signal65

Cyber Resilience with Cohesity

AUTHOR

Russ Fellows
VP, Labs | Signal65

IN PARTNERSHIP WITH

COHESITY

JUNE 2025

Overview

With the continuing rise of destructive cyber-attacks, exfiltration and extortion, Cyber Resilience remains an area of focus for many IT organizations. Data resilience and threat mitigation include many technologies and issues, but a critical foundational aspect is that of creating, storing, and protecting multiple copies of data on different types of media, at multiple locations.

Multiple studies from a leading analyst firm, The Futurum Group, show a growing awareness of the need for cyber resilience, due to a rise in incidents. As a result, firms are now focusing on how best to circumvent and respond when an attack occurs. In practice, this means companies' IT organizations of all sizes and geographies understand their need for enhancing internal data protection, security, and recovery procedures. While data protection including backup processes receive significant focus, recovery is the most critical feature when data or applications become unavailable.

Rapid recovery of data is a key ingredient in the process of clean room forensic analysis to determine which systems and data may be infected, and what may be compromised. This process often requires recovering systems from multiple points in time, to determine which is the most recent, clean image. Therefore, rapid recovery is one of the most important criteria for data protection tools and improved cyber resilience outcomes.

Highlights

Signal65 found that compared to a leading competitor, Cohesity delivered a better, faster, and more reliable backup and recovery solution as evidenced by the following:

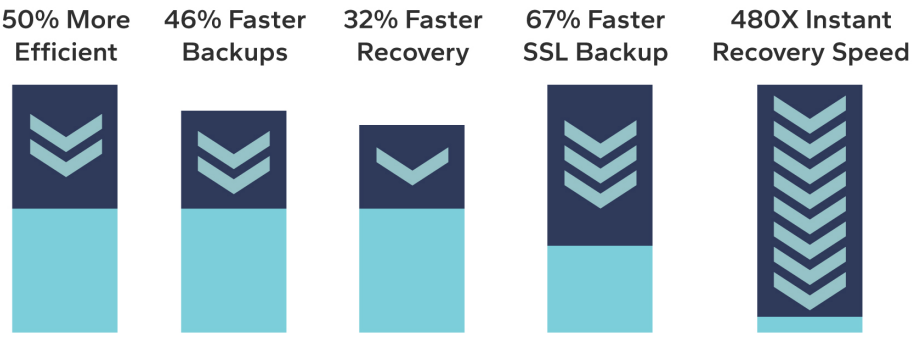


Figure 1: *Cohesity Advantage Overview*

1. Cohesity provided on average 50% greater data reduction, thereby increasing the effective capacity of the storage system.
2. For backup operations, Cohesity was on average 46% faster than the competitor, with the advantage increasing with larger data sets.
3. When recovering 100 to 1,000 VMs, Cohesity delivered 37-43% faster recovery speed than the competitor.
4. When using the NBDSSL (network block device SSL) method, Cohesity was able to recover 67% faster than the competitor.
5. For Instant Recovery of 25 VMs, Cohesity provided a significantly better experience, with a power on in < 1 minute vs. 8+ hours for competitor (480X faster).

Evaluation Overview

Signal65 was asked to independently compare Cohesity's data protection appliance to a leading alternative in a typical enterprise setting. The evaluation criteria included an analysis of the data protection process, storage efficiency, and data recovery.

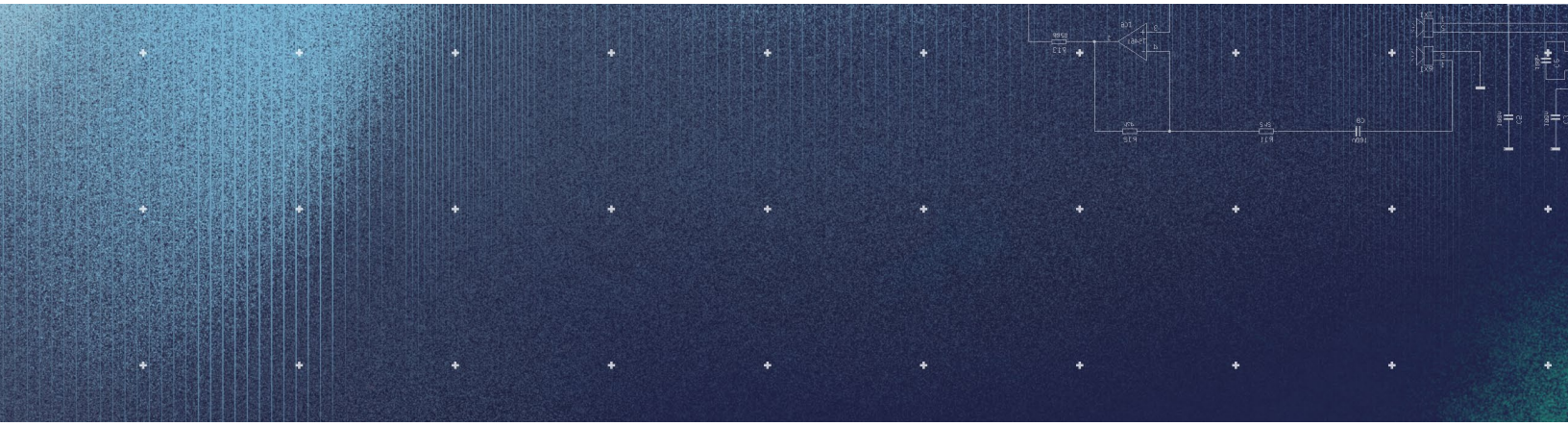
- Protection performance was measured by data transfer rates and how long the operations took to complete.
- Storage efficiency was measured by evaluating the capacity required to store all backups and comparing the total storage space required.
- Data recovery was assessed by measuring the time required to recover systems in groups, and for 100 VMs and 1,000 VMs.

While data deduplication rates were once a primary area of focus, this feature is now judged primarily by the increase in effective storage capacity. Although backup performance and efficiency are important considerations, data recovery is a primary factor when evaluating data protection options. When measuring data recovery, metrics include the restore success rate, time to power on, and full recovery time.

The term "Instant Recovery" is often used when a solution supports powering on a system or VM prior to fully restoring the data. This can be an important criterion, with Cohesity and the competing solution performing significantly differently.

Signal65 Comments: *The ability to rapidly power on multiple systems can be critical to quickly recovering from a data outage, ransomware attack or other disasters. During evaluation, Cohesity's ability to rapidly recover systems was significantly better than the competing solution.*

In all cases, the time required to recover data and applications is critical, with the impact of downtime resulting in lost revenue, reputational damage, or worse. Moreover, the Mean Time To Recovery (or MTTR) was a key criterion used during our evaluation.



Testing Methodology

Overview

Testing consisted of performing multiple backup operations, including a full backup and several incremental backup operations. Between incremental backups, differing amounts of data were modified in each of the backed-up VMs to simulate the impact of small change rates of less than 2% of total data, and one large change rate of approximately 15% of total data. This testing was focused on the time required to perform the operations, the data reduction ratio, and the total capacity consumed by the secondary / backup storage solution.

After the VMs were protected via backup, data recovery testing was also performed. The metrics measured for this testing were the success rates and the time required to restore the VM to operational status. Many vendors have an "Instant Recovery" option, enabling a VM to power on before the data is restored to the primary VMware datastore. Thus, for instant recovery, we measured both the time to power on a VM and the time required to migrate all the data from secondary storage to the original, primary storage media.

Testing Infrastructure

The testing was conducted in Signal65's lab facilities, utilizing several systems running VMware vSphere together with vSAN storage, which hosted the VM systems that were used for backup and recovery testing. The storage targets consisted of a Cohesity hyperconverged appliance as one solution, with the competitor's software-based solution utilizing two physical servers to act as data movers, along with an external storage system shared between them. All networking was 25 Gb/s to a single network switch, providing high bandwidth connectivity for all elements in the test environment.

For both solutions, all VMs being protected utilized vSAN storage as its primary storage location, with two independent VMware clusters used, each consisting of 3 nodes and NVMe storage for the two vSAN clusters. An overview of the Test Infrastructure is shown below in Figure 2:

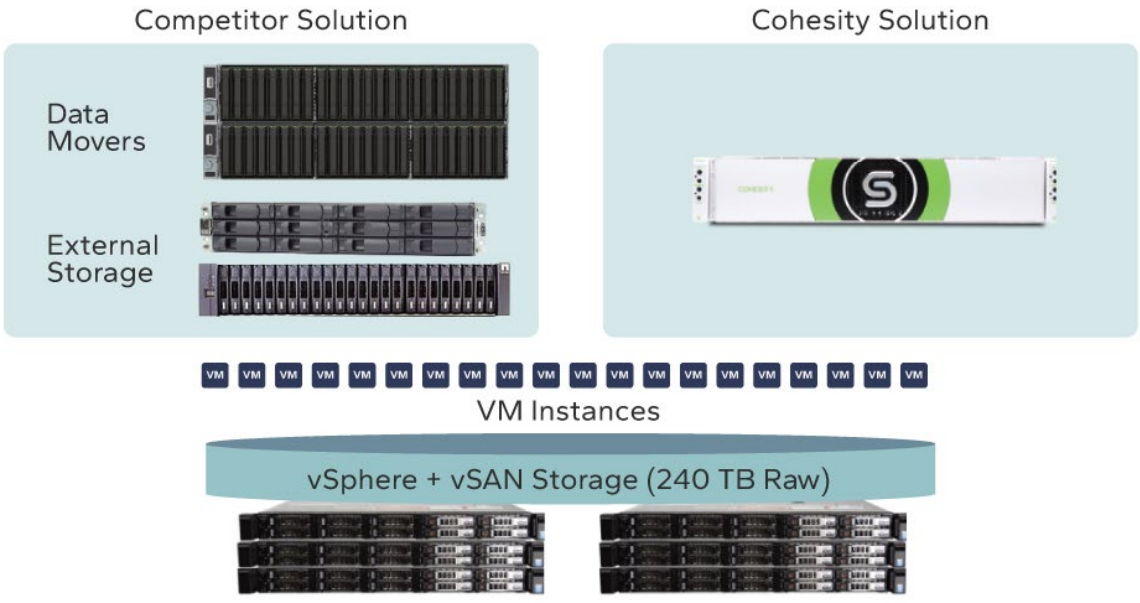


Figure 2: *Test Infrastructure*

Signal65 utilized the testing infrastructure shown above in Figure 2 to perform backup and recovery operations using two different data protection "solutions."

The Cohesity solution consisted of:

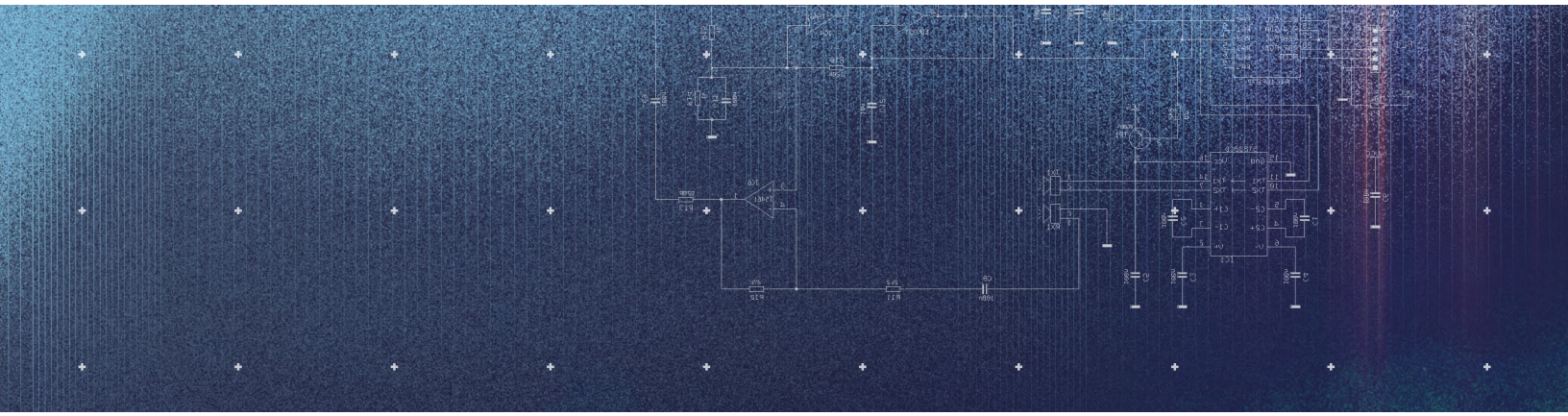
1. A single Cohesity 4-node in 2U C5036 appliance, with approximately 144 TB of raw capacity, which includes data protection software and backup storage capacity for retaining protected copies.

The second option used a software-based solution, which required the following:

1. A controller "server" running as a VM to orchestrate the data protection operations, including managing infrastructure.
2. Two media servers (aka data movers), responsible for moving data between the source and the target storage.
3. External storage, shared between the two media servers, with approximately 100 TB of usable capacity (before dedupe or compression).

To create realistic environments, two different VM configurations were utilized for protection and recovery.

- A 100 VM environment, with 4 different sized VMs consisting of both Linux and Windows VMs split between the two clusters, "A" and "B" as noted above
- A 1,000 VM environment, with a single size for Linux and Windows VMs, split between two clusters, "A" and "B"



Data Protection Testing

During the "Data Protection" portion of testing, we evaluated several criteria, including:

- The amount of time required to perform the operation
  - Both for individual VMs and for all the VMs together
- The amount of data stored on the target device which is a measure of the data reduction efficiency of the solution
- The overall ease of use and the success rate of the backup processing

Modes of Backup

VMware provides multiple methods of backing up and restoring data. However, many of these are limited to specific types of storage connectivity and therefore impose architectural constraints to utilize these methods.

The following transport modes are available in VMware. Advanced transport methods (SAN and Hot-Add) replace the proxy-based VMware Consolidated Backup (VCB) option:

- SAN (storage area network) - SAN mode is supported for directly connected storage using Fibre Channel (FC) or Internet SCSI (iSCSI) protocols and requires Enterprise VMware licensing or higher.
- NAS (network attached storage) - The NAS transport mode enables a media server agent to read or write data from the share without going through an ESXi host.
- Hot-Add - In this mode, a Media Server Agent running on a system communicates via external storage and an ESXi Server.
- Local Area Network (NBD and NBDSSL) - NBD (network block device) & NBDSSL (encrypted NBD) transmit data over the TCP/IP connection between the ESXi server and the backup target or proxy.

As our test setup utilized vSAN for primary VM storage, the SAN (or LAN Free) and NAS options were not available. Thus, the two potential methods for backing up and restoring data for the solutions were “Hot-Add” and “NBDSSL”.

VM Sizes During Testing

In the Appendix, we provide a table showing the various sizes of VMs used for testing. The terms used help explain the sizes in relative terms. However, it is also important to know their actual sizes. The sizes differed slightly between Linux and Windows VMs in each category, but roughly a Small VM was 70 GB, a Medium VM was 460 GB, Large was 3.6 TB, and Extra-large was 11.4 TB, with all those sizes being what the OS reports.

Another aspect of VM size is that the amount of data reported by the OS and that reported by VMware are different. With vSAN, using a default policy of RAID 1, resulted in VMware reporting a size 2X that of what the OS reports.

Backup Results for 100 Mixed VMs

A primary test case was backing up 100 VMs of mixed sizes, including small, medium, large, and extra-large, with a mixture of 80% Linux and 20% Windows VMs totaling approximately 85TB of primary storage. An initial backup was performed, along with incremental backup operations, with the following timings noted below in Table 1.

Operation	Cohesity	Competitor	Cohesity Advantage*
Initial Backup – 100 VMs	32h, 18m, 0s	39h, 18m, 19s	22% faster
1st Incremental	2h, 7m, 35s	2h, 54m, 50s	37% faster
Small Incremental (< 1 TB change)	35 – 39 min.	54 – 56 min.	38 – 54% faster
Large Incremental (12 TB change)	4h, 3m, 39s	7h, 18m, 32s	80% faster

Table 1: *Backup Operation Comparison for 100 Mixed VMs*

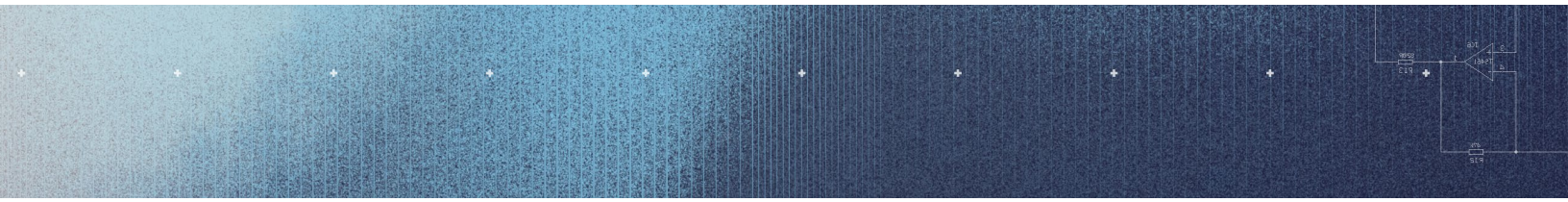
Backup Results for 1,000 Small VMs

Protecting 1,000 small VMs was similar to the mixed VM size, with the total amount of data being backed up and recovered nearly identical. Note that 1,000 Small VMs consumed approximately 85 TB of storage (more than 170 TB as reported by vSAN), with approximately 81 TB being protected. The difference of 4 TB was data that is not backed up, such as swap space.

Operation	Cohesity	Competitor	Cohesity Advantage
Initial Backup – 1,000 VMs	22h, 9m, 6s	32h, 32m, 32s	47% faster

Table 2: *Backup Operation Comparison for 1,000 Small VMs*

Overall, the Cohesity solution performed significantly faster than the competitor, with incremental backups completing 37 - 80% faster. This is an important consideration when sizing the backup solution for an environment, ensuring the ability to backup the required data in less time, or potentially protect more data during the same amount of time.



Data Recovery Testing

While data protection speed and efficiency are important considerations, the ability to recover data quickly is often a more critical issue. When data becomes unavailable due to human error, equipment failures or malicious acts, businesses depend upon the ability to restore systems to operational status quickly. Our evaluation looked at several aspects of recovery, including the following metrics:

- Restoration success rate, or percent of restoration operations that successfully completed
- The amount of time required to restore a VM, as measured by:
  - The time to power the VM on initially - “Power-on Time”
  - The time to fully migrate the VM to the target storage - “Full Recovery Time”
- The number of simultaneous VMs that could be recovered
- The overall ease of use, and of the restoration process

Note: *During recovery testing, the competitor’s solution had limited success when attempting to restore more than 5 VMs at once. While there was no firm failure rate, we did experience more errors when restoring batches of more than 7 – 15 VMs simultaneously. As a result, we limited our testing to using sets of 5 to ensure all VM’s would be recovered.*

Instant Recovery of 25% of VMs

Signal65 verified the time required to power on 25% of the VMs from the set of mixed size VMs across both Linux and Windows. This test measured the time required to power on 25 VMs.

Note: *The time scale of results between Cohesity and their competitor were significantly different, with Cohesity completing the task in under 1 minute, and their competitor requiring more than 8 hours. This was due to the competitor only being able to power on a few VMs simultaneously and then requiring the entire VM to be migrated from the backup media to primary storage before allowing another batch of VMs to be powered on.*

Operation	Cohesity	Competitor	Cohesity Advantage
Instant Power-On 25 VMs	< 1 minute	8+ hours	Orders of Magnitude

Table 3: *Backup Operation Comparison for 100 Mixed VMs*

The time shown for the Competitor was calculated based upon performing batches of recovery operations. All times listed below are for the competitor to get to 25 VMs:

- Recovery time for 4 sets of 5 Small VMs: 4h, 6m, 48s
- Recovery time for 4 sets of 1 Medium VM: 4h, 21m, 18s
- Time to power-on the 25th VM under 1 minute.
- Total calculated time was 8h, 47m (4:06:48 + 4:21:18 + 0:01:00)

Signal65 Comments: *Cohesity's recovery capabilities were significantly better than the competitor. Often, applications require multiple VMs in order to operate properly. The competitor's solution required multiple recovery sets, and several hours before the threshold of 25% of applications were functional. In contrast, Cohesity's product was able to power on all VMs, including larger VMs in under 1 minute. With Cohesity's solution, businesses are able to recover quickly, with a 100% success rate, unlike the competitor's solution.*

Small VM Recovery Comparison

For this operation, we performed a "Copy Recovery" meaning all data was copied from the backup media to the primary storage. Here, we tested restoring 5 VMs using approximately 70 GB of data. Note that the VMware reported size was approximately 160 GB, due to the 2X factor and the inclusion of Swap space. For this test, the time to completely recover the VMs to the primary storage was measured:

- 5 VMs at approximately 70 GB each, for a total of 800 GB
  - Cohesity required 26m and 30s
  - Competitor required 1 hour, 1 minute and 42s
- Cohesity was able to recover 1.78 times faster than the competitor

Recovery - 100 Mixed VMs

In comparing the results of recovering data, several elements are outlined above, with the success rate being one of the most important. For this test we performed a "Copy Recovery" meaning that the VM was copied back to primary media.

We expected a 100% success rate for both products' recovery operations. However, our testing revealed that quite often larger VMs or batches of recovery jobs with more than 10 VMs caused problems and failed recovery jobs for the competitor's product.

Operation	Cohesity	Competitor	Cohesity Advantage
Copy Recovery – 100 VMs	50h, 2m, 0s	71h, 35m, 6s	43% faster
Instant Power-On 100 VMs	< 1 minute	51 + hours *	Orders of Magnitude
Instant Recover – Then Migrate 100	52h, 13m, 0s	71h, 35m, 6s	37% faster

Table 4: *Backup Operation Comparison for 100 Mixed VMs*

As seen in Table 4, recovering 100 VMs of mixed sizes showcased an advantage for Cohesity in all cases. Important facts of the recovery include that we compared Cohesity's best performing option to the competitors fastest option. Looking at the first and third rows, the time to fully migrate showed an advantage of between 37% - 43% for Cohesity.

*** Note:** The differences were stark when evaluating the ability to perform an "Instant Power On" of 100 VMs. The exact time required for the Competitor was not measured but was instead calculated based upon the amount of time taken to recover a set of 25 VMs from Table 3. The competing solution could not reliably power on more than 5 VMs simultaneously, requiring us to create groups, and run batch recovery operations on small sets of VMs.

Signal65 Comments: *In comparing the recovery results of Cohesity to the competitor, we found Cohesity's approach delivered results in seconds, allowing businesses to resume critical operations quickly. Specifically, Cohesity's ability to power on 100 VMs, with 87 TB of effective storage capacity in under 1 minute, while the competitor's solution required more than 1 day to complete a similar process.*

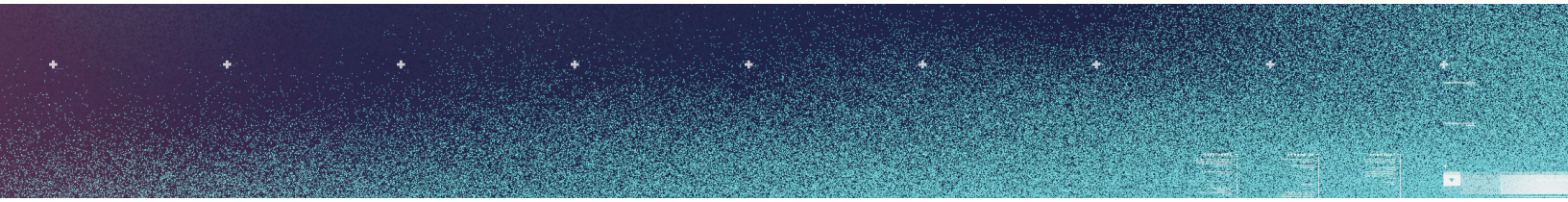
Recovery - 1,000 Small VMs

Using Copy Recovery method to restore 1,000 Small VMs of approximately 70 GB was similar to other recovery tests, with the total amount of data being backed up and recovered nearly identical. The total amount of data stored by both backup products for 1,000 Small VMs was approximately 81 TB.

Operation	Cohesity	Competitor	Cohesity Advantage
Copy Recovery 1,000 VMs	11h, 47m, 28s	15h, 32m, 5s	1.3X faster
Instant Recovery, then Migrate	12h, 36m, 29s	29h, 6m, 43s	2.3X faster

Table 5: *Backup Operation Comparison for 1,000 Small VMs*

For the recovery testing shown in Table 5, we utilized the fastest option for Cohesity (NBDSSL) compared to the fastest option for the Competitor (Hot-Add).



Other Considerations

Beyond measuring data protection and recovery speed and the amount of time operations require, there are other factors to consider. Specifically, the ability to backup and recover without errors can become a significant issue if the product doesn't deliver as expected.

Another aspect of these two data protection options is the difference in complexity, both in terms of initial setup and ongoing maintenance of the backup infrastructure. The Cohesity solution consists of one or more appliances, sized based upon the amount of data to retain and the desired retention period.

The competing software-based solution consisted of a controller VM to coordinate activities, along with multiple data mover physical servers and additional storage. Although the competing solution offers configuration flexibility, it requires additional software to install, configure, and manage. As a result, the infrastructure complexity of the alternative solutions was higher, requiring more IT staff administration time and cost to manage.

Additionally, the competitor's solution experienced recovery issues due to the architecture of the NAS datastores created to facilitate the instant recovery process. Multiple errors were noted in VMware logs regarding NFS timeouts or other datastore access issues. In contrast, no such errors were reported when recovering from the Cohesity system.

Although these aspects were not meant to be a part of the evaluation, their impact on IT operations should be considered when comparing a Cohesity appliance to alternative solutions.

Final Thoughts

In today's landscape, protecting sensitive corporate information from loss is one of the most important responsibilities that IT staff are tasked with performing. Although data protection speed and storage efficiency are important measures, perhaps no metric is more critical than the time required to restore multiple applications when a mistake or data loss is encountered. When any outage occurs for multiple applications, the ability to quickly recover all VMs is critical and can have significant financial impact as well.

Signal65 Comments: *Cohesity's appliance provided a significantly better result compared to that of a leading competitor by nearly every measure. The backup speed advantage of Cohesity ranged from 50% better up to 10X better, enabling organizations to shrink their backup windows. Additionally, Cohesity had a higher data reduction ratio or effective capacity, enabling organizations to store more data in the same usable capacity.*

The ability to quickly recover one or more VMs can be critical for resuming business operations after data loss, corruption or other accidental or natural disasters occur. A growing concern for companies of all sizes today is a ransomware attack. While backup alone does not safeguard IT systems, it is one of the primary methods for protecting against such attacks. Additionally, with Cohesity's built-in protection capabilities and the addition of services such as Cohesity FortKnox off-site cloud cyber vaulting, companies have the means to ensure their critical data is protected from disasters, including ransomware attacks.

Signal65 Comments: *The ability to resume operations quickly after a disaster depends upon the ability to get multiple systems up and running. Unlike the competitor which required more than 8 hours to resume operations with 25 systems, Cohesity enables companies to resume operations in under a minute - the value of this difference cannot be understated.*

However, the most important difference between these two solutions was Cohesity's ability to rapidly recover (i.e. "power on") all 100 VMs, with no failures and consuming 85 TB of primary storage in under 1 minute. In contrast, the competing solution repeatedly had recovery operations fail and required more than 8 hours to power a set of 25 VMs.

Appendix

Infrastructure for Testing

Common Infrastructure

The following infrastructure was used for the VMs which were backed up to the two solutions.

- Six (6) servers were utilized for the two clusters, each with its own vSAN cluster using local NVMe storage devices.
- An additional server was used to provide access VM's, along with a vCenter server instance to manage the VMware infrastructure.
- VMware ESXi version 8.0 U1 was installed on each system, along with a vCenter server instance.

Networking

Networking was 25 Gb/s per connection was used, with one connection to each of the 7 total servers. Additionally, a 40 Gb/s network connection was used between the external storage and the switch, which was used as target storage for the competitor's backup solution.

Competitor's Infrastructure

Two data-mover physical hosts were also used as part of the competitor's solution, each with 25 Gb/s network connectivity. Each system used 2 x 22 core CPUs (E5-2699 v4) along with 256 GB of RAM. These data mover systems ran Windows Server 2022, with the appropriate media agents installed as required by the competitor.

The competitor's solution also used external NAS storage system, along with one shelf of SSDs and one shelf of SATA HDDs for a total usable capacity of approximately 150 TB. Network connectivity was 2 x 40 Gb/s Ethernet, one per controller in an HA configuration.

Cohesity Infrastructure

As seen in Figure 2, the entire Cohesity solution consisted of a single, 4-node in 2U C5036 appliance, with approximately 144 TB of raw capacity.

Data for Backing up and Restoring 100 VM's of Mixed Sizes

Backup	Cohesity					Competitor					Cohesity Advantage
	Reported Size (TB)	Data Written	Reported (TB/HR)	Effective Xfer	Duration	Reported Size (TB)	Data Written	Reported (TB/HR)	Effective Xfer	Duration	
Full	84.14	61.90	2.6	0.00	32:18:00	75.53	67.89	1.92	0.00	39:18:19	1.22x
1st Incremental	4.39	0.77	2.06	2.06	2:07:35	4.16	1.38	1.44	1.43	2:54:50	1.37x
2nd Incremental	0.95	0.23	1.47	1.44	0:39:29	1.03	0.32	1.12	1.10	0:56:09	1.42x
3rd Incremental	**12.31**	**1.97**	**3.04**	**3.04**	**4:02:39**	**11.33**	**3.75**	**1.55**	**1.55**	**7:18:32**	1.81x
4th Incremental	0.93	0.22	1.44	1.41	0:39:47	1.04	0.32	1.16	1.13	0:55:00	1.38x
5th Incremental	0.93	0.22	1.6	1.57	0:35:43	1.01	0.31	1.01	1.10	0:54:58	1.54x
6th Incremental	0.93	0.22	1.55	1.52	0:36:38	1.01	0.32	1.01	1.11	0:54:36	1.49x

Note: In the "Reported Size" category below, the values differ because Cohesity and their competitor report a VMs size differently. Cohesity includes the swap space for Linux and Page File for Windows as part of the VMs size. However, their competitor does not, which results in a difference of approximately 8 GB per VM. This value across the 1,000 VMs results in a difference of about 7.5 TB in total size as seen below.

Recovery	Cohesity			Competitor			Difference %			Cohesity X Times Faster	Cohesity vs. HotAdd
	Reported Size (TB)	Data Written	Duration	Reported Size (TB)	Data Written	Duration	Redux (<)	Time (<CV)	Xfer (>)		
Copy Recovery - NBDSSL	84.14	84.14	50:02:00	75.53	75.53	153:43:28	-10.23%	207.24%	70.78%	3.07x	
Copy Recovery - HotAdd	84.14	84.14	0:00:00	75.53	75.53	71:35:06	-10.23%	N/A	N/A	N/A	1.43x
Instant Recovery	84.14	84.14	52:13:00	75.53	75.53	NaN	-10.23%	N/A	N/A	N/A	
Copy Recovery - Large and XL VM	15.40	15.40	7:39:22	15.40	15.40	78:05:19	0.00%	919.95%	90.20%	10.20x	

The VM sizes for the 100 VM mixed workload consisted of different sizes using both Windows and Linux of small, medium, large and extra-large as defined below:

				Linux		Windows		
	Linux Count	Windows Count	Total Count	Per VM (GB)	Used (GB)	Per VM (GB)	Used (GB)	Total Used (GB)
Small	60	16	76	68	4,080	75	1,200	5,280
Medium	8	2	10	460	3,680	465	930	4,610
Large	10	2	12	3,560	35,600	3,668	7,336	42,936
X Large	1	1	2	11,674	11,674	11,131	11,131	22,805
Total	**79**	**21**	**100**	**15,762**	**55,034**	**15,339**	**20,597**	**75,631**

Note: The table above shows that the total used is 75.6 TB, which does not include the swap space. When adding in the capacity actually consumed, that value is approximately 85 TB.

- A 100 VM environment, with 4 different sized VMs consisting of both Linux and Windows VMs split between the two clusters, "A" and "B" as noted above
  - 76 small VMs consumed approximately 5.3 TB
  - 10 medium VMs consumed approximately 4.6 TB
  - 12 large VMs consumed approximately 43 TB
  - 2 extra-large VMs consumed approximately 23 TB
- A 1,000 VM environment, with a single size for Linux and Windows VMs, split between two clusters, "A" and "B".
  - Of these 80% (800) were Linux VMs and 20% (200) were Windows VMs
  - Each VM was appx. 8 GB, for a total size of 85 TB

Important Information About this Report

CONTRIBUTORS

Russ Fellows
VP, Labs | Signal65

Stephen Cargile
Competitive Analysis Engineer | Signal65

PUBLISHER

Ryan Shrout
President and GM | Signal65

INQUIRIES

Contact us if you would like to discuss this report and Signal65 will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts, but must be cited in-context, displaying author's name, author's title, and "Signal65." Non-press and non-analysts must receive prior written permission by Signal65 for any citations.

LICENSING

DISCLOSURES

Signal65 provides research, analysis, advising, and consulting to many high-tech companies, including those mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

IN PARTNERSHIP WITH

COHESITY

ABOUT SIGNAL65

Signal65 is an independent research, analysis, and advisory firm, focused on digital innovation and market-disrupting technologies and trends. Every day our analysts, researchers, and advisors help business leaders from around the world anticipate tectonic shifts in their industries and leverage disruptive innovation to either gain or maintain a competitive advantage in their markets.

signal65

signal65

CONTACT INFORMATION
Signal65 I signal65.com