

Actiphy ImageServer

White Paper

Reduce Backup Storage, Offload Processing, and
Simplify Backup Operations

Executive Summary

Creating a backup is only the first step in a successful data protection strategy.

As backup environments grow, organizations must manage increasing backup data volumes, multiple generations and recovery points, storage capacity, replication targets, verification processes, and the processing resources required to maintain them. The operational challenge is no longer simply creating backups—it is managing them efficiently and ensuring usable recovery points are available when needed.

Actiphy ImageServer addresses these challenges by providing a centralized platform to store, manage, and post-process backup images created by ActiveImage Protector™.

ImageServer combines ImageCenter's centralized backup image management capabilities with StorageServer, secure storage designed specifically for ActiveImage Protector. It also provides Inter-File Deduplication, Workflow, Replication, Verify, Consolidation, BootCheck™, and file-recovery capabilities.

Together, these technologies address four important areas of backup operations:

Reduced physical storage requirements. Inter-File Deduplication identifies common blocks across backup image files within the same bucket and stores shared blocks only once. In one Actiphy test involving five virtual machines with common data, 170 GB of uncompressed backup images used 50.0 GB of physical bucket storage—a reduction of about 71%.

Reduced processing load on protected systems. ImageServer can perform Verify, Replication, Consolidation, and BootCheck operations rather than the backup source. The workflow lets administrators control the sequence and timing of these operations.

Improved recovery readiness. Routine Verify, BootCheck, and Replication operations provide administrators with current information about available recovery points before a failure occurs.

Centralized backup storage and management. Backup data arrives via the QUIC protocol and is organized into storage buckets, without exposing the backup destination as a Windows shared folder. Bucket-level and client-level quotas provide administrators with control over storage utilization.

The result is an architecture that extends backup beyond image creation. ImageServer provides a centralized environment where administrators can store, manage, optimize, process, verify, replicate, and prepare ActiveImage Protector backups for recovery.

1. The Growing Operational Challenge of Backup

Backup systems have traditionally focused on one fundamental objective: to create a reliable copy of production data that can be used after data loss or system failure.

That objective remains essential, but modern backup operations involve considerably more than creating backup files.

Organizations may protect multiple physical and virtual systems, retain multiple generations of backups, replicate data to remote or cloud storage, verify backup integrity, test system bootability, consolidate incremental images, and maintain enough recovery points to meet recovery requirements.

As the number of protected systems and retained backups increases, several operational challenges emerge.

1.1 Backup Images Frequently Contain Duplicate Data

Storage consumption presents an immediate challenge.

Consider a group of virtual machines running the same operating system and many of the same applications. Each machine may contain large amounts of identical or substantially similar data.

The same effect occurs over time. When you periodically create new base images for the same system, you may repeat much of the underlying operating system, applications, and unchanged user data from one generation to the next.

Traditional storage treats those backup images as separate files even when significant portions of their contents are identical.

As the number of protected systems and retained generations grows, that duplicated data consumes physical storage.

ImageServer addresses this problem with Inter-File Deduplication, which identifies common blocks among eligible backup image files within the same bucket and allows those blocks to be shared.

1.2 Post-Backup Operations Compete with Production Workloads

Backup creation is not necessarily the end of backup processing.

Organizations may need to:

- Verify backup integrity.

- Replicate backups to secondary or remote storage.
- Consolidate incremental backup images.
- Perform BootCheck operations to test whether backup images can boot.

When these operations run on the protected system, they consume CPU, memory, network bandwidth, and storage I/O that production applications may also need.

Long-running post-backup operations can also overlap with subsequent backup windows.

ImageServer provides a separate processing environment, offloading these operations from protected systems. Workflow controls the order in which tasks execute and the periods during which individual operations may run.

1.3 A Backup File Is Not the Same as a Recovery-Ready Backup

A backup may exist without an administrator immediately knowing whether it recently passed verification, whether a system image completed BootCheck, or whether the required recovery point replicated to another location.

Finding those answers only after an incident consumes valuable recovery time.

ImageServer brings backup storage, image management, verification, bootability testing, and replication status into the same operational environment.

Instead of asking only:

“Did the backup complete?”

administrators can begin asking the more important question:

“What recovery points do we have available, and what do we already know about them?”

1.4 Backup Storage Becomes Increasingly Difficult to Manage

Different departments, sites, and systems may use different backup destinations. Administrators must monitor available storage capacity, authentication, permissions, client connectivity, and retention across those destinations.

Even when multiple systems share a common storage destination, administrators still need to understand how much capacity each system consumes and prevent one client or workload from exhausting storage needed by others.

ImageServer consolidates backup storage into managed buckets. Administrators can assign quotas to individual buckets as well as default and individual quotas to clients.

The ImageServer Web Console provides centralized visibility into bucket capacity, physical disk capacity, connected clients, and transfer activity.

This changes backup storage from a collection of file destinations into a managed backup-storage resource.

2. A Centralized Architecture for ActiveImage Protector Backups

Actiphy ImageServer combines StorageServer and ImageCenter capabilities into a centralized platform for receiving and managing ActiveImage Protector backup images.

The basic flow is:

ActiveImage Protector → ImageServer → Management and Post-Processing → Secondary or Remote Storage

Within ImageServer, several functions work together:

1. **StorageServer** receives backup data and manages storage buckets.
2. **Inter-File Deduplication** reduces physical storage requirements by sharing common blocks among eligible images within the same bucket.
3. **Image Management** organizes related base, incremental, and differential images into image sets and recovery points.
4. **Workflow** controls post-backup Verify, Replication, Consolidation, and BootCheck operations.
5. **Image Browser** lets you retrieve files and folders from selected recovery points.
6. **Replication** provides copies of backup images to supported remote or cloud storage targets.

This architecture separates backup creation on protected systems from many storage-management and post-processing activities that occur after a backup is created.

2.1 Dedicated Backup Communication Using QUIC

ImageServer incorporates StorageServer, which uses the QUIC protocol for backup-data communication.

Backup destinations can be used without exposing them as Windows shared folders. Bucket authentication controls access to backup storage rather than Windows share permissions.

Authentication for the ImageServer Web Console is managed separately from authentication used to access backup storage.

This separation lets administrators manage the backup repository as a dedicated backup resource rather than another general-purpose network share.

2.2 Incoming Backup Cache

ImageServer includes an incoming backup cache that temporarily holds incoming data and adjusts the receiving process according to the status of writes to destination storage.

The cache can absorb temporary workload variations while receiving backup data. Administrators can configure the cache storage location, and cache behavior also considers memory usage.

Sustained backup-transfer performance ultimately depends on the network, server, and destination-storage configuration.

2.3 Buckets, Quotas, and Client Management

Storage is organized into buckets, each with its own name and storage path.

Buckets can be divided by organization, location, department, workload, or other operational requirements.

Administrators can configure:

- Overall bucket quotas.
- Default client quotas.
- Individual client quotas.
- Image passwords required for post-backup processing of encrypted backups.

The Web Console provides centralized monitoring of storage capacity and client connections.

Image passwords used to process encrypted backup images are separate from authentication used to access the backup destination.

3. Managing Backup Images as Recovery Points

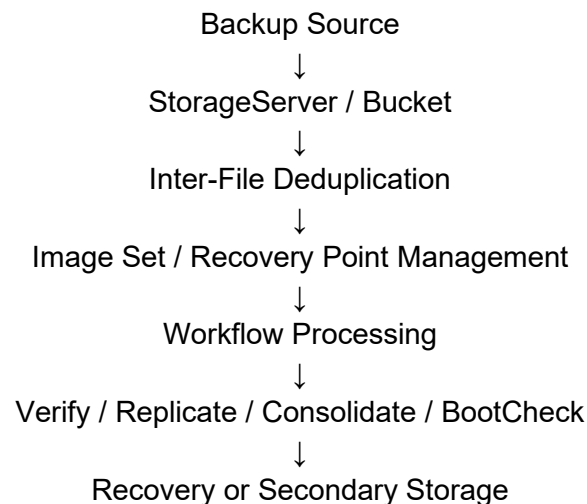
A backup environment becomes easier to manage when administrators can work with recovery points rather than individual files.

ImageServer's ImageCenter functionality organizes related base, incremental, and differential images into Image Sets.

Administrators can review the backup date and time, generation, size, and associated recovery points, then select images for operations such as Verify, BootCheck, or File Recovery.

This creates a logical view of backup history, rather than requiring administrators to interpret collections of backup files manually.

The overall process can be represented as:



Inter-File Deduplication is optional. You can also use image management and post-backup processing for backup images stored without Inter-File Deduplication.

4. Reducing Storage Requirements with Inter-File Deduplication

Storage efficiency becomes increasingly important as organizations protect more systems and retain more generations.

ActiveImage Protector already provides deduplication and compression while creating backup images. ImageServer introduces another layer of storage optimization: **Inter-File Deduplication**.

These technologies operate at different points in the backup process and solve different problems.

4.1 How Inter-File Deduplication Works

Inter-File Deduplication—called **Global Inter-File Deduplication** in the ImageServer settings—operates on eligible backup image files stored in the same bucket.

When ImageServer receives an eligible image, such as a base image or consolidated image, it divides its data into blocks.

ImageServer compares those blocks with blocks already registered within the bucket.

When a matching block already exists, ImageServer does not store another physical copy. Instead, the image's index references the existing block.

If the block is unique, it is stored.

Conceptually:



If the block already exists:

Reference Existing Block

If it does not:

Store New Block

Both paths then contribute to:

Image Index → Logical Backup Image

When ImageServer needs the image, it reconstructs the logical image from its index and the associated shared blocks.

4.2 Safe Block Reclamation

Multiple backup images may reference shared blocks.

Deleting one image does not automatically delete shared blocks another image still requires. Blocks are retained as long as an image references them.

Blocks no longer referenced by any image can be reclaimed for subsequent storage use.

During idle periods, ImageServer can also reorganize storage space to reduce fragmentation.

4.3 Two Different Layers of Deduplication

ActiveImage Protector's deduplication and compression and ImageServer's Inter-File Deduplication complement each other.

	ActiveImage Protector Deduplication & Compression	ImageServer Inter-File Deduplication
Processing location	Backup source	ImageServer
Data being processed	Source data being backed up	Eligible backup images within a bucket
Primary objective	Reduce the amount of data stored in the created backup image	Reduce duplicate physical data across stored images
Scope	Individual backup operation	Common blocks among eligible images in the same bucket
Configuration	ActiveImage Protector backup settings	ImageServer global settings

Because Inter-File Deduplication occurs after backup data reaches ImageServer, it is intended to reduce storage consumption at the backup destination—not network traffic between the backup source and ImageServer.

5. Measuring the Storage-Savings Opportunity

The benefit of Inter-File Deduplication depends heavily on how similar the stored data is.

Environments with multiple systems sharing the same operating system, common applications, standardized configurations, or repeated base images are more likely to contain reusable blocks.

Actiphy performed tests to illustrate the potential storage reduction.

5.1 Five Virtual Machines with Common Data

In one test, we created base backups simultaneously from five virtual machines containing common system data and data files.

The total size of the uncompressed backup images was:

170 GB

After Inter-File Deduplication, physical bucket usage was:

50.0 GB

This represents an approximate reduction of:

71%

We ran the same test with backup images already reduced using ActiveImage Protector's deduplication and compression.

Those backup images totaled:

101 GB

Physical ImageServer bucket usage after Inter-File Deduplication was:

46.1 GB

Compared with the 101 GB input, this represents an additional storage reduction of approximately:

54%

This illustrates an important architectural distinction: ImageServer can identify common blocks between backup image files, even when ActiveImage Protector has already reduced data within the individual backup images.

5.2 Ten Generations from the Same Client

A second test examined common data across generations.

We created ten generations of base backups from the same client.

Total backup size before Inter-File Deduplication:

108 GB

Physical bucket usage after the ten generations were stored:

37.6 GB

This represents an approximate reduction of:

65%

The result shows how common data can be shared not only across different protected systems, but also across generations within the same system.

5.3 Understanding These Results

Do not interpret these measurements as guaranteed product-performance figures.

Actual storage savings depend on factors including:

- Similarity of data among protected systems.
- Amount of changed data.
- Backup method.
- Compression.
- Image composition.
- Server configuration.
- Storage configuration.

However, the tests show the architectural opportunity: when backup images contain common data, Inter-File Deduplication lets ImageServer avoid storing identical blocks repeatedly.

6. Moving Post-Backup Processing Away from Production Systems

Storage consumption is only one part of the backup-management problem.

After creating a backup, organizations may perform several additional operations before it becomes part of their recovery strategy.

ImageServer Workflow lets you organize and schedule these operations.

Supported Workflow task types include:

- Verify
- Replication
- Consolidation
- BootCheck

Instead of running these processes on the backup source system, ImageServer can perform them.

This separation helps reduce competition between backup-management tasks and production workloads.

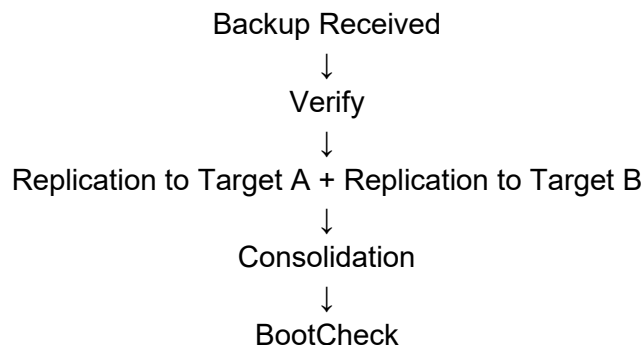
6.1 Workflow Stages

A Workflow consists of stages.

Administrators define the stage order and may include multiple tasks of the same type within a stage.

For example, a Replication stage might include multiple replication tasks that send backup images to different destinations.

A Workflow might look like:



Organizations do not need to use every task type. Organizations can assemble Workflow stages to meet operational requirements.

6.2 Execution Windows

Administrators can control when Workflow tasks execute.

Scheduling options include immediate execution, specific dates and times, weekly or monthly schedules, and specified days of the week within a month.

Execution windows can also define start and end times and repeat intervals.

This lets organizations move resource-intensive processing away from periods when production systems, backup infrastructure, networks, or storage are under the heaviest load.

6.3 Exclusion Periods

Some tasks, including Replication, support exclusion periods.

Administrators can specify dates, days of the week, or time periods when a task should not run.

Execution windows define **when a task may run**.

Exclusion periods define **when it must not run**.

Together, they provide more precise control over backup infrastructure usage.

6.4 Failure Handling and Monitoring

Workflow rules can be applied by folder. Administrators can choose whether child folders inherit task settings and whether subsequent processing continues when a preceding task fails.

Administrators can monitor task execution through ImageServer tasks and events, with email notifications available for operational awareness.

7. From Successful Backup to Recovery Readiness

A completed backup job confirms that it created backup data.

It does not, by itself, answer every question an administrator may face during recovery.

ImageServer provides several operations that give administrators additional information about available recovery points before they need them.

7.1 Verify

ImageServer provides Quick Verify and Deep Verify.

Quick Verify checks for changes or corruption since the image was created using verification data recorded in the image file.

Deep Verify reads volume data within the image to verify backup integrity.

Organizations can use these verification methods differently—for example, Quick Verify for routine checking and Deep Verify for periodic verification.

Available Verify options depend on the image format and the way the image was created.

7.2 BootCheck

BootCheck adds an extra layer of recovery validation by checking whether supported backup images can boot on a local or remote Hyper-V host.

Administrators specify the Hyper-V host, timeout, and retry behavior. If a BootCheck operation fails, ImageServer can be configured to retry using the previous incremental backup.

A successful BootCheck should not be interpreted as complete application-level recovery testing. Business applications, transactions, dependencies, and consistency among multiple systems should still be tested according to the organization's recovery procedures.

Instead, BootCheck provides useful information on whether the protected system represented by the backup image can reach the tested boot state.

7.3 Replication

Replication creates additional copies of backup image files on remote or secondary storage.

Supported destinations include network shares, FTP/FTPS, SFTP, WebDAV, Amazon S3 and S3-compatible storage including Wasabi, and Microsoft Azure.

Administrators can configure generation handling, destination subfolders, retry behavior, bandwidth limits, and I/O performance.

Mirror operations can also control synchronization and deletion behavior according to retention requirements.

7.4 Replication View

Creating a replication task is only part of the operational requirement. Administrators must also be able to determine what actually exists at the destination.

Replication View displays source and destination image sets side by side.

It identifies whether images exist at both locations, whether they match, and which copy is newer.

You can also copy images from the replication source to the destination, or from the destination back to the source, when needed. This gives administrators visibility into both the replication process and the resulting recovery data.

8. Managing Incremental Images and Individual File Recovery

Backup retention policies often require administrators to balance the number of available recovery points against storage requirements and operational complexity.

ImageServer Consolidation combines multiple ActiveImage Protector incremental backups according to configured policies.

Administrators can specify:

- Conditions that trigger consolidation.
- Retention periods for source images.
- Reconsolidation behavior.
- Consolidation policies.

This lets you incorporate incremental-image management into the same Workflow used for other post-backup processes.

ImageServer also provides Image Browser for file-level recovery.

Administrators select a recovery point, mount the backup, and retrieve required files or folders without restoring the entire protected system.

9. Aligning Backup Operations with Recovery Objectives

Backup technology supports recovery objectives, but technology alone cannot define or guarantee them.

ImageServer provides information and capabilities that help organizations plan for Recovery Time Objective (RTO), Recovery Point Objective (RPO), and recovery consistency across related systems.

9.1 Recovery Time Objective — RTO

RTO defines the target amount of time required to restore a service after an interruption.

ImageServer can help reduce time spent identifying a recovery candidate by maintaining Image Sets and providing historical Verify, BootCheck, and Replication information.

Actual recovery time also depends on factors outside ImageServer, including recovery-target performance, operating-system and application startup time, available infrastructure, and organizational recovery procedures.

9.2 Recovery Point Objective — RPO

RPO represents the maximum acceptable data loss, expressed in time.

Replication can preserve recovery points on secondary or remote storage.

Actual RPO depends primarily on the ActiImage Protector backup interval and the time required to make required recovery points available at the appropriate recovery location.

9.3 Recovery Consistency Objective — RCO

For this white paper, RCO refers to the objective of maintaining consistency among multiple restored systems and associated business data.

Verify and BootCheck can provide information about individual backup images, but organizations must evaluate application and transactional consistency among interconnected systems using application-specific and organization-specific procedures.

ImageServer does not determine whether an organization has achieved its RTO, RPO, or RCO.

Instead, it provides backup-management information and processing capabilities that organizations can incorporate into their own recovery planning and testing.

10. ImageServer Compared with General-Purpose Backup Storage

A standard file server or NAS can provide a destination for ActiveImage Protector backup files.

ImageServer approaches the destination as a managed component of the backup and recovery environment.

Capability	Shared Folder / General Storage	ImageServer
Backup access	Authentication and permissions determined by storage platform	QUIC and bucket authentication
Capacity management	Storage-platform dependent	Bucket and client quotas
Backup-image management	Backup software or separate tools	Image Sets and Recovery Points through Web Console
Post-backup processing	Performed through ActiveImage Protector or other management tools	ImageServer Workflow
Cross-image deduplication	Storage/product dependent	Inter-File Deduplication within individual buckets
Replication visibility	Replication or destination-specific tools	Replication View
Recovery validation information	Tool dependent	Integrated Verify and BootCheck results

This comparison is not intended to evaluate the capabilities of individual NAS or storage products. Instead, it illustrates the difference between using storage simply as a destination and incorporating the backup destination into the broader backup-management process.

11. Example Deployment Scenarios

ImageServer supports several operational models, depending on the number of protected systems, available storage, and recovery requirements.

11.1 Multiple Systems Sharing Central Backup Storage

An organization protecting multiple servers or virtual machines can use ImageServer as a common backup destination.

Buckets and client quotas provide storage controls, while Inter-File Deduplication can reduce physical storage requirements when backup images contain common blocks.

This model may be particularly useful for environments with standardized virtual machines or systems that share common operating systems and applications.

11.2 Separating Backup Processing from Production Systems

Organizations concerned about the CPU or storage-I/O impact of post-backup processing can deploy ImageServer on a separate system.

ActiveImage Protector creates the backups while ImageServer handles subsequent Verify, Replication, Consolidation, and BootCheck operations according to Workflow rules.

This separates production system protection from much of the ongoing processing required to manage the resulting backups.

11.3 Maintaining Secondary or Remote Recovery Copies

ImageServer can also serve as the central point for replicating backups to secondary storage.

Workflow can automate Replication, while Replication View provides visibility into the relationship between source and destination recovery points.

Organizations can combine this with Verify and BootCheck operations as part of their broader recovery-readiness procedures.

12. Evaluating ImageServer in Your Environment

Backup environments differ significantly, so evaluation should use representative production backup data and realistic retention requirements.

Actiphy recommends evaluating areas including:

Storage efficiency. Measure physical bucket usage while retaining the expected number of backup generations and evaluate the storage savings achieved through Inter-File Deduplication.

Concurrent backup performance. Measure backup completion time and destination-storage load when ImageServer receives backups from multiple clients.

Post-backup processing. Confirm that Verify, Replication, Consolidation, and BootCheck operations can complete within required execution windows.

Replication and recovery. Confirm the required images are present at replication targets and test retrieving files from appropriate recovery points.

Organizations currently using ImageCenter or StorageServer should also review product versions, stored backup data, and existing task configurations when planning migration.

Conclusion

The operational value of a backup is ultimately determined when recovery is required.

As backup environments grow, simply creating more backup files can introduce new challenges: increasing storage requirements, duplicate data, additional processing workloads, more complex replication, and greater difficulty determining which recovery points are ready to use.

Actiphy ImageServer brings these activities into a centralized environment designed specifically for ActiveImage Protector backups.

By combining dedicated backup storage, Inter-File Deduplication, centralized image management, Workflow-based post-processing, verification, BootCheck, replication, and file recovery, ImageServer helps organizations move from simply storing backups toward systematically managing recovery points.

For organizations protecting multiple systems or retaining more backup generations, that distinction becomes increasingly important.

ImageServer provides the storage and processing layer needed to manage those backups efficiently while giving administrators greater visibility into the recovery resources available when they are needed.

For information about supported environments, licensing, pricing, and evaluation options, contact Actiphy.

Feature availability and supported environments depend on the deployed product version. Storage-reduction measurements described in this document were obtained under specific test conditions and are not guaranteed product-performance figures. Actual results vary according to workload, data similarity, backup configuration, storage, network, and server environment.

ActiveImage Protector™, BootCheck™, and Actiphy ImageServer are trademarks of Actiphy Inc. All other trademarks and registered trademarks are the property of their respective owners.