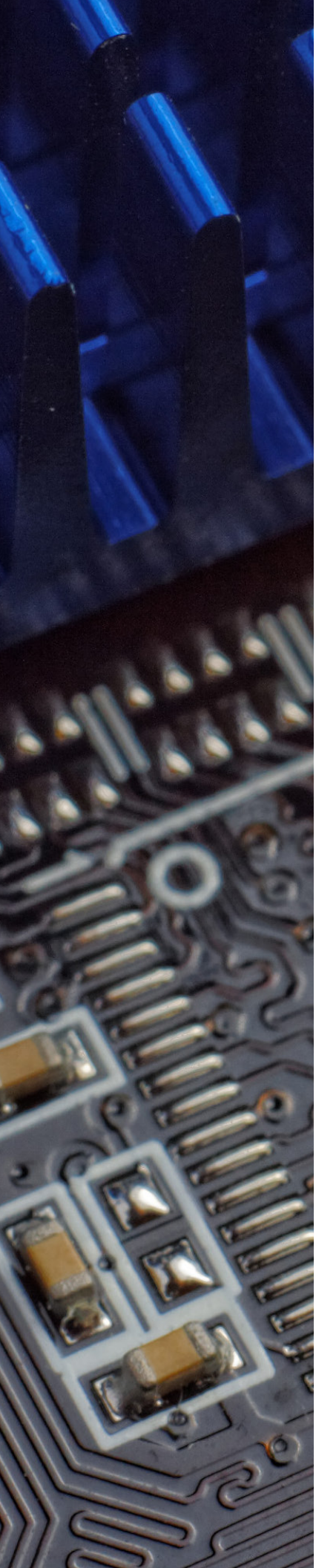


Petri Webinar Brief
February 28th, 2018

TOP 10 BEST AND WORST BACKUP PRACTICES

Presenter:
Noah Gamache,
Systems Engineer
Veeam Software

Moderator:
Brad Sams,
Executive Editor at Petri.com
Petri IT Knowledgebase

Petri IT Knowledgebase
A BWW Media Group Brand

SPONSORED BY VEEAM

Overview

When data disaster strikes, will your company be prepared? You can fully recover in the event of a disaster if you regularly back up your data but only if it's properly backed-up. Veeam technical expert Noah Gamache shares his experience and discusses best and worst backup practices in this webinar. Save time and money, and all of your data with these best and worst practices that are currently utilized across the industry.

Key Takeaways

In this section, the 10 best practices are outlined to help prevent the next outage from occurring or if it does occur, to help you recover faster.

1. **Understanding the Iron Triangle**

   a. When it comes to making intelligent choices about how to protect your environment, it is important to understand the impact from removing one component from the iron triangle. Each choice has a trade-off and this graphic will help you understand the impact of your decision.

   b.

2. Understand the Environment

a. Having a topographical understanding of your entire environment is critical to making sure that all aspects of your environment are being successfully replicated. This map should include all of the following items:

i. Hosts
ii. Physical Workloads
iii. Cloud Instances
iv. Virtual Machines
v. Storage devices
vi. Network
vii. Applications
viii. Change Rate

b. This map will help you identify any weaknesses in your environment and help you to develop a plan of preparation.

c. Using Veeam tools, Veeam One can help you with the following:

i. Before Install
    1. VM Configuration Assessment
    2. VM Change Rate Estimation
ii. After Install
    1. Monitor Capacity (Repo Space, Datastore)
    2. Early Warning (Snapshots)

3. Agreement

a. It is important to understand what business requirements and contracts are in place so that your outage has a minimal impact on your operation.

i. Service Level Agreements (SLAs)
ii. Recovery Point Objectives (RPOs)
iii. Recovery Time Objectives (RTOs)
iv. Group Workloads into Categories

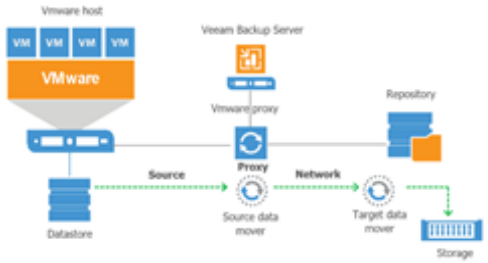
4. Planning

a. No matter the size of the software or hardware, you need to architect all alternative solutions ahead of an outage.

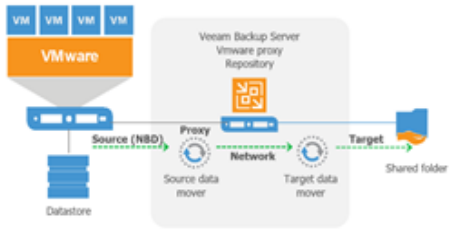
b. When it comes to planning, there are many free resources available from Veeam and other reputable sources:

i. RPS
ii. BP Guide
iii. WhitePapers
iv. Social Media

Components: 18,000 foot view



Components: Optionally All-In-1



5. Management

a. When deciding to update, replace, develop a backup strategy, or build-out a new data center, you need to decide if you are going to go physical or virtual with each having their own unique benefits – specifically for disaster recovery, some of the benefits are listed below:

i. Why go physical?
    1. Best practice for a DR solution: a DR system must not rely on the system it protects (and recovers) in any way
    2. Protect configuration database! Use built-in configuration backup, or Veeam Agent for Windows for the entire server
ii. Why go virtual?
    1. Gets you closer to having 100% virtual data center
    2. Simpler protection--make Veeam backup/replicate itself
    3. Think through and test your DR plan thoroughly

b. Your backup server also needs to be proper provisioned as well with Noah recommending the following settings:

i. Disable default proxy and repository unless beefy all-in-one backup appliance (don't make the brain dig pits)
ii. Allocate enough RAM for job manager processes (separate process per each concurrent job), 500MB
iii. Keep in mind memory requirements for any other Veeam roles present (and add them ALL up)
iv. Keep your backup server up to date!

c. And you need to manage your backup server placement as well:

i. Manage backups with local backup server
    1. Performance (slow vCenter interaction over WAN)

2. No major RTO impact in a DR situation (backup has inherently higher RTOs)

ii. Manage replicas with backup server in DR site

1. Failover with 1 click even when the production site is down
2. Virtual all-in-one backup server provides more options – you can replicate it to DR site just like any other VMs

6. Proxies

a. Managing your proxies is an important step in your backup process as it helps you maintain redundancy, but you also need to keep them moderated as well.

i. Why use more than one proxy?

1. Redundancy
2. Smaller backup window through better throughout
3. Hot add restores (one proxy per cluster)

ii. Keep them under control

1. Backup I/O Control is highly recommended
2. Standard Edition users can throttle at repository instead
3. Keep in mind Advanced Data Fetcher in 9.5 (recommend reducing the number of task slots per proxy by 50%)

7. Repository

a. Defining your backup schedule is based on the size, complexity, and frequency your data changes.

	Primary	Secondary	Archive
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

b. Best Raw Disk Repositories:

i. Any Windows or Linux server, physical or virtual usually backup server itself or backup proxy

ii. Physical server storage options:

1. Local storage
2. DAS (JBOD)
3. SAN LUN

iii. Virtual server storage options:

1. iSCSI LUN connected via in-guest iSCSI
2. Physical RDM disk
3. NOT VMDK

iv. Raw Disk Repositories to Avoid

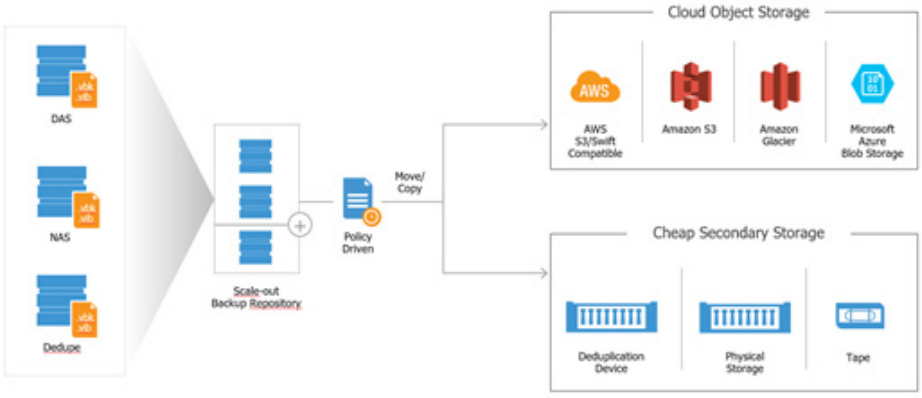
1. Low-end NAS and appliances – reliability
   a. Stuck with it? Use iSCSI instead of file protocols.
2. VMDK on VMFS – recoverability
   a. Dependent on vSphere being operational for recovery
3. SMB (CIFS) network shares – reliability and performance
   a. #1 source of corrupted backups in support
   b. SMB client/server issues
   c. Bad network hardware (and no traffic validation possible)
   d. If share is backed by a file server, add actual server instead

c. Best secondary storage

i. Long-term retention requires:

1. Full backup storage efficiency
   a. ReFS 3.1 (prevents duplication)
   b. Deduplicating storage appliances
2. Windows Server 2016 with deduplication enabled
3. Archive reliability
   a. ReFS 3.1 on Storage Spaces can't be beaten at the low end

d. Archive Tier



8. Other Component Considerations

a. Enterprise Manager – Self Service, Delegated Control, Distributed Veeam environment.

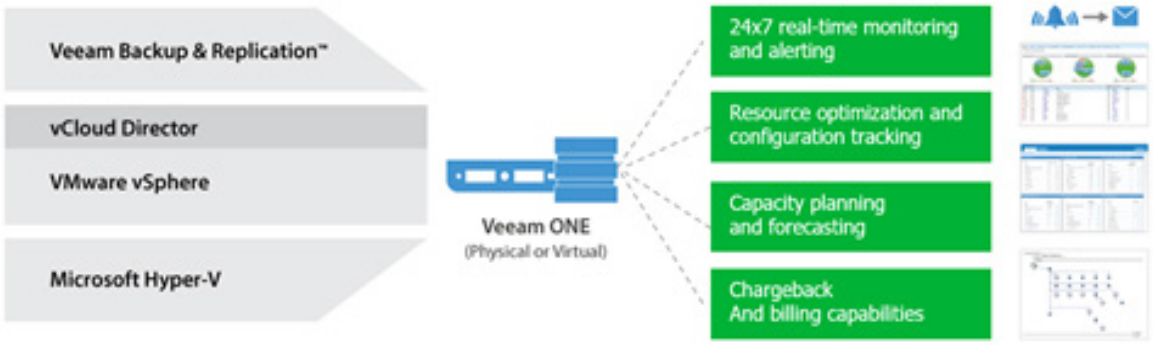
b. Tape – Air-Gapped, Off-site Location, Can be cheap

c. Cloud Connect – Off-site Location, Operational Expense Model

d. WAN Accelerator – Poor Links, High Change Rates

9. Monitoring and Reporting

a. When it comes to reporting and monitoring your environment, especially during and outage, or recovering from an outage, you need visibility into the entire environment and Veeam One can help with this insight.



10. Automation & Verification

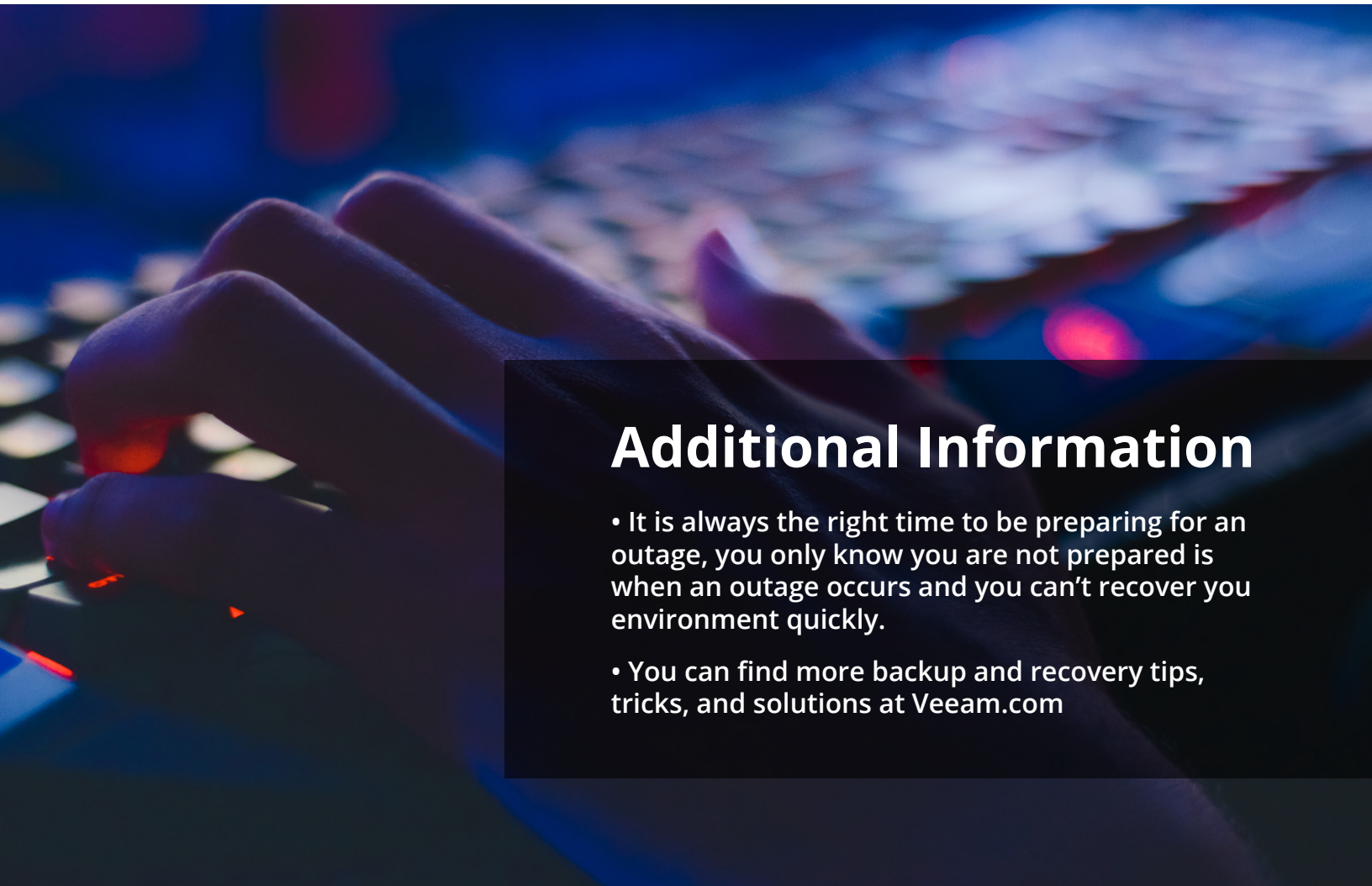
a. The recovery process is typically thought of as a manual process to verify ever put back into production. But, time spent investing in automating the verification process can save time and effort which results in a shorter downtime.

b. Rather than cutting corners find a way to automate.

i. Automate your VMs being added to a backup job by using vSphere Tags
ii. SPBM policies assigned to a VM will also be recovered
iii. The ability to automate the spinning up, the powering on, running tests against the VM, App & OS, powering down and sending the admin a report.

c. Bad Practices:

i. 100% virtual environment, could be many things have you checked the virtual network adapters. VMXNET3 FTW!
ii. Not finalizing Instant VM Recovery – this is going to break things not to mention be as slow as the repo storage.
iii. Storage Integration available, but Proxies not configured so failing back to Network.



Additional Information

- It is always the right time to be preparing for an outage, you only know you are not prepared is when an outage occurs and you can't recover you environment quickly.
- You can find more backup and recovery tips, tricks, and solutions at Veeam.com

SPONSORED BY

VEEAM