovery Assure™ active, AppAssure was 3X faster executing a full backup with validation testing of a VM running Exchange with 570GB of active data than Veeam Backup & Replication. Moreover, AppAssure was able to run incremental backups every 20 minutes and maintain a warm standby VM without negatively impacting the ability of the Exchange server to deliver 1,000 email transactions per second during a Jetstress benchmark.

  **Benefit:** Backup windows are effectively eliminated, every backup is automatically verified for application recovery assurance, and a warm standby VM is maintained to minimize RTO.
• Finding: Pipelining replication and recovery processes asynchronously enhanced fast recovery options with more recovery points. No data protection software tested by openBench Labs matches the ability of AppAssure 5 to maintain a warm standby VM for either a virtual or physical server while maintaining a five-minute RPO in addition to a five-minute RTO.

**Benefit:** Administrators have more recovery options with outstanding speed to meet today’s increasingly stringent service level agreements.

• Finding: Near-zero time recoveries perceived by users. The most magical and impressive Smart Agent technology is without doubt AppAssure Live Recovery™, which enables Smart Agent processes on both the protected machine and its AppAssure Core server to coordinate the order of data transfers to give users a perception of immediate access to all data, even when that data is still resident on the Core server.

**Benefit:** Users perceive a nearly instant recovery of a Windows application regardless of how much data they store.

• Finding: A disk volume rollback using the most recent recovery point utilizes AppAssure’s Change Block Tracking metadata. Smart Agents are able to reverse the process used in incremental backups when performing a rollback recovery from the most recent recovery point to minimize the amount of data that needs to be transferred to restore a protected machine.

**Benefit:** Actual recovery time is dramatically reduced in restoring full I/O throughput and access performance.
Building Business Continuity

For IT operations, the new object-oriented architecture of AppAssure 5 provides a highly scalable infrastructure for a powerful “forever incremental” backup scheme that eliminates all of the traditional overhead associated with incremental backups, including periodic full and synthetic backups, while simultaneously amplifying the business continuity benefits that a forever incremental backup policy provides.”

**Building Business Continuity on Block Virtualization**

**Under Test: Windows Server Data-Protection**

**Dell AppAssure 5 Value Proposition**

1) Maintain a Virtual Disk Block Space of all Protected Systems: AppAssure 5 maintains a repository of virtual disk blocks rather than an archive of backup sets. *Benchmark: Full backup, with deduplication and recovery verification, of a 417GB Virtual Machine (VM) was 3.3X faster with AppAssure 5 than Veeam 6.1.*

2) Extend Changed-Block Tracking (CBT) for Virtual Machines to Accelerate Data Transfer and Rollback Using Smart Agents™: AppAssure uses Smart Agents™ to track metadata about changes to disk blocks in multiple data transfer processes.

3) Minimize Physical Storage Using True Global Deduplication: AppAssure 5 stores a virtual space of globally deduplicated disk blocks of all protected systems in an object-oriented (OO) repository without the overhead level of an RDBMS. *Benchmark: We averaged 20X storage savings on each of 5 protected virtual machines yielding a 100X reduction over traditional storage methods.*

4) Simplify Application Validation with Recovery Assure™: Smart Agents automatically discover key applications and configure default recoverability tests.

5) Recover Files and Application Items via Universal Recovery™: Retrieve files or individual data objects, such as email messages and database tables, ad hoc by mounting and sharing any backup as a virtual disk.

6) Minimize DR restore Time with a Standby VM: Universal Recovery allows any backup to be used to automatically update system and data files on a warm standby VM or to burn a hot-metal backup CD for any hardware platform.


8) Minimize Data Loss with Near-Continuous Recovery Points: AppAssure leverages CBT with Smart Agents to schedule backups in five minute intervals.

9) Pipeline AppAssure Cores using True Scale™ Architecture: IT can readily scale data protection processes by configuring multiple AppAssure Core servers in a pipeline to scale a data protection process linearly and enhance off-site availability of warm-standby virtual servers using a WAN for replication.

In this analysis, openBench Labs compares Virtual Machine (VM) backup and recovery features and performance of Dell AppAssure Backup, Replication and Recovery software v5 with Veeam Backup & Replication v6. The ability to rapidly restart, non-disruptively move, and spawn new VMs are key features often cited by CIOs for implementing a Virtual Infrastructure (VI) to assuage the downtime fears of corporate executives. That’s made a highly flexible VI a necessary component of any IT arsenal; however, a VI alone is not sufficient to resolve all of the knotty IT issues related to data recovery.

For IT operations, the new object-oriented (OO) architecture of AppAssure 5 provides a highly scalable infrastructure for a powerful “forever incremental” backup...
scheme that eliminates all of the traditional overhead associated with incremental backups, including periodic full and synthetic backups, while simultaneously amplifying the business continuity benefits that a forever incremental backup policy provides.

Through its own CBT technology AppAssure empowers IT administrators with a single advanced data-protection infrastructure for both virtual and physical systems. Moreover, other key AppAssure features include True Scale™ Architecture to enable pipelining of Core server protection processes, True Global Deduplication to minimize the amount of repository data, Live Recovery™ for near-zero downtime; Recovery Assure™ for verifying object level recoverability of files and application-items in any backup; and Universal Recovery™ for cross-platform recovery of data volumes, including bare metal recovery, from physical to virtual (P2V), virtual to virtual (V2V), virtual to physical (V2P) or physical to physical (P2P) systems.

In contrast, Veeam provides an “agentless” approach to data protection exclusively for use in a VI. The Veeam data protection architecture leverages hypervisor-based CBT and utilizes a light-weight service architecture, which allows IT to decouple data protection management, data collection processes, and data storage processes.

Under the Veeam scheme, a Veeam backup proxy server moves data from a VM to a Veeam backup repository server. In this process, the backup proxy server offloads all data handling tasks, including data compression and deduplication, before it transfers traditional backup files via a TCP transport protocol to a backup repository server. In particular, a Veeam Backup repository server stores and manages the backup files and is responsible for the automated processing of synthetic full backups from incremental VM backups under Veeam’s forever-incremental backup plan.

Veeam Backup repository servers also do the work of staging datastores for vSphere hosts. When IT initiates a job to restore a VM by booting directly from a Veeam backup file, the backup repository server populates a special directory with a folder containing pointers to the contents of backup files that represent the desired restore point. Finally, the directory is published to a vSphere host as a datastore containing a VM. Nonetheless, while the light-weight Veeam architecture minimizes the overhead imposed on data protection processes, it does nothing to proactively optimize the performance of critical processes.

**SMART AGENT OPTIMIZATION**

For sites that need to squeeze the highest possible storage reduction savings, the lack of a global data deduplication scheme means IT administrators will have extra work planning backup job schedules that will optimize data deduplication savings. Without a global data deduplication function, every backup deduplication process invoked with
Veeam Backup & Replication is an isolated local event and that presents a number of process optimization issues beyond just storage utilization that will have to be resolved by the IT Operations group.

In particular, operating system (OS) data that are shared by multiple VMs cannot be discovered and deduplicated by Veeam Backup & Replication unless those VMs are part of the same backup job. While the simple solution to place all VMs in the same backup job provides the highest storage savings potential, that solution also hinders the ability of IT administrators to minimize backup time through backup process scalability and parallel job execution.

The problem for IT operations attempting to scale VM backup throughput stems from the dual nature of a VM, as an application running on a host hypervisor and as a logical system running a set of applications on a guest OS. VM duality requires more than a crash consistent recovery of a VM, which is why an agentless approach to data protection is not the same thing as being agent-free.

A full VM recovery must be able to recover the VM’s native file system. This means all transaction-based applications that are running within a VM, such as SQL Server or Exchange, must be completed and be in a consistent state at the time the VM is backed up on the hypervisor. In particular, a VM running any version of Windows Server must quiesce all of the internal logical NTFS volumes using the Volume Shadow Service (VSS), before the hypervisor initiates a snapshot of a vmdk disk file.

To invoke a VSS snapshot, an agent that is aware of the virtualization layer needs to be running inside Windows on the VM. One such agent is the VMware Tools application, which provides a means for the guest OS to communicate with the hypervisor. The ersatz agentless Veeam Backup & Replication invokes VSS on a VM running windows by logging into the VM using VMware tools. What’s more, the critical time constraints involved with quiescing a VM OS and applications are the basis for IT best practices calling for sequential processing of vmdk files within a data protection job. As a result, the only way to exploit parallel execution of VM backups is by running multiple independent backup jobs.

More importantly, an agent that is virtualization-aware can make a significant impact on more aspects of data protection than just backup alone. Given today’s business emphasis on system recovery, the ability of AppAssure Smart Agents to significantly impact the functionality and operational ease-of-use of core data recovery capabilities provides IT operations personnel with some of their greatest benefits. This is particularly true with respect to validation of VM recovery and the acceleration of recovery features for application data items.
Smart agents are particularly important for IT administrators at small to medium business (SMB) sites. While a large-scale VI allows IT at SMB sites to set up sophisticated operations comparable to those of high-end datacenters, few IT administrators at these sites have direct experience with disaster recovery (DR) operations. What’s more, IT administrators at SMB sites often struggle to support different data protection schemes for VMs and physical systems. AppAssure’s Smart Agent technology handles both to hold down escalating labor costs while enabling IT to support aggressive Recovery Time and Recovery Point Objectives (RTO and RPO).

### OPENBENCH LABS DATA PROTECTION TESTING SUMMARY

<table>
<thead>
<tr>
<th>Feature</th>
<th>Key Test Analysis</th>
<th>Dell AppAssure 5</th>
<th>Veeam Backup &amp; Replication v6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uniform Execution on Physical and Virtual Systems</td>
<td>•Uniform execution of all commands from a single GUI lowers operation complexity</td>
<td>•All AppAssure Core servers operate from a single GUI uniformly across all virtual and physical clients</td>
<td>•Veeam excludes physical servers and applies and agentless backup process restricted to VM clients</td>
</tr>
<tr>
<td>Global Data Deduplication</td>
<td>•D2D backup file size directly affects resource costs</td>
<td>•Global data deduplication standard</td>
<td>•Data deduplication applied per job</td>
</tr>
<tr>
<td>Backup Execution Performance</td>
<td>•Minimum time to back up governs frequency and bounds an obtainable RPO</td>
<td>•Only stores deduplicated disk blocks</td>
<td>•Backup repository stores traditional full, synthetic, and both forward and reverse incremental backup files</td>
</tr>
<tr>
<td>Granular Recovery of Files and Application Objects</td>
<td>•Recovery of application data objects localizes disruption of production processes</td>
<td>•Highest data reduction ratio</td>
<td>•Tight hypervisor integration introduces measurable overhead initiating data transfers, which raises the time interval required between recovery points</td>
</tr>
<tr>
<td>Standby VMs and Near-zero RTO Disaster Recovery</td>
<td>•Standby-VM support for both virtual and physical systems minimizes RTO</td>
<td>•Fastest backups with verification minimizes recovery point intervals</td>
<td>•Agentless approach cannot examine clients making application validation a special post-backup process only supported on vSphere</td>
</tr>
<tr>
<td></td>
<td>•Highly optimized proprietary features restore data with no perceived delay</td>
<td>•Smart Agents maintained user I/O throughput while disks were backed up allowing IT to meet SLAs for application performance</td>
<td>•To verify or recover applications or file data, IT must boot VMs directly from backup files and manually assign verification tests for every application running on a VM.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>•Independent export process updates standby VMs from normal incremental backups minimizing RPO intervals</td>
<td>•Special process collects incremental backup data and uses that data to synchronously update a replica VM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>•Smart Agents leverage CBT metadata for a Delta Change Rollback that minimizes the data needed to restore a protected machine and reorder data transfers to meet user I/O needs</td>
<td>•A vSphere VM can be booted from a backup file using redo logs or cache files to save writes adding I/O overhead until new and original data are consolidated in a second process for full production-level performance</td>
</tr>
</tbody>
</table>
OpenBench Labs conducted tests on Dell AppAssure 5 Backup, Replication, and Recovery software and Veeam Backup & Replication v6.1 using a test bed populated with six physical servers, and two VM backup servers. We centered physical systems around a Dell PowerEdge R710 server, which was provisioned with dual 6-way core processors. This system served as the primary AppAssure 5 Core server running AppAssure Central Console and the primary Veeam Backup & Replication v6.1 server.

For network-centric AppAssure 5, we utilized physical and virtual 1GbE and 10GbE networking connections. For AppAssure Core on a physical server, we increased typical backup throughput for VMs from 100MB per second to 300 MB per second by switching to 10GbE networking infrastructure. More importantly, we accomplished a similar boost in throughput by simply creating VM equivalents of our PowerEdge 1950 servers on each vSphere and Hyper-V host. In this configuration, each VM-based AppAssure Core server was provisioned with four CPUs, 8GB RAM, and an internal 10GbE virtual NIC. In addition, all production VMs were also provisioned with 10GbE virtual NICs.

For Veeam Backup & Replication, which can leverage an underlying Storage Area Network (SAN) resources through tight integration with the snapshot capabilities of vStorage APIs for Data Protection (VADP), we provisioned an 8Gbps Fibre Channel (FC)
SAN to provision storage resources with optimal hardware. In order to enhance the scalability of Veeam Backup & Replication v6.1, we utilized two quad-core Dell PowerEdge 1950 servers with 8GB of RAM and dual FC ports to run Veeam backup proxy and Veeam backup repository services.

Within this environment, we set up data protection tests designed to assess each package’s ability to add value through the simplification of IT management tasks and the reduction of operating expense (OPEX) costs. In particular, we focused testing on three critical data-protection goals for IT operations:

- Reduce backup time
- Speed recovery
- Reduce backup storage

A critical success factor for achieving those goals is the implementation of an optimized disk-to-disk (D2D) backup strategy using incremental backups of all servers. While a primary D2D strategy provides IT with a number of operating efficiencies versus a primary disk-to-tape (D2T) strategy, a long standing IT rule of thumb calls for an overall data reduction ratio of 20:1 for D2D operations to be as cost effective as D2T. To meet that storage footprint heuristic, IT will need to achieve an average storage reduction of 95% through data deduplication.

**The Business Continuity Restore Mandate**

Our main concern, however, was recovery. In a business continuity context, backup is simply a means to an end. Specifically we assessed the ability to leverage incremental backups to support an aggressive RPO target to mitigate the amount of processed data that would likely be lost when recovering from a computer outage.

Minimizing data loss by using closely spaced recovery points intrinsically links RPO to the minimum time required to complete a backup. Not only does this underscore the importance of an incremental backup scheme, it also spotlights the need to keep any series of traditional forward-chained incremental backups short to minimize the possibility of a corrupted backup invalidating every follow-on backup in the chain. To resolve the incremental backup dependency issue while maintaining minimum backup
windows, many sites have adopted an “incremental forever” backup scheme that utilizes the creation of periodic synthetic full backups. Nonetheless, the work to provide an aggressive RPO can be quickly negated by a prolonged recovery process. Fast backup must be complemented with reliable accelerated recovery technologies to support an aggressive RTO, which must be measured in minutes for critical business applications.

Through the use of CBT, global data deduplication and an OO file system, AppAssure 5 transcends incremental, full, and synthetic backup, by providing IT with a virtual block space—complete with recovery points—representing all systems protected by a Core server. With its virtual block space, the AppAssure repository changes the dynamics of both backup and recovery, by shifting the focus of IT data protection operations from an archive of disparate backup files to a repository containing a live virtual disk block space.

**Email Checking**

On our ESXi and Hyper-V hosts, we set up multiple VMs running Windows Server 2008 R2 and various key applications, including Active Directory, SQL Server 2008 R2 and Exchange Server 2010. To stress test I/O in this environment, we set up an enterprise-class VM-based Exchange 2010 server with six dedicated virtual disks to service 1,000 email accounts. In particular, we dedicated a pair of disks to store the mailbox database and the transaction logs for every group of 500 email users.

To stress 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 and heavy processing extends the email TPS load to all of a server's mailboxes: 1,000 email TPS in our scenario.
Backup Software Architecture Differences

A central issue for comparing AppAssure with Veeam Backup & Replication is the scope of services provided by the two products. To set up AppAssure’s generalized disk-block tracking mechanism on virtual or physical systems, IT Administrators install a Smart Agent for the AppAssure service on every client system to collect, package, and send block data back to an AppAssure Core server.

The AppAssure Smart Agent places a filter driver between the Windows file system and the Windows kernel to capture block-level changes on the underlying logical disk volume associated with data changes in files made by applications. Using the filter driver, AppAssure Smart Agents on client systems log meta data about disk-block changes for each logical disk.

During a backup, the agent utilizes the meta data to send an AppAssure Core all of the block-level data changes that have occurred since the last backup. Moreover, data transfer is a TCP-based, direct, agent-to-agent process that is independent of whether the protected machine is physical or virtual. As a result, an AppAssure incremental backup bypasses the connection overhead that occurs when transferring data through the hypervisor—Veeam typically takes 90 to 105 seconds before it begins a data transfer.
More importantly, when an AppAssure 5 Core receives block data from a Smart Agent on a protected machine, it does not follow the traditional backup scheme of storing that data in disparate sets of backup files that must be processed during a restore operation. Instead, the AppAssure 5 Core server first applies a global data deduplication—a process dubbed True Global Deduplication—to the block data from a backup. Next, the AppAssure 5 Core server incorporates the deduplicated data blocks in a repository that is built on an OO file system. As a result, AppAssure 5 is able to assign extensive characteristics to stored data blocks, including, source machine, volume, and recovery point time. In this way, an AppAssure 5 Core server is able to directly ingest continuous incremental backups into a multi-dimensional, single-instance, repository representing the entire storage space underpinning the Core server’s protected machines, without ever having to schedule real or synthetic full backups.

What’s more, the scalability of an AppAssure 5 Core repository is just as impressive as its functionality. IT administrators use standard NTFS directories as containers—from up to 255 different disk volumes and reach a capacity of 32 exabytes—to contain and extend the encapsulated OO file system that underpins an AppAssure 5 repository.
For IT, AppAssure data protection infrastructure starts to pay off as Smart Agents optimize data transfers for a unique level of I/O performance during incremental forever backups. Using AppAssure 5, we ran incremental backups every 20 minutes on our Exchange VM, while the server processed 1,000 email TPS. When we ran an incremental backup with Veeam Backup & Replication, Exchange could not process more than 300 email TPS. By monitoring email and backup transactions, AppAssure Smart Agents were able to increase I/O transfers during disk backups to maintain application I/O at production levels, such as on our Exchange VM as it serviced 1,000 email TPS.

We ran incremental backups with AppAssure and Veeam in conjunction with our heavy email transaction use case based on Jetstress delivering 1,000 email transactions per second to a VM running Exchange. AppAssure’s Smart Agents identified monitored user and backup transactions and raised I/O throughput for each mailbox disk (E: and F:) as it was backed up. In contrast, an incremental backup with Veeam disrupted Exchange I/O performance, which dropped to 300 TPS.

For IT, AppAssure data protection infrastructure starts to pay off as Smart Agents optimize data transfers for a unique level of I/O performance during incremental forever backups. Using AppAssure 5, we ran incremental backups every 20 minutes on our Exchange VM, while the server processed 1,000 email TPS. When we ran an incremental backup with Veeam Backup & Replication, Exchange could not process more than 300 email TPS. By monitoring email and backup transactions, AppAssure Smart Agents were able to increase I/O transfers during disk backups to maintain application I/O at production levels, such as on our Exchange VM as it serviced 1,000 email TPS.
We used the ability to pipeline AppAssure processes between Core servers to extend our data protection plan, which successfully met a 20-minute RPO, to include an RTO of five minutes. To accomplish this task, we replicated all repository changes on the AppAssure Core VM protecting the Exchange VM server to a physical server running OPENBENCH LABS...

In addition to uniquely providing a 20-minute RPO while our Exchange VM processed 1,000 TPS, AppAssure was also able to support an RTO of 5 minutes. To do this, we set up a pipeline between the AppAssure Core on the Exchange VM’s host and our Central AppAssure Core. Generated by Jetstress, we ran incremental backups on the VM-based Core server every 20 minutes. During backups of disks containing mailbox databases and logs, Smart Agents ensured our Exchange server continued to deliver the required 1,000 TPS by increasing throughput on the disks being backed up. When the backup completed, the VM-based Core replicated its Exchange VM repository data to the Central AppAssure Core allowing us to run any recovery tasks from the replicated data. In particular, we maintained a standby VM for an enhanced RTO on the Central AppAssure Core asynchronously from the RPO-oriented backup tasks running on the AppAssure VM Core.

We used the ability to pipeline AppAssure processes between Core servers to extend our data protection plan, which successfully met a 20-minute RPO, to include an RTO of five minutes. To accomplish this task, we replicated all repository changes on the AppAssure Core VM protecting the Exchange VM server to a physical server running...
the AppAssure Core and Central Administration software, after completing each incremental backup of the Exchange VM.

Once the repository update was complete and the two Core Servers were synchronized, we were able to immediately decouple RPO-oriented tasks on the VM Core server from RTO-oriented tasks on the Central Administration server and process the two sets of tasks asynchronously. In particular, we used the Central Administration server to export disk updates to the vSphere host supporting a standby Exchange VM to comply with our five-minute RTO. Updating the standby VM server was the only process without full end-to-end Smart Agent optimization, which made it essential to decouple that task from our time sensitive RPO-oriented incremental backups.

In addition to unique backup performance support, AppAssure with global data deduplication combined with an OO repository typically provided storage reduction ratios on the order of 20- or 30-to-1 for each protected machine. Furthermore, since separate backup files are not saved for each protected machine, the overall storage savings for a Core server can be estimated from the sum of the savings calculated for each protected machine. On the AppAssure Core servers that we ran on V1 hosts, overall storage savings typically ranged from 75- up to 100-to-1. In contrast Veeam limits the scope of duplication to only those machines in a current backup job.

Nonetheless, what makes AppAssure 5 radically different for data protection is its aggressive exploitation of Smart Agents for multiple data protection operations, beyond backup alone. Smart Agents are used in three key restore technologies: Recovery Assure to verify that a backup, including the application data within a backup, is recoverable; Live Recovery to meet near-zero RTO; and Universal Recovery to support granular recovery of files, application items, as well as P2P, V2V, P2V, and V2P recovery options.

To control backup operations overhead, AppAssure Smart Agents immediately check every new machine protected by an AppAssure Core server to discover protected applications, such as Exchange and SQL Servers. When a protected application is found by a Smart Agent, AppAssure automatically sets up custom verification tests, which may be performed in seconds on the Core server after every backup or on the final backup of the day for more complex tests. In contrast, Veeam Backup & Replication, which is agentless, is devoid of any specific knowledge of client applications. To run a backup verification, IT administrators have to select application tests and boot the VM from a backup file to run the tests, which typically took about 30 minutes in our tests.

AppAssure, however, customizes the Core server management GUI to display configuration options for a new client based on applications running on that machine. Not only are all of the disks used by the application grouped as a resource unit, Smart Agents drill down into the application and create subgroups of disks that also act as unified resources. On our Exchange server, Smart Agents grouped the disk volumes used
to store a mailbox database and its logs and configured tests that checked on the integrity of mailbox data to run automatically as part of the backup process. In addition, icons were added to the Core server administration GUI to display the results of the tests with respect to the resource groups.

Since Veeam backups have no knowledge of applications running on a VM, backup verification requires separate post-backup processes, in which VMs are booted from backup files. Dubbed SureBackup by Veeam, the process requires a fenced virtual lab to isolate production VMs from their backup image, which has all of the same network identifiers. As a result, SureBackup incurs significant overhead instituting each verification process, which must also include all VMs that the test VM is dependent upon, such as a domain controller and DNS server, to work properly in the isolated lab. What's more the solution only works with VMware.
With Smart Agents to accelerate data transfers and setup application testing as part of the backup process, AppAssure was able to forge measurable advantages in our backup scenarios. Specifically, AppAssure was consistently faster performing full and incremental backups with verification testing than Veeam performing just a backup alone.

What’s more, Veeam’s SureBackup verification requires booting a VM backup on line to verify an application is running correctly via test scripts. Bringing the VM backup on line, however, has the potential to create a conflict with the source VM. Veeam Backup & Replication avoids these conflicts in vSphere environments by installing an appliance that creates a virtual production network hidden from machines running on the actual production network.

When a VM is booted into Veeam’s fenced virtual lab and tested for recoverability, it cannot communicate with any production server. As a result, testing has to include booting a backup of every VM on which the VM being tested is dependent for application test to be successful.

---

### Single-Server Backup

<table>
<thead>
<tr>
<th>Protected Machine Configuration</th>
<th>Backup Software Options</th>
<th>Backup Window (hh:mm:ss)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physical Server</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Server 2003</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory PDC, DNS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>30.5GB active data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>250MB average change</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AppAssure 5</td>
<td>00:03:29 Full</td>
<td></td>
</tr>
<tr>
<td>Compress, Dedupe</td>
<td>00:00:19 Incremental</td>
<td></td>
</tr>
<tr>
<td>Verify</td>
<td>00:00:09 Verify</td>
<td></td>
</tr>
<tr>
<td>Veeam 6.1</td>
<td>NA</td>
<td></td>
</tr>
</tbody>
</table>

| vSphere 5 VM                  |                         |                          |
| Windows Server 2008 R2        |                         |                          |
| Active Directory PDC, DNS     |                         |                          |
| 19.9GB active data            |                         |                          |
| 500MB average change          |                         |                          |
| AppAssure 5                  | 00:01:58 Full           |                          |
| Compress, Dedupe             | 00:00:50 Incremental    |                          |
| Verify                       | 00:00:05 Verify         |                          |
| Veeam 6.1                    | 00:04:32 Full           |                          |
| Compress, Dedupe             | 00:02:33 Incremental    |                          |
| SureBackup Test             | 00:23:56 Verify*         |                          |

| vSphere 5 VM                  |                         |                          |
| Windows Server 2008 R2        |                         |                          |
| SQL Server 2008 R2            |                         |                          |
| Active Directory PDC, DNS     |                         |                          |
| 30.6GB active data            |                         |                          |
| 500MB average change          |                         |                          |
| AppAssure 5                  | 00:02:09 Full           |                          |
| Compress, Dedupe             | 00:00:28 Incremental    |                          |
| Verify                       | 00:00:05 Verify         |                          |
| Veeam 6.1                    | 00:04:46 Full           |                          |
| Compress, Dedupe             | 00:02:22 Incremental    |                          |
| SureBackup Test             | 00:31:10 Verify*         |                          |

| vSphere 5 VM                  |                         |                          |
| Windows Server 2008 R2        |                         |                          |
| SQL Server 2008 R2            |                         |                          |
| Active Directory PDC, DNS     |                         |                          |
| 37.1GB active data            |                         |                          |
| 500MB average change          |                         |                          |
| AppAssure 5                  | 00:02:34 Full           |                          |
| Compress, Dedupe             | 00:00:41 Incremental    |                          |
| Verify                       | 00:00:05 Verify         |                          |
| Veeam 6.1                    | 00:05:28 Full           |                          |
| Compress, Dedupe             | 00:02:30 Incremental    |                          |
| SureBackup Test             | 00:29:24 Verify*         |                          |

| vSphere 5 VM                  |                         |                          |
| Windows Server 2008 R2        |                         |                          |
| Exchange Server 2010          |                         |                          |
| 570GB Active Data             |                         |                          |
| 250MB average change          |                         |                          |
| AppAssure 5                  | 00:31:44 Full           |                          |
| Compress, Dedupe             | 00:00:56 Incremental    |                          |
| Verify                       | 00:02:56 Verify         |                          |
| Veeam 6.1                    | 00:40:02 Full           |                          |
| Compress, Dedupe             | 00:05:12 Incremental    |                          |
| SureBackup Test             | 01:06:32 Verify*         |                          |

| Hyper-V VM                    |                         |                          |
| Windows Server 2008 R2        |                         |                          |
| SQL Server 2008 R2            |                         |                          |
| 29.7GB active data            |                         |                          |
| 250MB average change          |                         |                          |
| AppAssure 5                  | 00:02:22 Full           |                          |
| Compress, Dedupe             | 00:00:37 Incremental    |                          |
| Verify                       | 00:00:06 Verify         |                          |
| Veeam 6.1                    | 00:06:07 Full           |                          |
| Compress, Dedupe             | 00:04:52 Incremental    |                          |
| N.A.                         | 00:23:56 Verify*         |                          |

*Verify includes initial setup of a Windows Domain Controller with DNS (20 to 25 min)*
Recovery and Replication Performance

For AppAssure 5, changed blocks also represent an alternative construct with respect to a rollback of a disk volume on a protected machine: To restore a volume to its most recent restore point, the only data blocks that must be transferred back to the source machine from its protecting server are the data blocks that correspond to the data blocks currently in the machine’s list of blocks that have changed since the last backup.

The Road to Zero RTO

For IT, backup has long been a necessary daily activity centered on backing up data, applications, and OS files in a minimal amount of time. From the perspective of a Line of Business (LoB) executive, however, the value of IT data-protection operations rests entirely in recovery processes. As a result, data-protection Service Level Agreements (SLAs) between IT and LoB units focus on RPO and RTO targets and leave backup as simply a means to provide a recovery point.

More importantly, LoB executives are beginning to link computer downtime to more than lost sales revenue: They now equate computer outages to potential losses in customer confidence and market share. That’s why growing numbers of senior executives expect IT to meet RTOs for critical business applications measured in minutes rather than hours, which is typical of traditional restore techniques. The challenge for many IT decision makers is to assuage the business-continuity fears of corporate executives within budget constraints that exclude capital expenditures on costly components, such as fault-tolerant servers.

For an RPO target, the key metric is the minimum time to establish and run an incremental backup. In our backup testing AppAssure with Smart Agent technology was consistently able to start data transfers more quickly and as a result, incremental backups were also faster. More importantly, backups were much less intrusive on protected machines that were heavily used. Smart Agents were able to
monitor user traffic and increase overall throughput for each disk during a backup to minimize the impact on production processing.

For setting an RTO target, the base line is the time required to perform a standard recovery operation. In tests of VMs less than 50GB in size, AppAssure 5 was typically 3-to-4X faster than Veeam Backup & Replication 6.1 using a standard restore from a backup file. In these tests, AppAssure's key advantage was the ability of Smart Agents to setup and begin data transfers more quickly.

While AppAssure measured to its own advantage through most of our testing, there was one circumstance where Veeam pulled ahead. For a large VM with over 500GB of active data that has been provisioned via a high-speed Fibre Channel SAN, Veeam is able to utilize higher SAN throughput to offset initial connection overhead to gain an advantage. When we restored our Exchange VM with 570GB of active data, Veeam Backup & Replication proved to be 35% faster than AppAssure 5.

For critical business applications, however, LoB executives continue demands for IT to reduce the RTO of a burgeoning class of time-sensitive operations down to minutes. To support an aggressive RTO of five minutes, both AppAssure and Veeam provide IT operations with ways to maintain a copy of a production VM in a ready-to-boot state.

**STANDING BY**

To resolve the problems associated with meeting strict RPO and aggressive RTO requirements, AppAssure provides IT with the ability to maintain a warm standby VM of any existing system, whether physical or virtual, as part of the backup process. If the primary server fails, the warm-standby can be booted directly into the production network and transparently replace the primary system. In providing for a warm-standby VM, AppAssure leverages the ability of a vSphere host to update a VM that is not in a running state using disk snapshots.

AppAssure 5 begins creation of a warm-standby VM with a standard restore using an export process that creates a copy of the original VM. Once the VM copy is created, AppAssure 5 is able to keep it updated by generating disk snapshots using incremental backups. By leveraging vSphere disk snapshot updates, Smart Agent optimization of data transfers between protected machines and Core servers, and the ability to copy backup repositories between Core servers, AppAssure 5 is able to enhance RTO through a powerful pipeline process.

In tests of AppAssure 5 pipelining with a VM running Exchange, we leveraged Smart Agents to safely run incremental backups every 20 minutes, while Exchange was processing 1,000 email transactions per second. In those tests, incremental backups typically transferred a total of 20GB of new data and took 12 to 15 minutes. As soon as the incremental backup completed, we replicated the repository on the AppAssure Core

"In tests of AppAssure 5 pipelining with a VM running Exchange, we leveraged Smart Agents to safely run incremental backups every 20 minutes, while Exchange processed 1,000 email TPS."
server handling the backups, to a second AppAssure Core server, which typically added another three minutes to the pipeline process as the two Core server repositories were synchronized after each backup.

Once the replication process completed, we were then able to completely decouple the process of running incremental backups on the first AppAssure Core server from the process of updating of the standby VM by running that process entirely from the second AppAssure Core server. Excluding the synchronization of the repository replication of the Exchange VM block data, all other processes were performed asynchronously.

**REPLICATING SNAPSHOTS**

Veeam also provides a method to enhance RTO using disk snapshot updates. Veeam Replication lets IT administrators leverage Veeam proxy backup services to transfer a source VM to a copy of the VM, dubbed a replica, located on a vSphere host. For both the AppAssure warm-standby VM and the Veeam replica, the use of vSphere disk snapshots results in a recovery VM that can be booted directly into production with full functionality and performance.

In particular, Veeam proxy backup services are used to collect and transfer scheduled updates of a source VM to a replica VM. The process is very similar to Veeam's incremental backup process; however, data updates are stored as an uncompressed non-deduplicated VM disk snapshots in native vSphere format along with the virtual disks of the replica VM, rather than as backup files optimized to minimize storage.

The source-side Veeam backup proxy accesses the original VM image and copies data using standard transport modes, including direct SAN and appliance hot attachment. The target-side proxy service decompresses replica data and writes the result to the destination datastore. In addition, replica metadata files containing CBT checksum data are placed on a backup repository associated with the source VM. When the use of vSphere CBT data cannot be used directly, such as when executing a failback from the replica to a recovered configuration of the source VM, the source-side backup proxy service interacts with the repository service to obtain replica metadata.

To compare the performance of Veeam Replication with an AppAssure 5 warm-standby VM, we configured a VM running SQL Server and generating 200 TPS (50% 8KB reads and 50% 8KB writes). That level of I/O accounted for about 1MB of changed data per second. We then set out to determine a minimum interval in which we could successfully continue updating a Veeam replica or an AppAssure warm-standby VM, while the user process continued to run on the VM.

For optimal replication, the Veeam replication wizard automatically configured our physical Dell PowerEdge R710 server as the source backup proxy using SAN connectivity to accelerate backups of the original VM. Veeam then used a VM-based backup server for the target backup proxy using hot datastore attachment for replica updates. In essence, Veeam reversed the data flow configuration of the AppAssure 5 process pipeline that we had set up for Exchange.
To maintain a stable transport connection, Veeam replication maintains communications between the Veeam backup proxy services on the source and replica VM servers. Unlike the event-driven communications that occur between the Core servers in an AppAssure 5 pipeline, communications between Veeam backup proxy services are continuous throughout the replication process. In particular, the initiation of replica updates on the source backup proxy and the transfer of disk snapshots to the VM replica from the target backup proxy have to be run sequentially and can not be decomposed to run as separate asynchronous processes. As a result, it is not possible to fully decouple replica updates of the source VM from replica updates of the target VM.

Using AppAssure 5, which has the ability to run source backups and targets updates asynchronously and benefits from active Smart Agents monitoring I/O and optimizing data communications, we were able to support a minimum RPO of five minutes. In comparison, we needed to set a minimum RPO of ten minutes with Veeam Backup & Replication 6.1.
Veeam Backup & Replication also provides another alternative to the problem of meeting strict RPO and RTO requirements in a VI environment. Veeam’s Instant VM Recovery provides the ability to boot a VM directly from a backup file without first returning the data to its original state. From a process perspective, booting a VM into a production environment directly from a backup file via Veeam Instant VM Recovery follows many of the techniques used to boot a VM into an isolated SureBackup lab environment to validate the recoverability of a VM.

**Boot Directly from Backup File**

To boot from a backup, Veeam Instant VM Recovery sets up pointers to the files in a VM backup image in a separate directory and exports that directory as a read-only VMFS network-attached datastore via NFS. We then chose to remap I/O via disk snapshots to a faster SAN-attached datastore for full read-write functionality. We then ran Jetstress to measure the overhead imposed by this I/O remapping scheme. In this configuration, we averaged about 300 email transactions per second.

Instant VM Recovery, however, is simplified by the elimination of the lab networking appliance, since there is no need to hide VMs that are intended to run in the production network. As a result, Veeam automatically places cache files in the NFS-shared datastore to handle data changes. In our Instant VM Recovery tests of our VM running Exchange 2010, we staged the VM backup to boot in just 34 seconds and accessed an Exchange mailbox using Outlook on a client system within three minutes.

An IT administrator also has the option to redirect data changes to a different datastore that provides higher throughput and IOPS performance than the default NFS-shared datastore. For this option, the Instant VM Recovery wizard creates a VeeamIR
directory containing VM disk snapshots and CBT files on the designated datastore. Nonetheless, when we chose this option, we were still confronted with significant I/O throughput issues imposed by data remapping.

For insight into these problems, we ran Jetstress performance benchmarks during the Exchange VM recovery process. In particular, even after remapping VM disk snapshots to a faster datastore, we were still unable to sustain more than 300 email TPS. Furthermore, it is still necessary to complete the recovery process by consolidating the data in the read-only NFS mounted datastore with any new data in a fully functional datastore via vMotion. When we ran vMotion, the added overhead of the migration process further dropped the email transaction load that we were able to sustain to 70 TPS. More importantly, we also needed to schedule a maintenance shutdown to complete the recovery process, which was extended to 6.5 hours as we continued to run Jetstress.

**SMART AGENTS & ZERO RTO**

The most magical and impressive Smart Agent technology is without doubt AppAssure Live Recovery. Live Recovery is a unique volume restoration feature. During a recovery, a Smart Agent monitors block data requests from users and instructs the backup server to reorder the data being transferred to meet user requests. As a result, users perceive all data as having been restored immediately and have immediate access to any data on any volume.

With Live Recovery, the restoration of a logical volume starts with the transfer of the volume's Master File Table (MFT). With the MFT in place, users immediately see all of the files that were on the drive at the time of the restore point. As a result, end users have the impression that the drive has been magically restored to full operational status in seconds. Nonetheless, in a database environment, there is the distinct risk of corrupting one or more critical internal tables or causing considerable delays and problems for mission-critical, transaction-processing applications.

When an application attempts to access data queued on the AppAssure backup server, the requested data addresses are transferred to the backup server, which reorders the block stream queued for the client so that the requested blocks are at the top of the queue. As a result, a large volume file server or an Exchange mailbox database can be restored instantaneously from the perspective of an end user.

Nonetheless, there is more Smart Agent legerdemain to restoring data—dubbed a Rollback in the AppAssure management GUI. To enable incremental, block-based backups, a Smart Agent on a protected machine tracks the disk blocks that have changed since the last backup. For AppAssure 5, changed blocks also represent an alternative construct with respect to a rollback of a disk volume on a protected machine: To restore a volume to its most recent restore point, the only data blocks that must be transferred back to the source machine from its protecting server are the data blocks that correspond to the data blocks currently in the machine's list of blocks that have changed since the last backup. Restoring a volume from its most recent recovery point is a “reversed CBT” operation.
We rolled back two volumes used for a mailbox database and logs for 500 users. We used the most recent recovery point for the volumes, which had been created with just 3.97MB of data. The recovery point represented 247GB of data, which a traditional restore would have to transfer to the Exchange VM. Using CBT metadata, however, Smart Agents on the Exchange VM and AppAssure Core server determined only 128GB of data were needed to replace data on the two volumes to restore the recovery point. Via Smart Agents and a reverse CBT restore, the required data for a rollback was cut in half. During that rollback, we applied our heavy Jetstress processing load and monitored I/O transaction rates and CPU overhead imposed by the Smart Agent on the VM. Smart Agents and Live Recovery immediately serviced 70 email TPS, which doubled as we restored 65% of the data. That rate doubled again to 350 TPS as the rollback completed. On completion, processing immediately rose to full 1,100TPS, while the Smart Agent averaged about 0.6% of the VM’s CPU capacity. Moreover, unlike the Veeam Instant VM Recovery process, once we completed the Live Recovery process, the VM was in a production-performance state.
To test the ability of smart Agents to support a near-zero RTO with Live Recovery assisted by CBT metadata, we rolled back the data on two volumes dedicated to a mailbox database for 500 users along with the log data for that mailbox. Both volumes were automatically grouped as a single storage resource by AppAssure’s Recovery Assure technology when we established our Exchange VM as a protected machine.

After running 1,000 email transactions per second for over half an hour, we stopped Jetstress and began the rollback of data on the two volumes. Normally that would mean restoring all of the data on the disk as it was at the time of the recovery point. That was not the case with our AppAssure 5 rollback. The amount of data required to restore both volumes to the recovery point was immediately cut in half, as Smart Agents accessed the CBT metadata on the VM and determined that only half of the data on the two volumes—128GB instead of 247GB—had changed since the last incremental backup.

In addition to minimizing the amount of data transferred, AppAssure’s Live Recovery can also reorder the data being transferred from an AppAssure Core server to meet user I/O demands on the protected machine. To test this capability, we ran our Jetstress heavy transaction load configuration, as we transferred the 128GB of data needed to bring our server back to the rollback recovery point. From the start of the test, the AppAssure client coordinated the order in which mailbox data was transferred from the AppAssure backup server.

At the start of testing, Live Recovery was immediately able to support a transaction rate of about 70 email transactions per second. This rate slowly increased as the data was transferred. When we had completed 65% of the transfer process, Live Recovery was supporting about 150 email transactions per second. The transaction rate doubled again to around 340 email transactions per second as we transferred the remaining 35% of the data. Then on completion of the roll back, the transaction rate immediately returned to the full 1,100 TPS. In contrast, Veeam Instant VM Recovery required a consolidation of remapped and original data via Instant vMotion before returning to full I/O processing levels.

More importantly, we were able to complete every I/O request from Jetstress throughout the recovery process. Moreover, when the process was complete, there was nothing that we needed to do as the protected machine was already functioning as a normal production machine.
REWITING THE RULES OF BUSINESS CONTINUITY

Concerns expressed by Line of Business (LoB) executives over business continuity are helping to drive the next wave of IT projects. In a competitive 24x7 environment, computer downtime represents more than lost revenue to sales and marketing executives. These executives equate lengthy computer outages with potential losses in customer confidence and market share. As a result, senior LoB executives expect IT to meet an RTO that is measured in hours rather than days and an RPO that is close to zero.

AppAssure 5 Backup, Replication and Recovery software is designed to leverage changed disk blocks in place of changed files on any Windows system—physical or virtual—to ensure RPO and RTO objectives. More importantly, AppAssure 5 introduces an OO-based file system that underpins a globally deduped repository of which represents a virtual disk space for all systems protected by the AppAssure 5 Core Server.

For IT operations, the new OO architecture of AppAssure 5 provides a highly scalable infrastructure for a powerful “forever incremental” backup scheme that requires a minimal amount of computer processing time.

Test Summary

“"No data protection software tested by openBench Labs has been able to match AppAssure’s ability to provide a warm VM for both virtual and physical production servers while maintaining a minimal five-minute RPO in addition to a five-minute RTO.”

AppAssure Feature Benefits

1) Object-Oriented Repository Stores a Virtual Disk Block Space: AppAssure 5 maintains a repository of virtual disk blocks rather than an archive of backup sets which radically improves the dynamics of restore operations.

2) Agent-based Changed Block Tracking: IT administrators install agents on client systems that utilize a filter driver to track block-level changes to greatly reduce the processing of incremental backups and rollback recoveries.

3) Minimize Physical Storage Using True Global Deduplication: AppAssure 5 leverages an object-oriented repository in a global deduplication scheme that reduces storage consumption without incurring the overhead level of an RDBMS.

4) Pipeline AppAssure Cores using True Scale™ Architecture: It can readily scale data protection processes by configuring multiple AppAssure Core servers in a pipeline to scale a data protection process linearly.

5) Live Recovery™ Restores Volumes and Key Application Files with Zero Perceived Delay: Live Recovery immediately restores directory details and reorders the transfer of blocks based on user access of files during recovery.

6) Recovery Assure™ Automatically Tests and Verifies Application Recoverability: AppAssure discovers key applications, such as SQL Server and Exchange, on clients and applies special item-level verification tests for these applications.

7) Universal Recovery™ to Any Hardware for DR: Recover systems using a bare metal recovery CD, a hot standby server or a warm standby VM.

8) Universal Recovery™ at Any Granularity: Recover systems, disk volumes, files, or application-level data items, such as email messages and database tables using standard application management tools.
Using AppAssure 5, IT is empowered to implement a DR plan with aggressive RTO and RPO levels to support any SLA required by Line of Business executives. Moreover, IT can double down on the advantages garnered in incremental backup processing to utilize very frequent automated incremental backups to provide minimally spaced recovery points for mission critical systems.

Specifically, IT operations managers can leverage AppAssure incremental backup advantages by running frequent incremental backups to minimize the time intervals between recovery points of mission critical systems and use standby VM servers to double down on an aggressive DR plan with an RTO measured in minutes. No data protection software tested by openBench Labs has been able to match AppAssure's ability to provide a warm VM for both virtual and physical production servers while maintaining a five-minute RPO in addition to a five-minute RTO.

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