Petri
IT Knowledgebase

Technical Brief

VMware Backup: Best Practices and Strategies

Presented by: **Michael Otey**, President, TECA, and **Michael Cade**, Technical Evangelist, Veeam

Sponsored by Veeam

OVERVIEW

As data volumes have grown, businesses recognize that their information is an asset. Data loss avoidance and high-speed recovery of data are high priorities. To ensure business continuity, IT teams must focus on implementing robust backup and restore processes for all data, including information stored on virtual machines.

For organizations using VMware, Veeam offers flexible solutions for handling disaster recovery and meeting service-level agreements.

CONTEXT

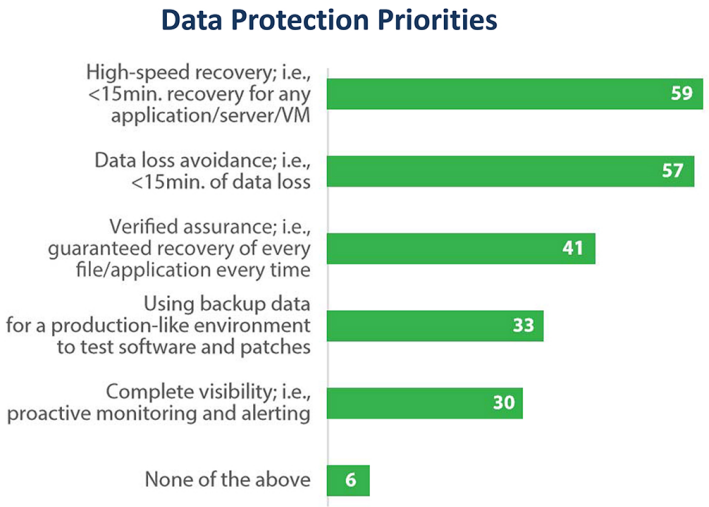
Michael Otey described backup best practices that help ensure business continuity. Michael Cade discussed how Veeam's flexible architecture meets organizations' backup and restore needs.

KEY TAKEAWAYS

Data is a strategic asset and data protection is more important than ever.

As data has become a critical resource, data protection is now IT administrators' most important job. Data is growing between 30% and 50% per year, while new threats like ransomware are becoming more prevalent.

The ability to restore data with minimal downtime is critical. At the same time, technologies like virtualization and the cloud have changed data protection requirements and strategies. A recent survey by Veeam found that high-speed recovery and data loss avoidance are top priorities for businesses.



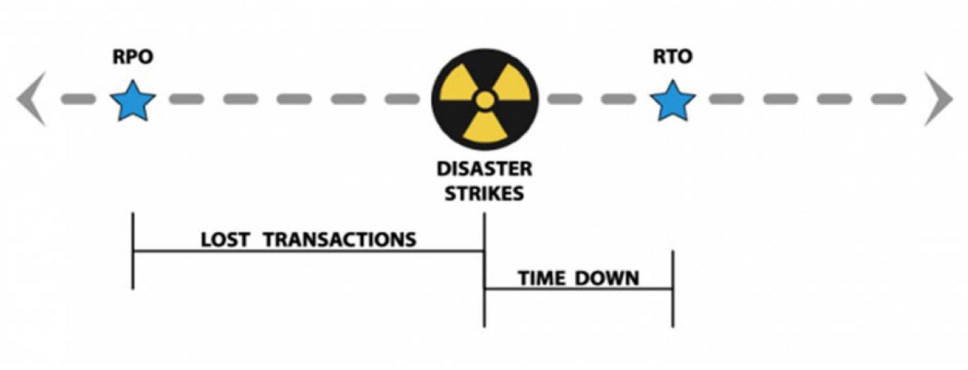
A data protection best practice is the 3-2-1 rule:

- 3 copies of data should be maintained. This includes the original data in the virtual machine, plus two copies.
- 2 backups should be kept on different types of media.
- 1 backup should be stored offsite or in the cloud.

Backups and restores are essential for data protection, but they aren't without problems.

Common backup challenges include:

- **Meeting recovery objectives.** As companies consider backup strategies, they must take into account Restore Time Objectives (RTOs) and Restore Point Objectives (RPOs). RTOs define the required time for a data restore, while RPOs relate to the ability to recover data to a particular point in time.



- **Host vs. guest backups.** As a rule, guest backups should be avoided since multiple backups run simultaneously out of the VMs. Host backups are a better alternative, since they generate one backup for all operating systems and are image based. They are higher performance than guest backups and use fewer system resources.
- **The backup window.** Most businesses avoid running backups during production hours. As storage types change and server sprawl occurs, backup windows are becoming larger.
- **Cloud integration.** Although cloud storage options are inexpensive and eliminate the need for tape, they are higher latency than local backup processes. This can affect RTOs and RPOs. Organizations may need to adjust their SLAs and backup window times.
- **Verifying backup integrity.** Media corruption is the leading cause of restore failures. vSphere Data Protection restores VMs and does automated backup verification. Other third-party tools can also perform automatic backup verification.

> Restore operations are more important than backups. It's great to do backups, but if you can't restore them, it's a real problem. You don't want to be the one stuck in that situation.
>
> *Michael Otey, TECA*

Backup best practices can ensure business continuity.

Eight data protection best practices are:

1. **Be sure VMTools are installed.** Use Volume Shadow Copy Service-aware backups, quiesce the host, and make data-consistent backups for applications.
2. **Take advantage of compression, deduplication, and encryption.** These technologies increase backup security and shorten backup windows.
3. **Use vSphere tags and policies to backup related VMs together.** Tags and policies enable users to categorize backups, so like systems can be backed up together.

4. **Take advantage of Change Block Tracking.** This backs up only data that has changed and helps with faster backup times.
5. **Look into support for granular recovery.** Most restore requests are for individual files.
6. **Take advantage of storage snapshots, if they're supported.** This creates multiple restore points.
7. **Train IT.** Teams can't minimize downtime if they don't understand the tools available to them.
8. **Document backup and restore processes.** Create standards, documentation, and runbooks.

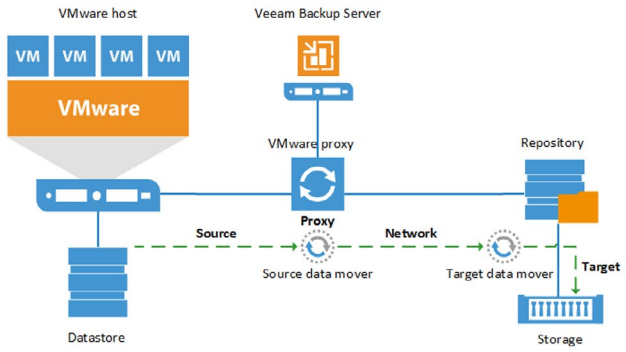
Veeam's flexible architecture meets organizations' backup and restore needs.

Michael Cade discussed the Veeam architecture and reviewed different system components:

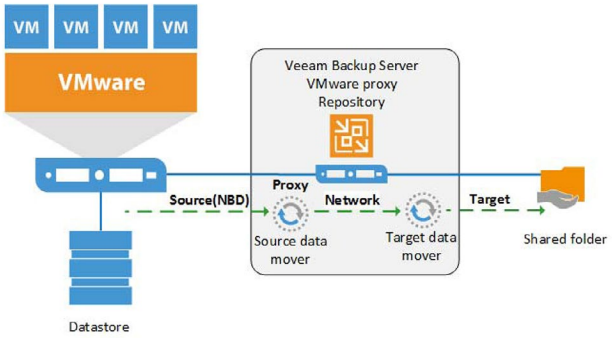
- **Veeam can be scaled out or self-contained.** Veeam's mandatory components include the Veeam Backup Server, the Backup Proxy, and Backup Repository. Veeam can be deployed either physically or virtually.

> A common myth is that Veeam doesn't scale, but that's absolutely untrue. The system can be scaled to handle all sizes of workloads.
>
> *Michael Cade, Veeam*

Components: 18,000 foot view



Components: Optionally All-In-1



Veeam Backup Server

- **Remember to keep it up to date and allocate memory appropriately.** In addition, it is important to allocate enough RAM for job manager processes.
- **Manage backups with a local backup server.** This enables fast system restores in disaster recovery (DR) situations.
- **Manage replication with a backup server in the DR site.** This supports failover with one click, even when the production site is down.

Proxies

- **Deploy more than one proxy for redundancy.** In addition, multiple proxies offer better throughput and smaller backup windows.
- **Keep proxies under control.** Veeam Enterprise and Enterprise Plus Editions support Backup I/O Control to throttle workloads. With Veeam Standard Edition, users can throttle proxies at the repository.

Proxy Server

- **To reduce operating system licensing costs, client Windows editions are supported.** This is helpful for small and medium-sized businesses.
- **Keep the CPU's default compression level at "Optimal."** Veeam's Advanced Data Fetcher doubles the CPU load per task slot.

Transport Modes

- **Select from five different transport modes based on your needs.** Options include Direct Storage Access (SAN or NFS), Virtual Appliance (Hot-Add), and Network (NBD/NBDSSL). The Advanced Data Fetcher is not available with Direct SAN or NBD.

	Direct SAN	SAN+BFSS	Direct NFS	Hot Add	NBD
Adv. data fetcher	no	yes	yes	yes	no
Performance	fast	fastest	fastest	fastest	slow
Impact	low	lowest	lowest	high	high
Reliability	ok	best	best	worst	best
Supportability	ok	best	best	ok	ok

Veeam Backup Repository

- **Three backup storage tiers are available.** These are primary, secondary, and archive.

	Primary	Secondary	Archive (v10)
Cost per TB	High cost	Low cost	Lowest cost
Storage capacity	Low capacity	High capacity	Incredible capacity
IOPS capacity	High	Average	Ridiculously low
Reliability	Standard	Worse	Best
Restore costs	Lowest	Average	Worst

Veeam supports next-generation storage like VVols and vSAN.

Veeam is designed to interact with next-generation storage:

- **With VVols and vSAN, the Storage Policy-Based Management (SPBM) association is critical when it comes to backup and restore.** Veeam Quick Migration can be used to migrate to vSAN and VVol storage resources. This should be considered when developing a migration plan.
- **vSphere tags can be used for Veeam backup and replication jobs.** vSphere tags are a great way to automate the VMs that are added to Veeam backup and replication jobs. SPBM policies assigned to a VM will also be recovered.
- **VVol support came with complete vSphere 6 support in Veeam Availability Suite v8.** VVol backups follow much of the same workflow as regular VM backups, except their path is more VVol aware.

- **Veeam provides Smart Logic for vSAN.** Smart Logic gathers data distribution from vCenter and determines where most VM data resides. The result is more efficient use of proxies and resources.
- **Different options exist for restore within Veeam.** These include Instant VM Recovery and Quick Rollback. Many other specific options exist for infrastructure restores. Veeam Explorers are provided for SQL Server, Exchange, Active Directory, Oracle, and SharePoint. It is important to ensure that the restore process correctly matches the SPBM association.