

NAKIVO®

VMware vSphere Backup

**Top 10 Best Practices with
NAKIVO Backup & Replication**

Table of Contents

Executive Summary	3
Introduction	4
Phase I. Data Protection Strategy and Planning	5
1. Keep Your Software Up-to-Date	5
2. Align Your Strategy with Business Needs	5
3. Assess Your Ability to Meet Recovery Objectives	6
4. Secure Your Backup Environment	6
Phase II. Optimizing the Backup Process	9
5. Minimize VM Backup Size	9
6. Create Application-Aware Backups	11
7. Verify VM Recoverability	12
Phase III. Maximizing Performance	12
8. Ensure Efficient VM Recovery	13
9. Leverage Automation Techniques	14
10. Adjust to Changing Circumstances	17
Bonus Tip: Monitor Your VMware vSphere Infrastructure	20
Conclusion	21
NAKIVO Backup & Replication at a Glance	22
About NAKIVO	22

Executive Summary

VMware delivers powerful virtualization software for creating and managing virtual infrastructures. By simulating hardware functionality through virtual machines (VMs), VMware vSphere offers businesses greater operational flexibility, reduced overhead and simplified administration.

When it comes to protecting VMware environments, businesses need backup and recovery software that is just as agile and efficient as their virtualization software. This whitepaper lays out the best practices for protecting VMware vSphere VMs with NAKIVO Backup & Replication to help businesses avoid data loss in vCenter-managed and standalone ESXi workloads. The 10 VMware vSphere backup best practices presented here cover the three phases of backup administration:

1. Data Protection Strategy and Planning
2. Optimizing the Backup Process
3. Maximizing Performance

Phase I: Data Protection Strategy and Planning

With a robust data protection strategy coupled with an enterprise-class backup solution, businesses can easily set expectations, improve accountability and establish consistency. A solid strategy also makes it easier to communicate IT budgeting needs by linking infrastructure capacity and data protection metrics.

Phase I best practices:

1. Keep your software up-to-date.
2. Align your strategy with business needs.
3. Assess your ability to meet recovery objectives.
4. Secure your backup environment.

Phase II: Optimizing the Backup Process

Data protection activities should not compromise operational efficiency or hog all available resources. To avoid straining storage or network bandwidth, NAKIVO Backup & Replication provides VMware vSphere backup optimization features that reduce the impact of data protection on your production environment. To achieve optimal results, you should clearly understand how these features work and how to use them.

Phase II best practices:

5. Minimize VM backup size.
6. Create application-aware backups.
7. Verify VM recoverability.

Phase III: Maximizing Performance

Just like a business environment, an IT infrastructure is hardly static. To maximize efficiency, you should aim to reduce complexity, improve recovery times and verify whether established processes are still the best fit for your current situation.

Phase III best practices:

8. Ensure efficient VM recovery.
9. Leverage automation techniques.
10. Adjust to changing circumstances.

Introduction

NAKIVO Backup & Replication delivers advanced backup and recovery functionality designed specifically for VMware vSphere environments. The data protection solution leverages native VMware tools and offers additional features to simplify administration, streamline processes, boost performance and lower storage costs.

With fast installation and no special technical training required, you can begin protecting your VMware vSphere VMs nearly instantly. However, to ensure the optimal use of your resources and the recoverability of your data with NAKIVO Backup & Replication, make sure to follow NAKIVO's 10 best practices for VMware vSphere data protection.

These practices address the technical aspects of VM backup and recovery, such as network load management, as well as strategic aspects, such as defining recovery metrics and testing backup procedures. They highlight how specific activities can directly contribute to the larger objectives of data resiliency, high availability and cost reduction.

Phase I. Data Protection Strategy and Planning

Forming a solid data protection strategy ensures that your VMware vSphere environment is protected. While the planning process may initially appear daunting, it can be broken down into four manageable steps.

1. Keep Your Software Up-to-Date

Before getting into the details of strategy and planning, make sure that you are using the most up-to-date versions of VMware vSphere and NAKIVO Backup & Replication. New versions of VMware vSphere come with advanced features to simplify management of your virtual infrastructure, improve performance and increase security. Similarly, NAKIVO Backup & Replication regularly receives new updates that add new backup destinations, expand recovery options, improve reliability and streamline backup management.

NAKIVO Backup & Replication automatically checks for updates once a day. A notification will appear in the web interface if an update is available. By clicking the notification link, you can choose to download and update immediately or schedule the update for installation at a later time.

2. Align Your Strategy with Business Needs

For the vast majority of businesses, every department – from core operations to HR and accounting – relies on data and application availability. Yet, just as different business units have varying levels of importance for business continuity, data and applications also have varying levels of criticality for different operations. As such, businesses should trace which departments are most important to business operations as well as which applications and data require high availability.

Once you have a clear understanding of how business operations depend on different applications and datastores, assign priority levels to each application and datastore accordingly. For each priority level, you should define expectations for recovery times and the amount of data that can be lost to establish predictability and accountability. The most relevant metrics in this regard are:

- **Recovery Time Objective (RTO)** refers to the time it takes to resume operations after a disruption. An RTO signifies the maximum amount of downtime a business can afford as an acceptable risk.
- **Recovery Point Objective (RPO)** refers to the maximum amount of data that a business can afford to lose as an acceptable risk. An RPO determines how often backups are performed.

3. Assess Your Ability to Meet Recovery Objectives

It is not enough to simply define recovery metrics and expect results. The effectiveness of VMware vSphere data protection is a direct function of the IT infrastructure, including storage capacity, network bandwidth, CPU power and IT personnel. As a result, businesses need to clearly understand how much of these resources can be devoted to backup and recovery in normal circumstances, operational recovery scenarios and disaster recovery scenarios.

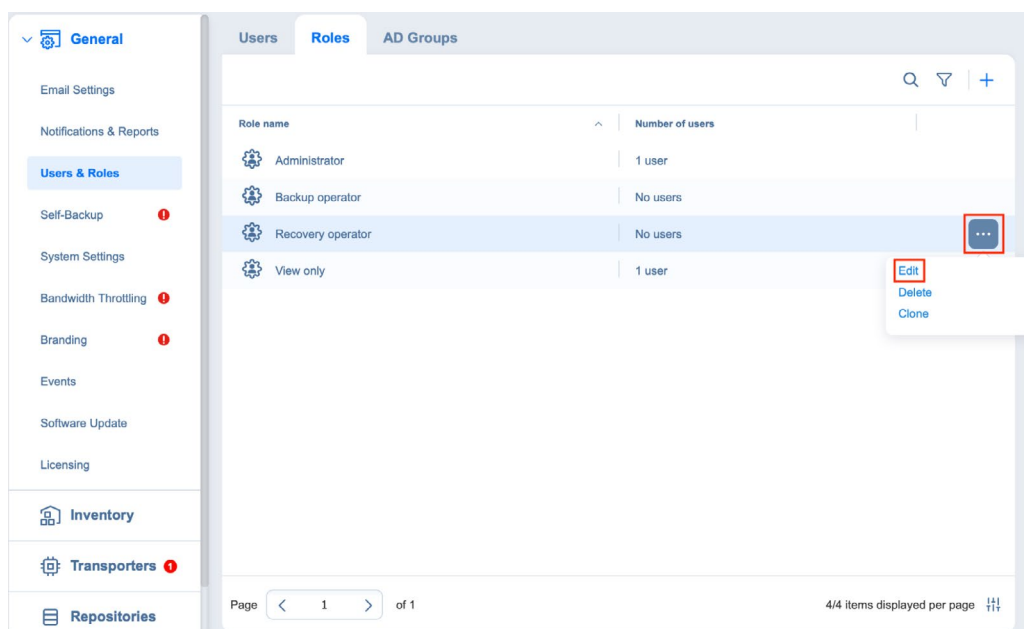
Once you've mapped your infrastructure and capacity limits, you can determine whether it's possible to meet your recovery metrics. If the metrics prove too ambitious, you should recalibrate them to an achievable level. Alternatively, if tight metrics are a strategic priority for the business, you should seek the budgeting and resources necessary to meet the recovery goals.

4. Secure Your Backup Environment

Your entire backup environment is a target for malicious, unauthorized access and activity. To increase security against cybercrime, you need to protect your VMware vSphere backup software as well as the VM backups themselves.

Without having adequate precautions in place, your backup and recovery solution could be used by malicious agents to lock you out of your backups. It's also possible for an insider threat to delete backups by abusing access privileges, leading to potentially catastrophic data loss. With NAKIVO Backup & Replication, you can use the [role-based access control \(RBAC\)](#) feature to block unauthorized access and limit users' access to specific data protection activities. The solution also features [two-factor authentication \(2FA\)](#) to improve security against unauthorized access.

To implement RBAC, click **Settings** in the left pane of the **Dashboard**, go to **General** and click **Users & Roles**. Here, you can add, manage and delete users, as well as assign roles and grant specific user permissions.

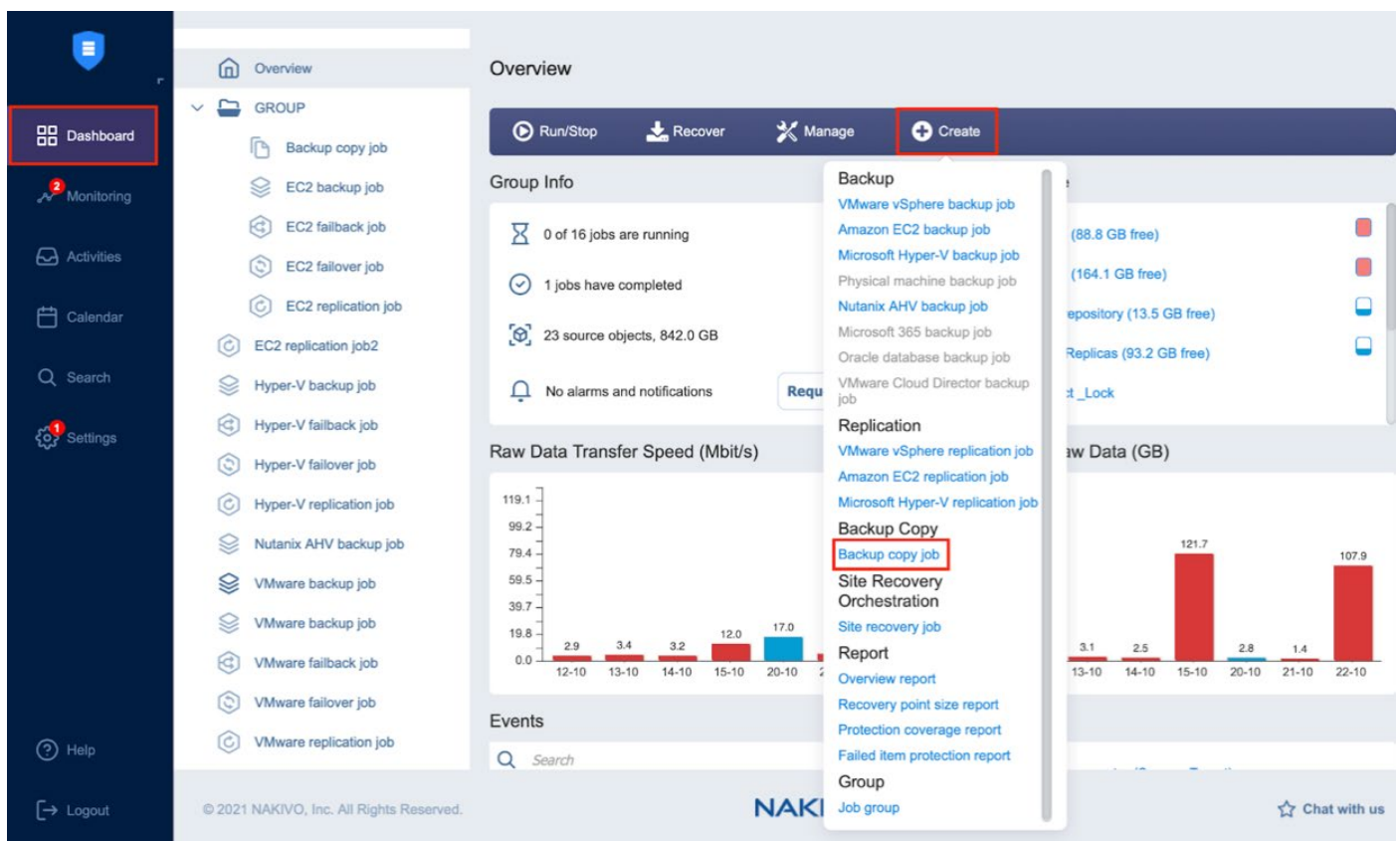


On the same **Users & Roles** page, you can also enable 2FA by selecting a user, clicking **Edit** then checking **Two-factor authentication**. NAKIVO Backup & Replication enables user verification via either **Google Authenticator** or **Email**.

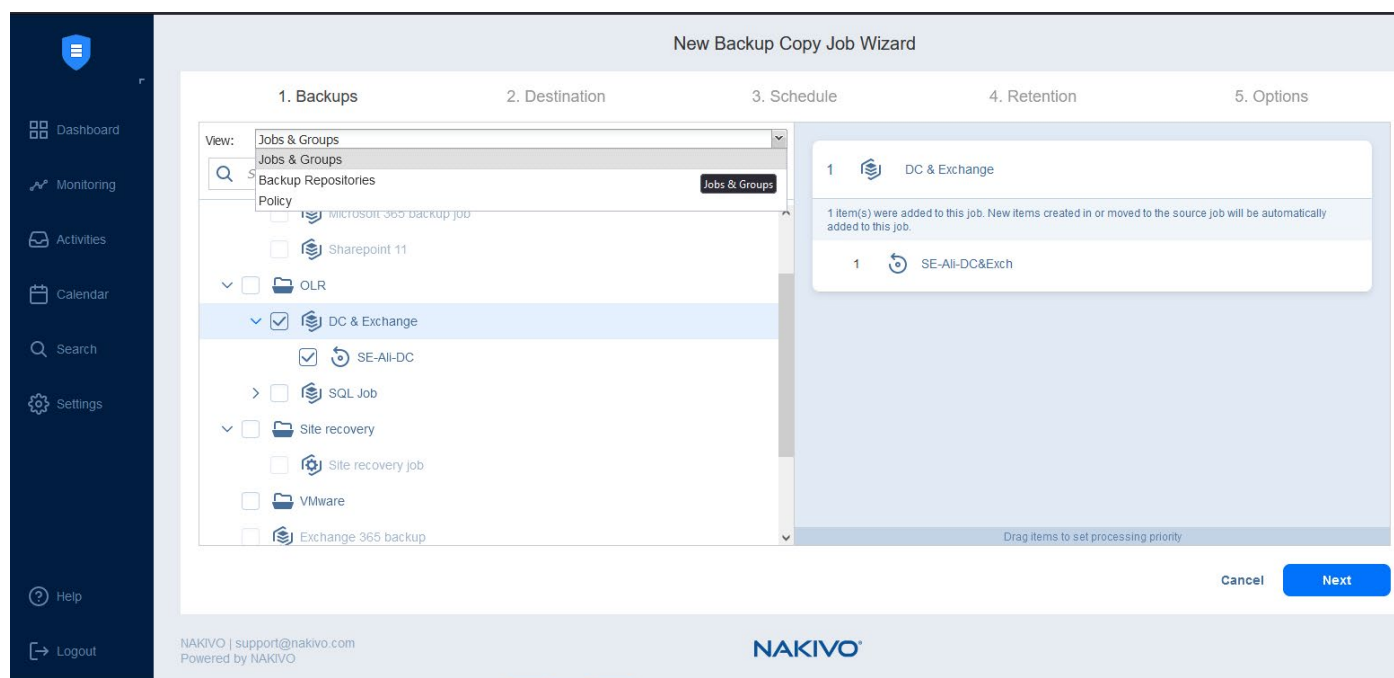
Apart from preventing unauthorized activity, you should create copies of your VMware vSphere backups and store them offsite to ensure that critical data is safe, whatever the scenario.

To prevent bottlenecks, NAKIVO Backup & Replication allows you to create VMware vSphere backup copies directly from existing backups without interfering with source ESXi hosts or VMs. To increase security, you can configure these copies to be sent to a public cloud storage service like Amazon S3 or Wasabi Hot Cloud Storage. In addition to the offsite copy, keep at least one additional backup copy onsite on a different storage media than the original backup (for example, on tape). This strategy is called the 3-2-1 backup rule, and it minimizes the chances of losing all of your backup data during a disruptive event.

To create a backup copy, click **Create** on the **Dashboard** and select **Backup copy job**.



Choose one of the three inventory views from the **Backups** tab of the **New Backup Copy Job Wizard** to create your backup copy job. For example, the **Jobs & Groups** view allows you to create copies of existing backup jobs and groups, whereas the **Policy** view contains policy rule configurations.



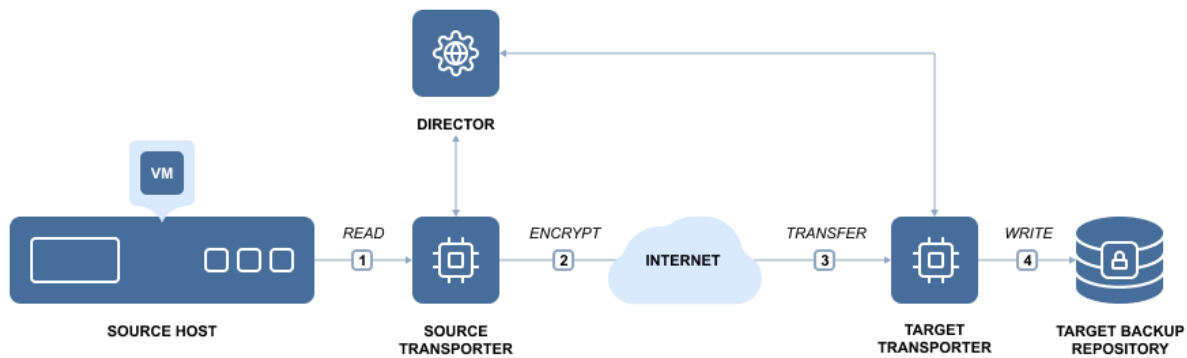
With that said, your backups could still be compromised and encrypted by ransomware even when they're away from your primary site. To prevent such a scenario, immutability technologies make backups immune to modification, deletion and encryption, adding a layer of ransomware resilience. With NAKIVO Backup & Replication, you can make recovery points in cloud-based and local repositories immutable for as long as needed, such that even the root user can't modify or delete them.

To enable immutability, configure the **Make recovery points immutable for X days** option in the **Retention tab** of the **New Backup Job Wizard for VMware vSphere**. You can also apply immutability to additional backup copies from the **Retention tab** of the **New Backup Copy Job Wizard**.

1. Sources	2. Destination	3. Schedule	4. Retention
<p>Retention Settings</p> <p><input checked="" type="checkbox"/> Keep 10 last recovery points</p> <p><input checked="" type="checkbox"/> Keep one recovery point per day for 10 days</p> <p><input checked="" type="checkbox"/> Keep one recovery point per week for 4 weeks</p> <p><input type="checkbox"/> Keep one recovery point per month for 12 months</p> <p><input type="checkbox"/> Keep one recovery point per year for 3 years</p> <p>Learn more</p> <p>Immutability</p> <p><input checked="" type="checkbox"/> Make recovery points immutable for 10 days ?</p>			

For additional security, NAKIVO Backup & Replication features in-flight encryption to transform backup data into unreadable ciphertext via the AES 256 standard during transmission over the internet. You can enable in-flight encryption from the **Options tab** of the **New Backup Job Wizard for VMware vSphere**.

You can also apply at-rest encryption to ensure that backup data remains secure while stored in a local repository. This option is available in the **Options step** of the **Create Backup Repository wizard**.



Phase II. Optimizing the Backup Process

Once you've developed your data protection strategy and secured your VMware vSphere backups, you should start optimizing the backup process itself. As an advanced VMware vSphere backup and recovery solution, NAKIVO Backup & Replication offers numerous backup efficiency features. This white paper focuses on the three most effective optimization functionalities: backup size reduction, application-aware backups and VM verification. These tools allow you to create backups that are:

- Storage-efficient
- Cost-effective
- Transactionally consistent
- Fully recoverable

NAKIVO Backup & Replication also supports backup for VMware vSphere fault-tolerant VMs. vSphere Fault Tolerance is a VMware feature that protects VMs against data loss and downtime by providing live shadow instances of each VMs.

5. Minimize VM Backup Size

The larger the size of backups, the more storage space you will need for them. Cutting backup size lowers your storage requirements and helps optimize existing hardware. This can result in lower capital expenditure (CapEx), reduced costs for cloud storage and lower overall operating expense (OpEx). The most effective ways to minimize backup size are:

- Deduplication
- Compression
- Incremental backup
- Swap data and unused block exclusion
- Log truncation

Deduplication is the process of excluding duplicate data blocks from a backup. VMware vSphere VMs often contain duplicates of data. These can be VMs deployed from the same

template, VMs with the same OS or VMs with identical or semi-identical files (for example, database entries). Block-level data deduplication reduces the backup size by copying only unique data blocks while replacing duplicate blocks with references to existing ones.

NAKIVO Backup & Replication automatically deduplicates all backups stored in the backup repository. This ensures that all data blocks, whatever the source, are accounted for during backup deduplication.

Compression reduces the backup size by recoding backups to consume less space. You can enable deduplication and compression with NAKIVO Backup & Replication by configuring the backup repository settings during the repository creation process. To do so, click **Settings** on the **Dashboard** and go to the **Repository** tab, click **Add Backup Repository**, and select **Create new backup repository**. In the options tab of the Create backup repository page, enable **Data size reduction**.

The screenshot displays the 'Options' tab of the 'Create new backup repository' wizard. The 'Storage Savings & Encryption' section includes a dropdown for 'Data size reduction' (set to 'Enabled') and a checkbox for 'Encryption' (set to 'Disabled'). The 'Reliability & Maintenance' section contains several checkboxes: 'Enable automatic repository self-healing' (checked), 'Run repository self-healing on schedule', 'Run full data verification on schedule', 'Reclaim unused space on schedule', and 'Enforce explicit file system sync'. A 'Data Size Reduction Settings' dialog box is open, showing 'Compression' set to 'Fast' and 'Store backups in separate files (recommended)' unchecked. The 'Scheduled Detach' section has 'Detach this repository on schedule' unchecked. At the bottom right are 'Finish' and 'Cancel' buttons.

Incremental backup works by copying only data blocks that have changed since the last backup. NAKIVO Backup & Replication leverages the VMware Changed Block Tracking (CBT) technology to create incremental backups of VMware vSphere VMs.

Swap data and unused block exclusion and **log truncation** result in additional space savings by cutting unnecessary data out of the backup process.

You can configure all storage space savings settings on a per-job basis in the **Options** tab of the **New Backup Job Wizard for VMware vSphere**. Collectively, these settings allow you to lower storage costs and increase backup speed.

New Backup Job Wizard for VMware vSphere

1. Source	2. Destination	3. Schedule	4. Retention	5. Options
<div style="border: 1px solid red; padding: 5px; margin-bottom: 10px;"> Job Options Job name: VMware backup job App-aware mode: Enabled (proceed on error) settings Change tracking: Use VMware CBT settings Network acceleration: Disabled i Network encryption: Disabled i VM verification: Disabled i Exclude swap files and partitions: Enabled i Exclude unused blocks: Enabled i </div> <div> Full Backup Settings Create full backup: Every i Friday i Full backup mode: Synthetic full i <input type="checkbox"/> If a full backup fails, create a full backup on the next job run i </div>				

6. Create Application-Aware Backups

When backing up VMware vSphere VMs that house applications and databases, it's important to ensure that the backups are application-aware. This type of backup maintains transactional consistency to keep applications and databases (Active Directory, Microsoft Exchange Server, Microsoft SQL Server and Oracle Database) ready for use immediately after recovery. Otherwise, backups may become crash-consistent, missing vital portions of data and transactions.

To create application-aware backups, NAKIVO Backup & Replication freezes application operations and flushes data to disk using native VMware Guest OS Quiescing technology and VMware Tools before taking a snapshot of the source workload.

You can enable app-aware mode in NAKIVO Backup & Replication by selecting **Enabled (proceed on error)** or **Enabled (fail on error)** from the dropdown menu in the **Options** tab of the **New Backup Job Wizard for VMware vSphere**.

New Backup Job Wizard for VMware vSphere

1. Source	2. Destination	3. Schedule	4. Retention	5. Options
<div> Job Options Job name: VMware backup job <div style="border: 1px solid red; padding: 2px;">App-aware mode: Enabled (proceed on error) settings</div> Change tracking: Use VMware CBT settings Network acceleration: Disabled i </div>				

- **Enabled (proceed on error):** With this option selected, NAKIVO Backup & Replication proceeds even if an application quiescing error is encountered.
- **Enabled (fail on error):** With this option selected, NAKIVO Backup & Replication automatically fails the job if an application quiescing error is encountered.
- **Disabled:** Selecting this option disables the app-aware mode.

7. Verify VM Recoverability

The worst time to discover that a VMware vSphere VM backup is not recoverable is after a data loss incident. An effective way to protect yourself from such a scenario is to verify that a VM backup is recoverable after creating it. NAKIVO Backup & Replication offers two methods of [instant verification](#) for VMware vSphere backups: Screenshot Verification and Boot Verification.

With Screenshot Verification, the solution boots the VM from the backup and takes a screenshot of the VM screen. With Boot Verification, the solution starts the VM and checks whether the VMware tools are running properly.

You can set NAKIVO Backup & Replication to automatically verify VM recoverability by selecting your preferred verification method in the **Options** tab of the **New Backup Job Wizard for VMware vSphere**. With either method, you can choose to receive verification results via email or check the results from the web interface.

The screenshot displays the 'New Backup Job Wizard for VMware vSphere' interface. The 'Options' tab is active, showing various configuration options. The 'VM verification' dropdown menu is highlighted with a red box, indicating the selection of 'Screenshot verification'. A 'VM Boot Location' dialog box is open, allowing users to specify the target container, datastore, and proxy transporter. The 'Verification Options' section shows settings for the number of VMs to verify simultaneously (2), the recovery time objective (5 minutes), and the screenshot delay (30 seconds).

Phase III. Maximizing Performance

After formulating a data protection strategy and optimizing the backup process, the next target is to improve the performance and efficiency of your data protection activities. The objectives of this phase are:

- Ensuring fast recoveries and minimal downtime by determining the most suitable type of recovery for each situation
- Lowering administrative overhead by automating data protection activities
- Optimizing resource usage and avoiding recovery gaps by adjusting to changing circumstances

NAKIVO Backup & Replication provides a range of features designed to achieve these objectives. Here's how to use each feature to its full potential.

8. Ensure Efficient VM Recovery

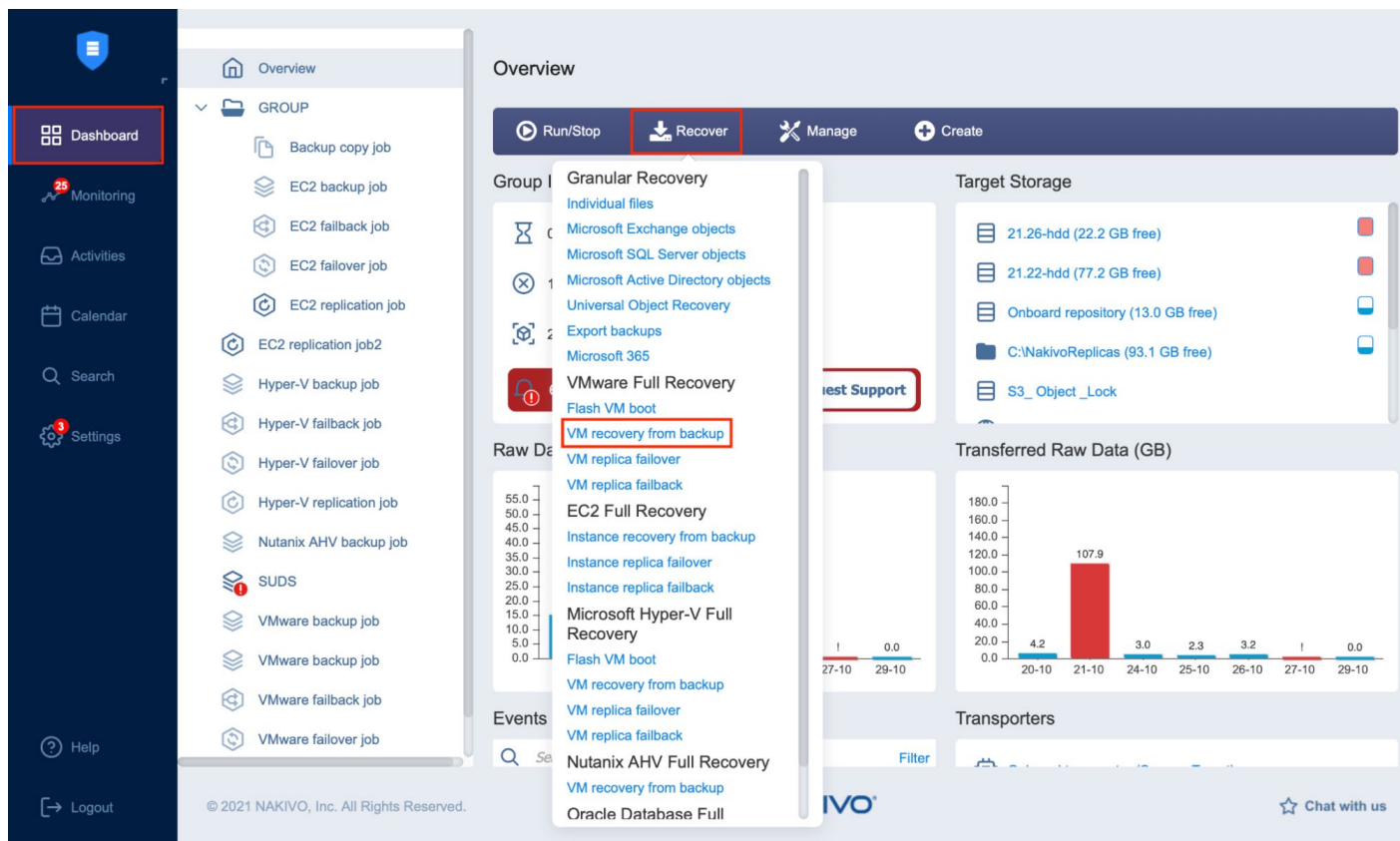
There are multiple methods to recover backup data with NAKIVO Backup & Replication, including full, granular, physical-to-virtual and cross-platform recovery. Understanding the most suitable recovery type for each scenario is key to meeting tight VM recovery objectives.

- **Granular recovery** involves restoring individual files and objects instead of recovering the entire VM in case a specific item has been deleted or lost. Recovering only the needed items saves time and reduces the load on network resources.
- **Flash VM Boot** enables booting a full VMware vSphere VM from a backup in just a few seconds. The feature works by creating a new VM on the target host and exposing the VM disks from the backup repository. Exposed disks are mounted to the new VM as iSCSI targets. This reduces downtime and improves adherence to tight RTOs. Flash VM Boot is useful for testing purposes, as well, since booted VMs can serve as temporary test environments.
- **Full VM recovery** is best used when you need to recover an entire machine. The most common use case for a full VM recovery is avoiding downtime after a VM has failed, become corrupted, or been deleted.
- **Physical-to-virtual (P2V)** recovery refers to restoring full physical machines as a VMware vSphere VM directly from compressed backups. The P2V recovery feature can come in handy for businesses with a hybrid environment of physical machines and VMware vSphere VMs. There are two types of P2V recovery in NAKIVO Backup & Replication: instant and full. While different, both types share the same general purposes:
 - Recovering in the event of a physical machine failure
 - Creating safe environments for testing and development
 - Performing physical-to-virtual migrations

With that said, there is one key difference between instant and full P2V recovery. During an instant P2V recovery, the backup disks are mounted and exposed, making them perfect for quick deployment. On the other hand, full P2V recovery creates VMs ready for long-term use in a production environment.

- **Cross-Platform Recovery** enables you to seamlessly recover VMware vSphere VMs as Microsoft Hyper-V VMs or vice-versa. The feature lets you export VM data from any backup into a standard format (VMDK, VHD or VHDX).

You can perform any of these recovery types by clicking **Recover** on the **Dashboard** and selecting the desired type.



9. Leverage Automation Techniques

Manually performing backups can be time-consuming and pull IT personnel away from other essential tasks. Additionally, any oversight or mistake by IT administrators can undermine data protection efforts. Automating data protection activities saves time and reduces the chances of human error, thereby lowering the organization's risk profile. NAKIVO Backup & Replication enables backup automation through a combination of policy rules, scheduling, job chaining, API integration and custom scripts.

Configuring [job policies](#) allows you to perform backups for entire groups of VMs based on specific parameters, such as name, tag, size, location, RAM amount, network name and power state. If you make a change to a VM, NAKIVO Backup & Replication automatically recognizes the change and includes or excludes the VM from jobs according to your policies.

To create policy rules for a VM backup job, open the **Policy** view in the **Source** tab of the **New Backup Job Wizard for VMware vSphere**. You can create multiple rules for each policy.

1. Source 2. Destination 3. Schedule 4. Retention 5. Options

View: Policy

Include items if ALL rules are matched

☐ Map new VMs to matching backups. ⓘ

Rule #1

Search by: VM name

Which:

Search criteria:

+ Add rules

VM name

VM location

VM Path

Name of VM network

Size of VM

Amount of VM RAM

Number of VM processors

Policy Container

Centos2012

Drag items to set processing priority

Cancel Save Save & Run

Job Scheduling allows you to create backup routines based on a suitable timetable. You can schedule VMware vSphere backups to run daily, weekly, monthly or yearly, or create a custom schedule. Use the **Schedule** tab in the **New Backup Job Wizard for VMware vSphere** to set up job schedules.

New Backup Job Wizard for VMware vSphere

1. Source 2. Destination 3. Schedule 4. Retention 5. Options

☐ Do not schedule, run on demand

(UTC+02:00, EET) Eastern European Time

Schedule #1

Run daily/weekly

Starting at: 0:00 Ending: 6:00

☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat ☐ Sun

All days Work days Weekends

every 1 weeks

☐ Effective from

[Add another schedule](#)

[Show calendar](#)

Next Cancel

[Job Chaining](#) makes it possible to join data protection activities in a single integrated workflow. For example, you can chain a VMware vSphere backup copy job to an existing backup job. This would allow you to send backup copies to different storage media without constant manual intervention. You can chain jobs in NAKIVO Backup & Replication from the **Schedule** tab in the **New Backup Job Wizard for VMware vSphere** using the **Run after another job** option.

New Backup Job Wizard for VMware vSphere

1. Source 2. Destination 3. Schedule 4. Retention 5. Options

☐ Do not schedule, run on demand

(UTC+02:00, EET) Eastern European Time

Schedule #1

Run after another job

After the job: Physical machine backup job

Run this job: Immediately

☒ After successful runs ☐ After failed runs ☐ After stopped runs

☐ Effective from

[Add another schedule](#)

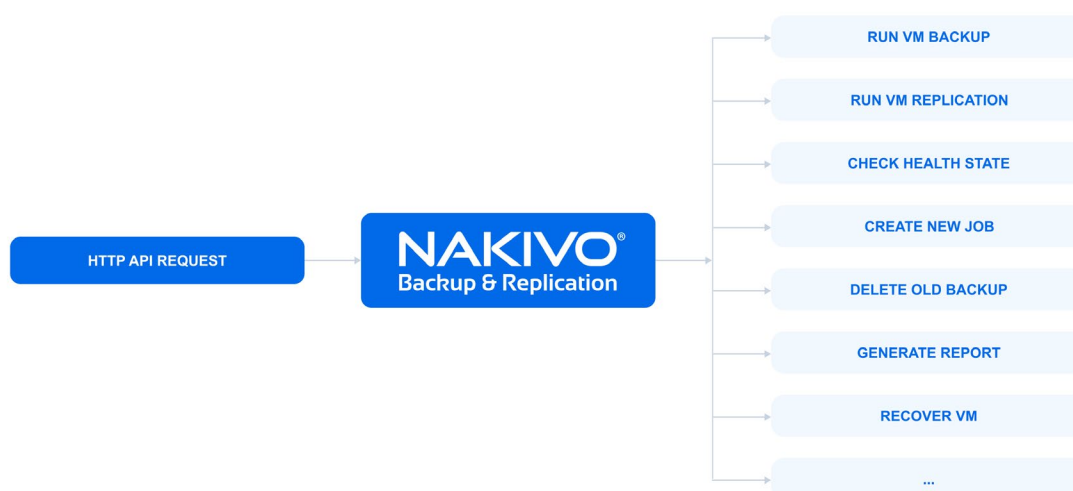
[Show calendar](#)

Next **Cancel**

[Custom scripts](#) also enable you to perform and automate various actions, such as waking servers, mounting volumes and starting services.

To run custom scripts in NAKIVO Backup & Replication, use **Run local pre job script** and **Run local post job script** under **Pre and Post Actions** in the **Options** tab of the **New Backup Job Wizard for VMware vSphere**.

Finally, you can integrate NAKIVO Backup & Replication with different third-party solutions using the [API Integration Kit](#). This feature can be used to improve automation, management and monitoring of data protection activities via the JSON-RPC-based HTTP API feature.

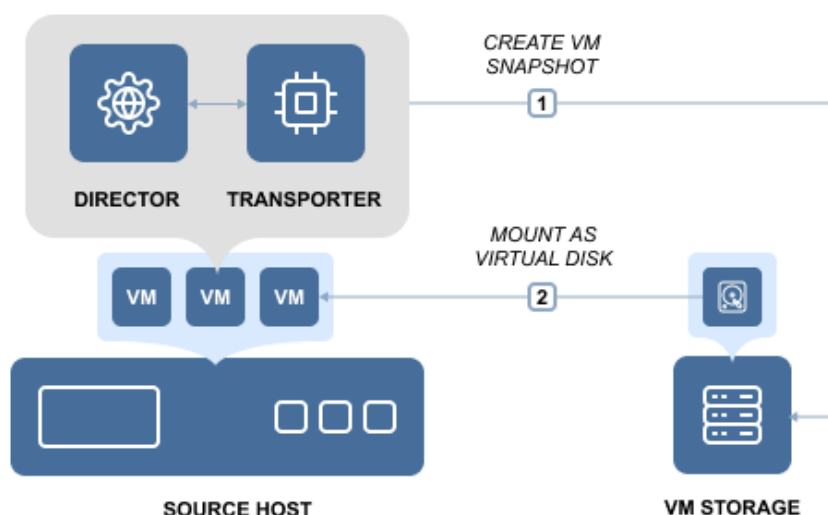


10. Adjust to Changing Circumstances

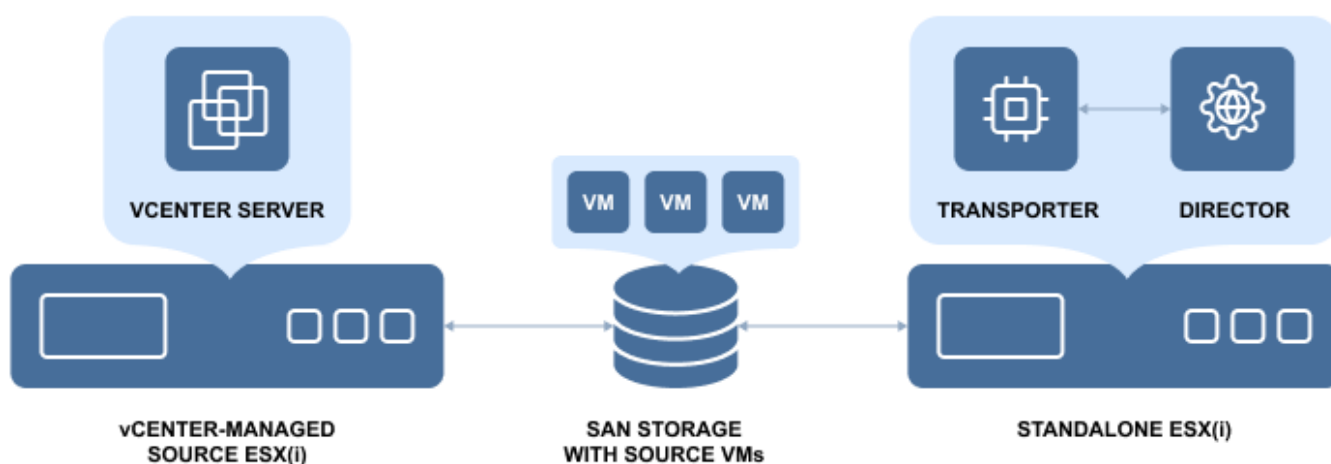
Just because your backup strategy and practices are acceptable today doesn't necessarily mean that they will be as effective next month. Efficient backup administration requires that you stay ahead of potential disruptions by proactively addressing changes at both the micro- and macro-levels.

At the micro-level, you can use various tools to regulate network bandwidth availability and boost backup speed. NAKIVO Backup & Replication automatically uses a LAN-free data transfer mode for VMware vSphere backup and replication jobs via the HotAdd and Direct SAN Access features.

HotAdd allows NAKIVO Backup & Replication to bypass the host's TCP/IP stack, improving VM backup and replication speed and reducing the network load.



Direct SAN access significantly increases backup and replication speed while decreasing the load on your production network. It can also be of use when the VMware vSphere VM is located on a Fibre Channel or storage area network (SAN).



You can apply HotAdd or direct SAN access in the **Options** tab of the **New Backup Job Wizard for VMware vSphere**. Simply click the dropdown menu for **Transport Mode** and select your preferred mode.

New Backup Job Wizard for VMware vSphere

1. Source	2. Destination	3. Schedule	4. Retention	5. Options
<div> <div>Job Options</div> <div> <div>Job name:</div> <div>VMware backup job</div> </div> <div> <div>App-aware mode:</div> <div>Enabled (proceed on error)</div> <div>?</div> <div>settings</div> </div> <div> <div>Change tracking:</div> <div>Use VMware CBT</div> <div>?</div> <div>settings</div> </div> <div> <div>Network acceleration:</div> <div>Disabled</div> <div>?</div> </div> <div> <div>Encryption:</div> <div>Disabled</div> <div>?</div> </div> <div> <div>VM verification:</div> <div>Disabled</div> <div>?</div> </div> <div> <div>Skip swap files and partitions:</div> <div>Enabled</div> <div>?</div> </div> <div> <div>Skip unused blocks:</div> <div>Enabled</div> <div>?</div> </div> </div>				
<div> <div>Full Backup Settings</div> <div> <div>Create full backup:</div> <div>Job runs #</div> <div>5</div> </div> <div> <div>Full backup mode:</div> <div>Synthetic full</div> <div>?</div> </div> </div>				
<div> <div>Pre and Post Actions</div> <div> <div><input checked="" type="checkbox"/> Send job run reports to</div> <div>administrator@nakivo.com</div> <div>?</div> </div> <div> <div><input type="checkbox"/> Truncate Exchange logs</div> <div>On successful VM processing only</div> <div>?</div> </div> <div> <div><input type="checkbox"/> Truncate SQL Server logs</div> <div>On successful VM processing only</div> <div>?</div> </div> <div> <div><input type="checkbox"/> Run local pre job script</div> <div>?</div> </div> <div> <div><input type="checkbox"/> Run local post job script</div> <div>?</div> </div> </div>				
<div> <div>Data Transfer</div> <div> <div>Transport mode:</div> <div>Automatic selection</div> <div>?</div> </div> <div> <div>Transporters:</div> <div>Automatic selection</div> <div>?</div> </div> <div> <div><input type="checkbox"/> Limit transporter load to</div> <div>3</div> <div>concurrent tasks</div> <div>?</div> </div> <div> <div>Bandwidth throttling:</div> <div>Disabled</div> <div>?</div> </div> </div>				

Backup jobs require creating VM snapshots, thus consuming resources and time, especially in large infrastructures. Constantly making VM snapshots can have a detrimental impact on your production environment. To address this issue, NAKIVO Backup & Replication allows you to create backups of VMware vSphere VMs hosted on HPE 3PAR and Nimble Storage devices directly from storage snapshots instead of VM snapshots.

To do so, add VMs whose disks are residing on the supported storage device, then enable **Backup from storage snapshot** in the **Options** tab of the **New Backup Job Wizard for VMware vSphere**. Make sure that you've added your HPE 3PAR or Nimble Storage device to the **Inventory** beforehand.

Data Transfer

Transport mode: Automatic selection ⓘ

☐ Transporter pool: Select transporter pool ⓘ

Transporters: Automatic selection ⓘ

☐ Limit transporter load to: 3 concurrent tasks ⓘ

Bandwidth throttling: Disabled ⓘ

☐ Bottleneck detection ⓘ

Backup from storage snapshot: Disabled ⓘ

Cancel Finish Finish & Run

The [Network Acceleration](#) feature further shortens backup windows and reduces network load when performing backups over WAN or in busy LAN environments. Network Acceleration is enabled in the **Options** tab of the **New Backup Job Wizard for VMware vSphere**.

New Backup Job Wizard for VMware vSphere

1. Source 2. Destination 3. Schedule 4. Retention 5. Options

Job Options

Job name: VMware backup job

App-aware mode: Enabled (proceed on error) ⓘ settings

Change tracking: Use VMware CBT ⓘ settings

Network acceleration: Disabled ⓘ

Network encryption: Disabled ⓘ

Furthermore, with [Advanced Bandwidth Throttling](#), you can limit how much bandwidth your backup jobs use. This enables you to run backups during office hours without affecting core business operations and regulate bandwidth usage according to changing needs.

To use **Advanced Bandwidth Throttling**, click **Settings** in the left pane of the main dashboard and select **Bandwidth Throttling** in the **General** tab. You can throttle all your jobs with a **Global** rule or only a specific job with a **Per Job** rule.

Create Bandwidth Rule

Type Settings

Name: New

Throttle bandwidth to: 10 Mbit/s ⓘ
Equals 1.25 MB/s or 14 minutes to transfer 1GB of data

Rule schedule: Active on schedule ⓘ

Starting at: < 2 > : < 2 >

☒ Ending at: < 6 > : < 7 >

Days: MO TU **WE** TH FR SA SU

Every: 1 weeks

Time Zone: (UTC+02:00, EET) Eastern European ...

Previous Cancel Finish

Once you've created a throttling rule, you can apply it to a specific job at the bottom of the **Options** of the **New Backup Job Wizard for VMware vSphere**.

Data Transfer

Transport mode: Automatic selection ⓘ

☐ Transporter pool: Select transporter pool ⓘ

Transporters: Automatic selection ⓘ

☐ Limit transporter load to: 3 concurrent tasks ⓘ

Bandwidth throttling: Disabled ⓘ

☐ Bottleneck detection ⓘ

Backup from storage snapshot: Disabled ⓘ

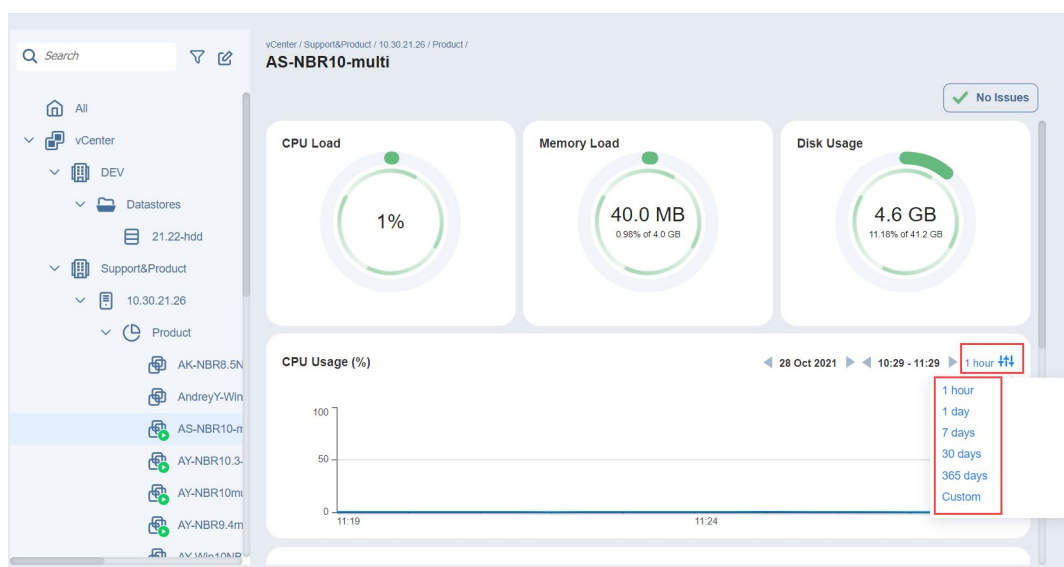
Cancel Finish Finish & Run

At the macro level, you need to regularly verify that your data protection activities continue to protect your environment by auditing your practices. One way to do this is to perform regular test recoveries to ensure that you can meet previously set RTOs and RPOs. During these tests, simulate different scenarios with varying levels of available network bandwidth and CPU resources.

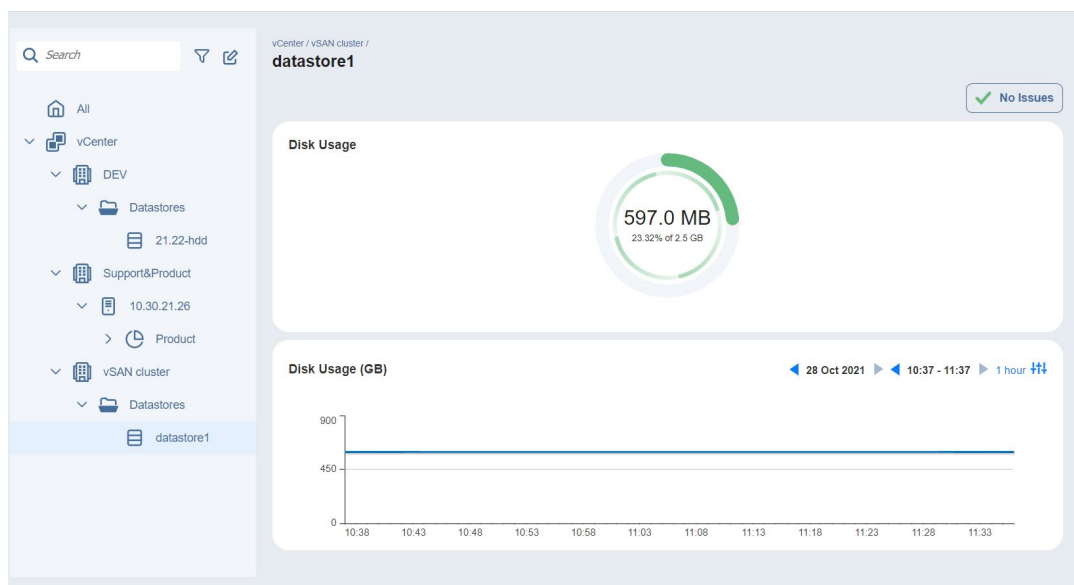
Bonus Tip: Monitor Your VMware vSphere Infrastructure

Keeping an eye on the inner workings of your VMware vSphere environment is another vital best practice that can help you take complete control of your environment. Monitoring key metrics and virtualization resources leads to more effective performance optimization decisions.

By tracking the performance of virtual environments historically and in real-time, [NAKIVO's IT Monitoring for VMware vSphere](#) allows you to detect anomalies early and minimize disruptions to business operations. The solution also helps implement efficient resource distribution within your VMware vSphere infrastructure, providing full visibility into CPU, RAM, and disk usage of VMware vSphere VMs and VMware vSphere hosts and datastores.



NAKIVO's IT Monitoring for VMware vSphere collects data every minute and presents performance metrics in easy-to-consume pie and line charts for better visualization. Using the included search feature, you can easily find inventory items, filter results, and choose what items you would like to include in your monitoring routine. The solution's ease of use is typified by the availability of all monitoring activities behind a single pane of glass within the NAKIVO Backup & Replication user-friendly web interface. The interface allows you to choose a specific time frame to display historical CPU, memory, and disk usage charts, ranging from 1 hour to 1 year.











Conclusion

Common disruptions such as hardware failures, natural disasters, malware attacks and human error can cost an unprepared business valuable data. By combining VMware vSphere with NAKIVO Backup & Replication, you can mitigate the financial, operational and reputational costs of data loss without high IT costs. NAKIVO Backup & Replication offers all the tools you need to ensure recoverability and simplicity right out of the box. To take your data protection efforts to the next level, make the best use of these best practices for VMware vSphere backup to improve efficiency and minimize setbacks.

NAKIVO Backup & Replication at a Glance

NAKIVO Backup & Replication is a reliable data protection solution for all workloads. The solution offers backup, replication, instant granular recovery, ransomware protection, and IT monitoring from a single pane of glass.

-  **All-in-One Data Protection**
Protect VMware vSphere, Microsoft Hyper-V, Nutanix AHV, Amazon EC2, NAS, Windows, Linux, Microsoft Office 365 and Oracle Database environments.
-  **Ransomware Protection**
Immutable backups protected from deletion and encryption by ransomware in Amazon S3 and Linux-based repositories; air-gapping with offline storage and tape.
-  **Flexible Installation Options**
Install on Linux, Windows and NAS (such as Synology and QNAP), or deploy as a VMware vSphere VA, Nutanix AHV VA or Amazon Machine Image with a few clicks.
-  **Backup Data Tiering**
Backups and backup copies on onsite storage, CFS/NIFS shares, offsite, in the cloud (Amazon S3, Wasabi) and on tape.
-  **IT Monitoring**
Get complete visibility through pie and line charts to visualize the virtual environment's performance and health metrics.
-  **Simple Administration**
Features enterprise-grade functionality behind a user-friendly web interface for businesses of all industries and sizes.
-  **Excellent Support**
Get free demos and deployment sessions for you and your clients to get you started with NAKIVO Backup & Replication. 24/7 tech support when needed to ensure the strictest SLAs.
-  **Competitive Pricing Model**
Offers flexible pricing models that let customers pay only for what they need and easily scale up to accommodate their growing infrastructure.

About NAKIVO

NAKIVO is a US-based corporation dedicated to delivering the ultimate backup, ransomware protection and disaster recovery solution for virtual, physical, cloud and SaaS environments. As one of the fastest-growing backup and ransomware recovery software vendors in the industry, NAKIVO boasts 24 consecutive quarters of double-digit growth, 5-star online community reviews, 98% customer satisfaction with support and a network of over 7,000 partners worldwide. Over 22,000 customers in 171 countries trust NAKIVO with protecting their data, including major companies like Coca-Cola, Honda, Siemens and Cisco.