VEEAMON 2023

Protecting Your Data: More Than Just VM Backups

Billy Cashwell

Principal,
Product Marketing Manager

Matt Crape

Senior Technical Product Marketer

Veeam® Data Platform

Proven Recovery Orchestration

Proactive Monitoring and Analytics

Secure Backup and Fast Recovery

Native APIs

TARGETED OFFERINGS

- Microsoft 365
- Salesforce
- Kubernetes

On Premises • In the Cloud • XaaS

Over 15 years of ongoing innovation

Over

1,000,000

ACTIVE installations

Agenda

- Mind the protection gap
- Oracle, SQL, SAP - oh my!
- When things are cloudy, recovery should be clear
- Let’s get physical
- Structure your unstructured data
- Recovery at the speed of instant
- Q&A

Does your organization have a ‘reality gap’

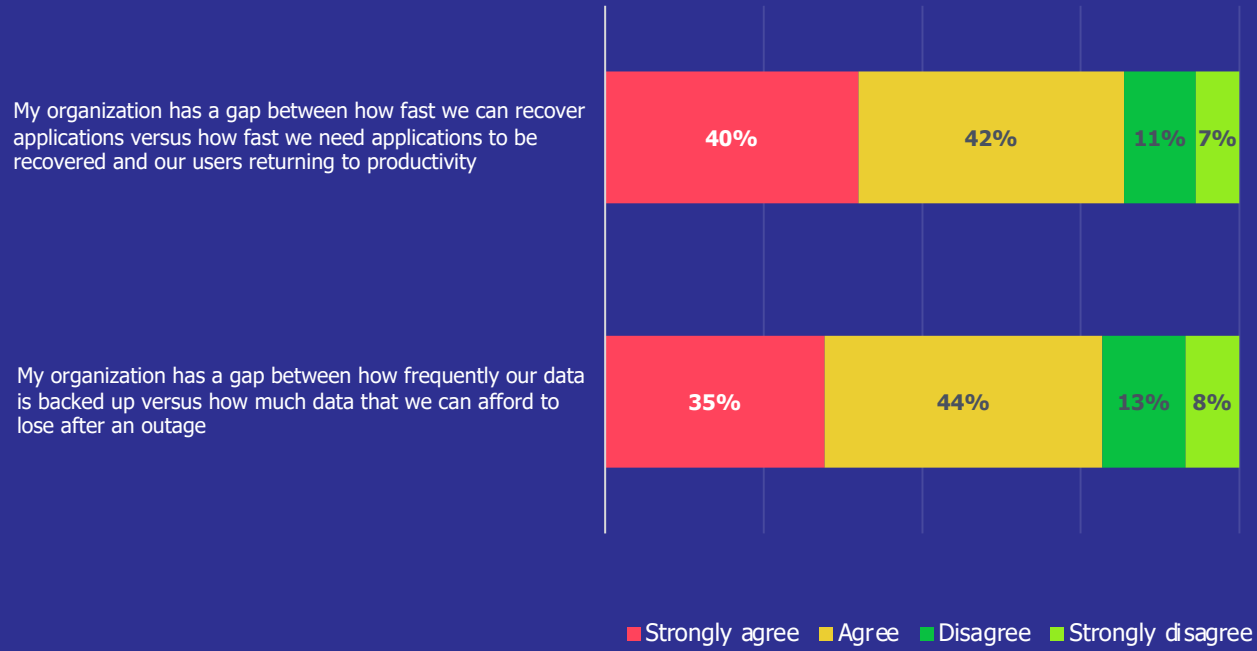
79%

of organizations admit to having a gap in their data protection SLA

82%

of organizations admit to a gap in their ability to protect their data

Does your organization have a ‘reality gap'?



Source: Data Protection Trends Report 2023
https://vee.am/DPR23

Common backup gaps

- Where does the primary data live? Is the data unstructured NAS data?
- What applications, including LOB apps, are running on physical?
- When do you need an application aware backup?
- Where, and how, will you keep your backup data secure?
- Do you understand your shared responsibility with SaaS and cloud?

Common recovery gaps

- Do you understand or know your service level objectives (SLOs)?
- Do you have the necessary tools or expertise to successfully recover the data set?
- Can you trust your backups? Have they been tested?
- Do you have a valid recovery location ready to receive your recovery data?
- Will you introduce a latent cyberthreat during recovery?

Common compliance gaps

- Do you document your process today? How do you gain approval from your change advisory board?
- Can you prove your backup compliance?
- How do you intelligently identify and protect new workloads as they are introduced?
- Can you prove data sovereignty for your backup data?
- Can you ensure compliance in that you can show that you can recover?

VEEAMON 2023

Oracle, SQL, SAP - oh my!

Challenges

- Meeting recovery objectives for the application.
- The performance impact of backup on systems at scale.
- Adherence and compliance with your company's enterprise data protection policies.
- Siloed teams complicating budgeting, decision making and prioritization.
- Using multiple, disparate tools to protect a single application.

Veeam’s got your back!

Recovery:

— Full or granular recovery of applications or their objects.

Performance:

— Snapshot-based, image level backups reduce impact at any scale.

Compliance:

— Automated backup and recovery testing with security scans.

Decision making:

— Centralized information and management, including usage and chargeback.

One tool for your enterprise:

— Single platform for application data protection and recovery that integrates with native application backup tools (SAP, SAP HANA, Oracle, MS Apps, PostgreSQL).

Veeam plug-ins for Enterprise Applications

Veeam plug-ins for Enterprise Applications extend the functionality of Veeam Backup & Replication™ and allow you to create transactionally-consistent backups of SAP HANA, Oracle and Microsoft SQL Server databases.

Veeam offers plugins for:

Microsoft SQL Server

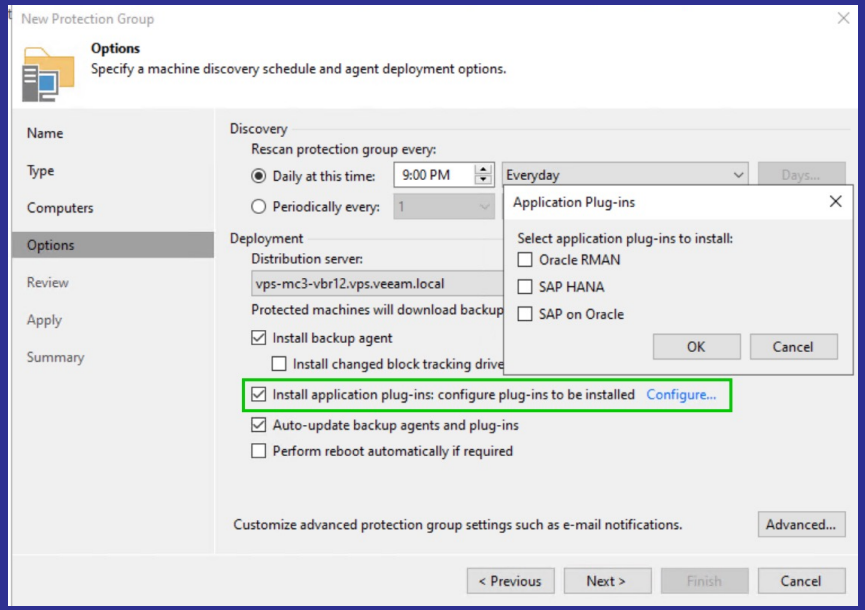
ORACLE

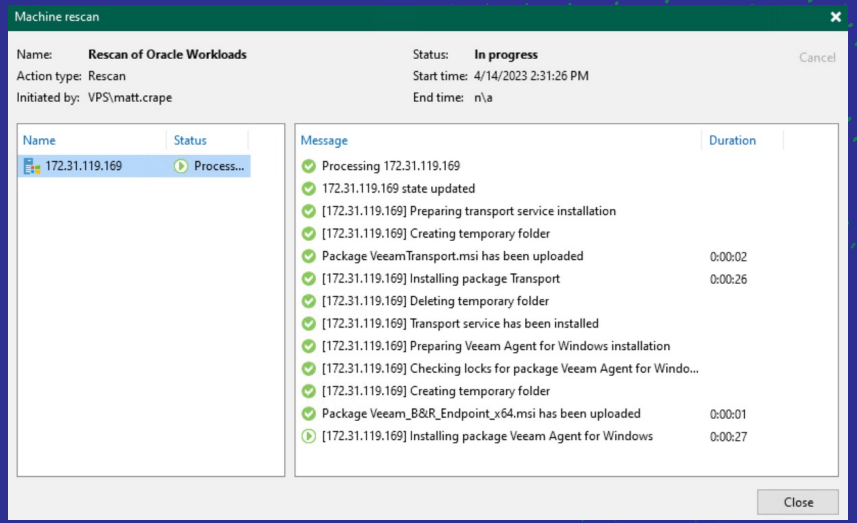
SAP HANA

SAP

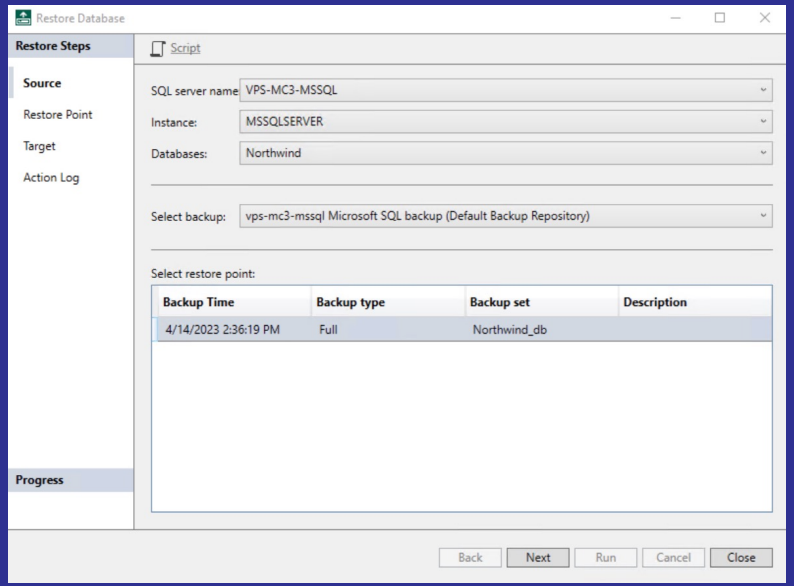
Rollout via protection group

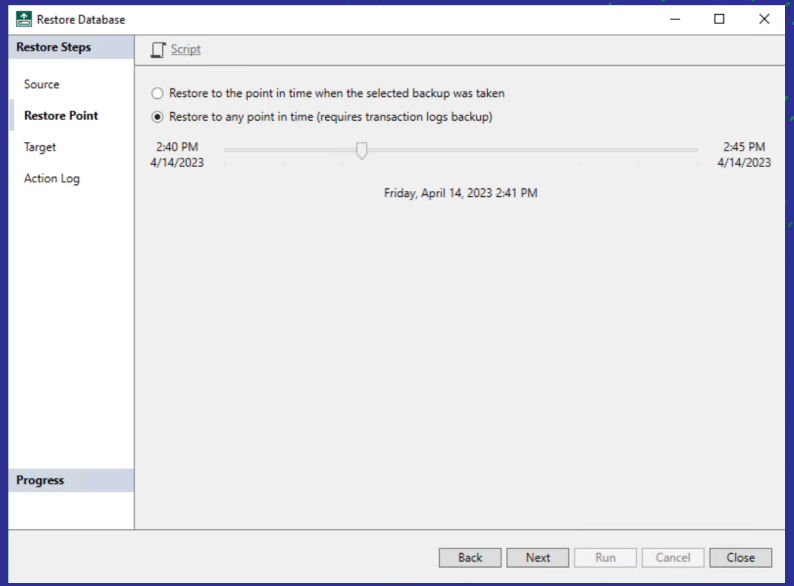
Rescan collects information about application topology that is used backup policy





Point-in-time recovery





Veeam Explorers

Veeam Explorers™ help you to quickly and easily restore application-level items (files, emails, attachments, AD objects, databases, etc.) and objects to their original location, standardizing recovery across your organization with support for:

Cloud

Challenges protecting the cloud

Backup in general, especially for lift and shift migration situations.

- Legacy, on-premises backup solutions are not ideal or designed to take advantage of the cloud.
- Migration using traditional, born in the physical data center backup and recovery methods are costly in time and effort.

Lack of understanding of the shared responsibility and ownership model.

Controlling costs (minimize egress charges, minimize resources used, etc.).

Insufficient permissions/authority within the hyperscaler inhibit deployment.

Lack of portability from the cloud back to on premises.

Veeam’s got your back!

Recover across multiple clouds and platforms in a portable data format.

Centralized AWS-, Microsoft-Azure- and Google-Cloud backup and recovery with application aware, cloud-native backup agents.

Use AWS KMS, Azure Key Vault, immutability and more to keep ransomware out.

Two-step recovery to any cloud for agile disaster recovery (DR), dev/test and analytics.

End-to-end immutability for your backups everywhere, from the data center to the cloud.

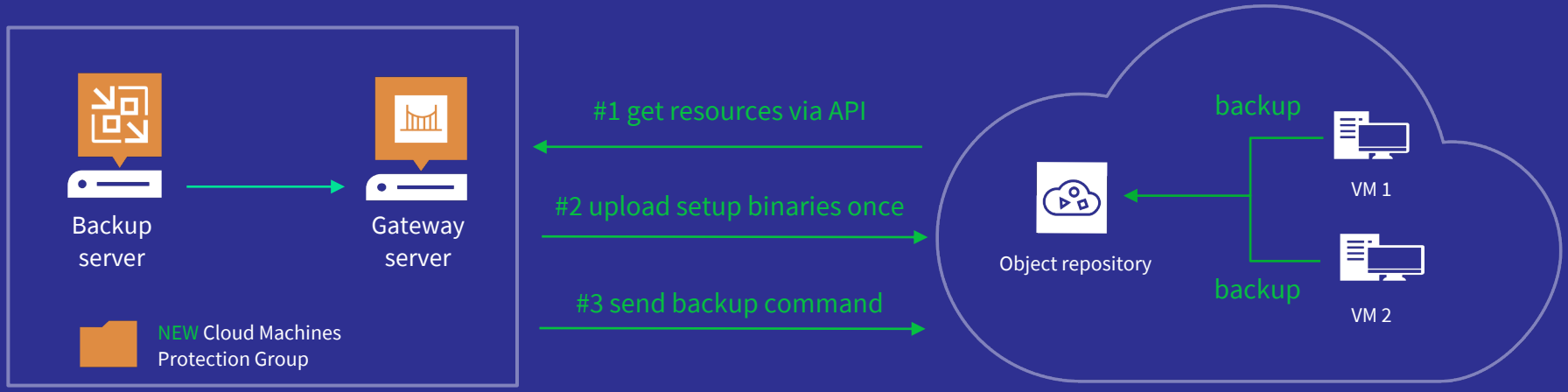
Microsoft Azure

aws

Google Cloud

Cloud file backup

Communication via AWS/Azure APIs (VeeamCloudMsgSvc service running on VMs).
No VPN / direct network connection to cloud VMs needed!



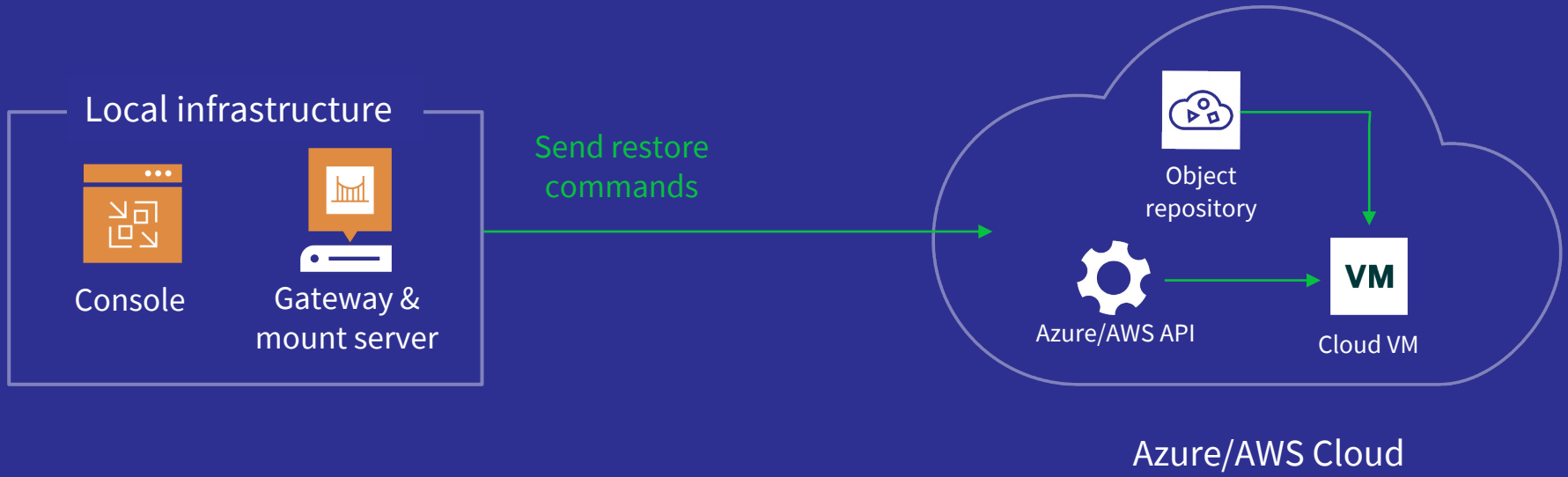
Local infrastructure

Azure/AWS Cloud

Cloud file restore

File-level restore directly from object storage into VM

Command channel via Azure/AWS APIs



Let’s get physical

Challenges

- Protecting workloads at scale can be a burden to manage and deploy.
- Different teams or applications may have different requirements or skill sets. Who manages those? Who needs to control the backups?
- Validating backup and recovery is time-consuming and expensive!
- Bare metal recovery is complex, manual and near impossible at any type of scale.
- Not all data lives in the data center! How do you protect user data on remote workstations at home and at the edge?

Veeam’s got your back

Centralized deployment and configuration allows you to automate protection with ease.

Flexible ownership.

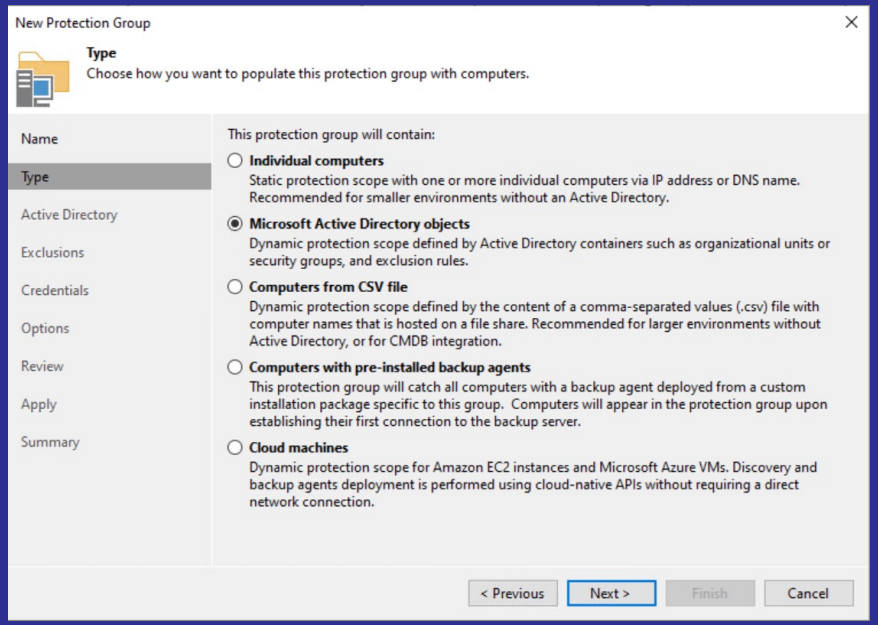
- **Command and control from a Veeam console, native app tools and user-created API management portals.**
- **Validation and testing.**

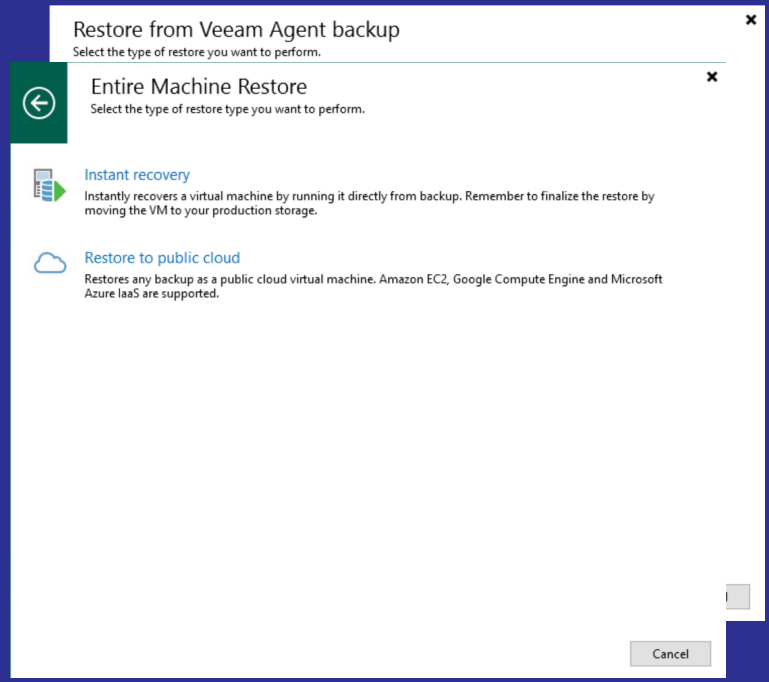
  Automated backup and recovery testing that include security scans.
- **Disaster recovery.**

  Secure, bare metal recovery to dissimilar hardware.
- **Protecting data on the move, at home and at the edge.**

  Automated protection designed for laptops and workstations that are not always on or in the same place.

Centralized management & recovery





VEEAMON 2023

Structure your unstructured data

Challenges with unstructured data

Challenges with protecting unstructured NAS data:

- The constraints of using NDMP:
  - Reliably backing up all your data in a single pass.
  - Requirements to recover the entire data set.
  - Platform or vendor lock-in.
- Scale:
  - Overall dataset size – NAS is typically large in size.
- Staying in business:
  - Loss of file connectivity for end users.
  - Loss of productivity for your business.

Veeam’s got your back!

Break free from lock-in and fortify your NAS data with unrivaled backup and instant recovery:

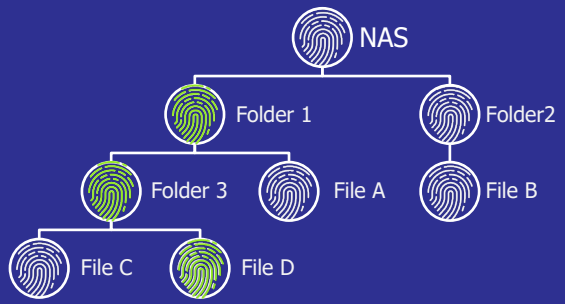
- Break the bonds of NDMP – process petabytes of data with Veeam’s differentiated NAS backup.
- Space-optimized, changed file tracking protects only what has changed since the last backups.
- Secure, immutable protection when writing to object storage, disk or tape.
- Instantly publish file shares with read/write access, unblocking your workforce.
- Background migration of full recovery set while users continue to work.

Enhanced NAS backup

Flexible

- SMB v1, 2, 3
- NFS v3, 4.1
- Windows file server
- Linux file server

Changed file tracking

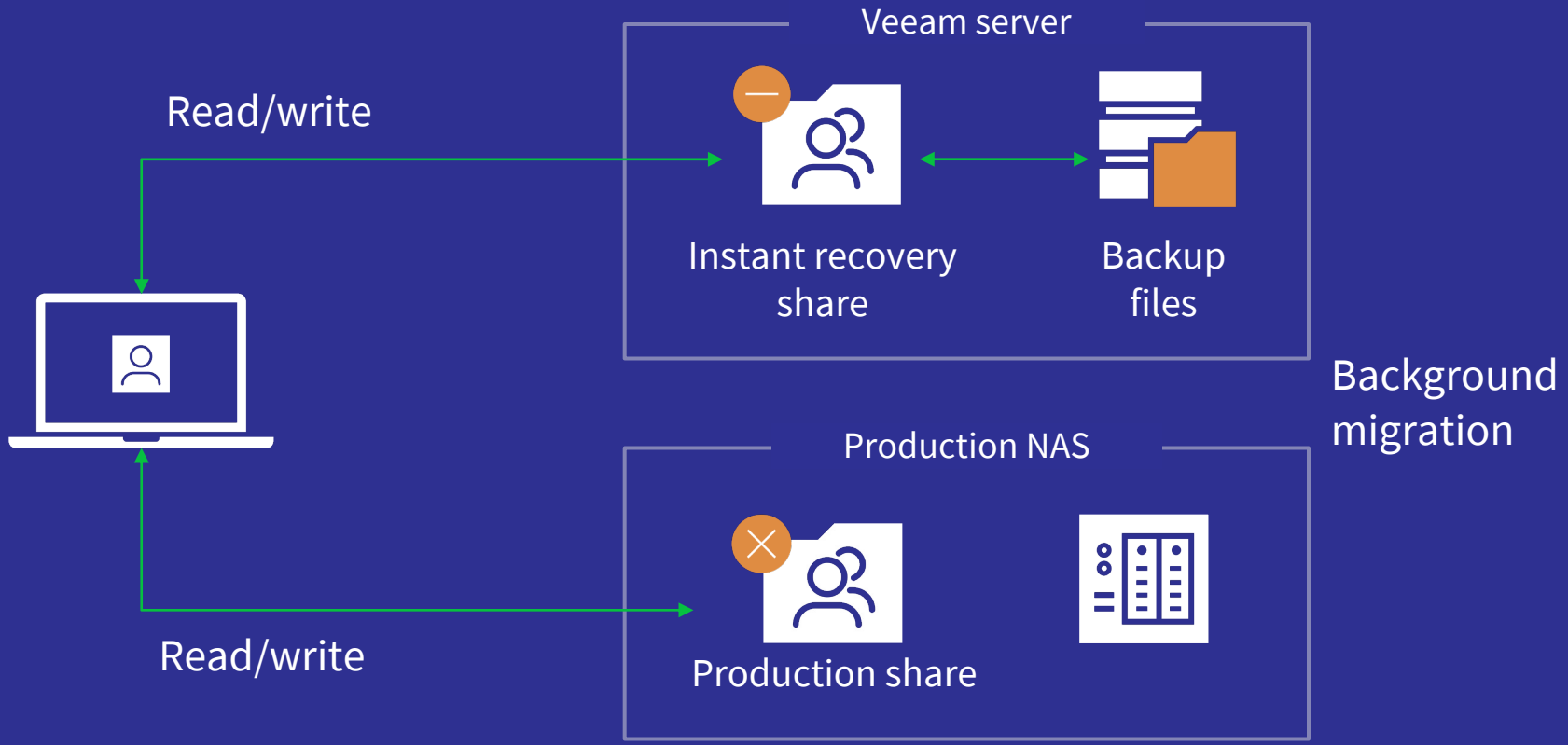


Snapshot-friendly

- No file locks
- Point in time
- Offload performance

Recovery options: instant publish, entire file share, point-in-time, file-level recovery

Instant recovery for SMB shares

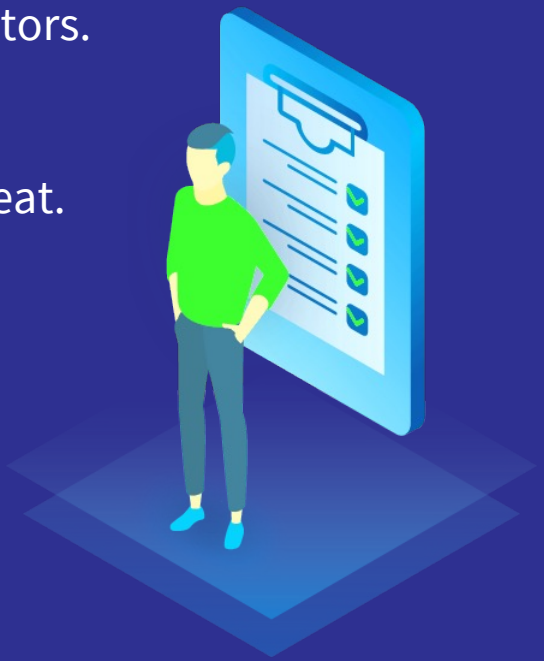


VEEAMON 2023

Secure recovery at the speed of INSTANT

Challenges

- Keeping your backup safe from ransomware and threat actors.
- Having the confidence that your restores will succeed.
- Knowing that your recovery is not introducing a latent threat.
- Responding and recovering in a cyberthreat scenario.
- Recovering at scale in the face of disaster.



Secure recovery begins with you

Backups are your last line of defense — keep them safe!

- Leverage immutability and encryption throughout the entire lifecycle.
- Restrict access to management planes.
- Monitor for suspicious activity.

Test and validate for recovery with automation

- Backup testing – confidence that you successfully protected your data.
- Threat scanning – be sure there are no threats waiting to attack.
- Recovery validation – the only way to ensure successful recovery is to test!

Orchestrate recovery

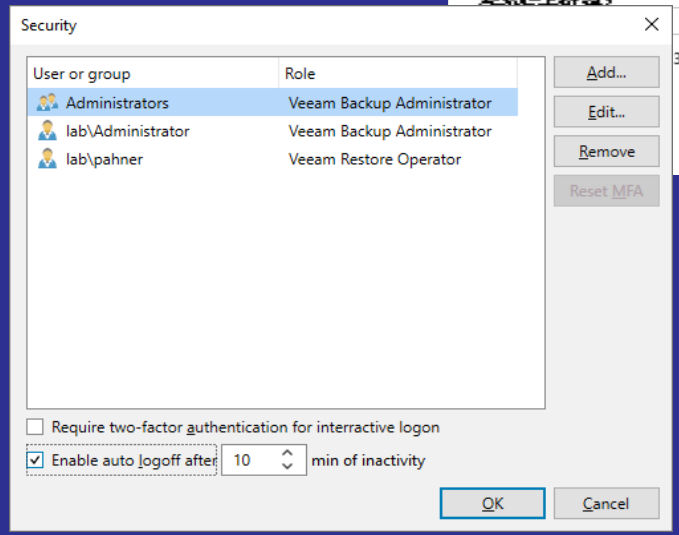
- Remove unnecessary manual processes that are prone to human error.
- Orchestrate recovery and availability in the necessary order that best works for your business.

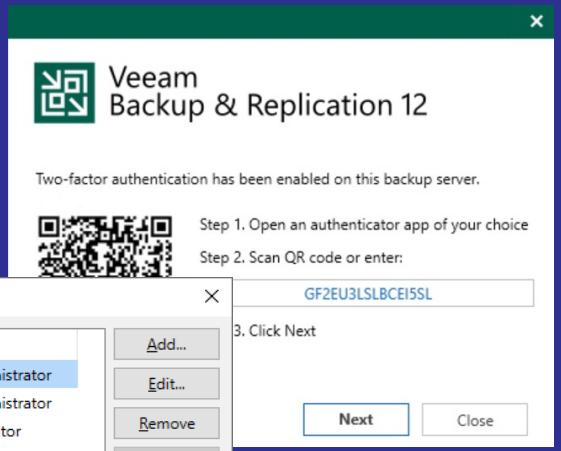
Is the door locked? Secure the console!

Enable multifactor authentication for all users:

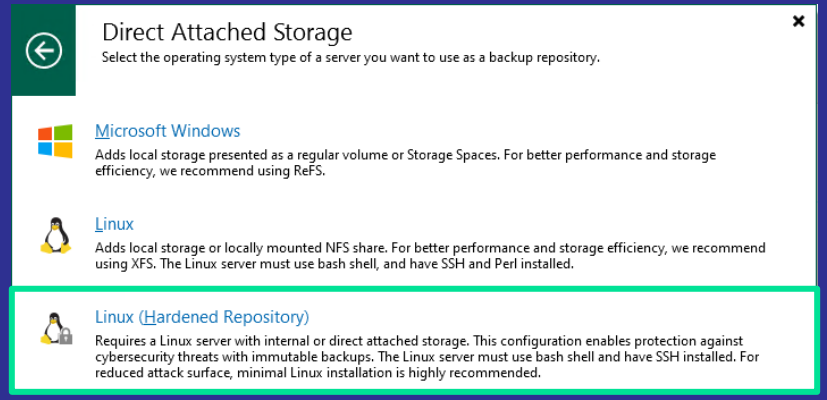
- For best results, use in addition to MFA on guest OS.
- Can be disabled for service accounts.

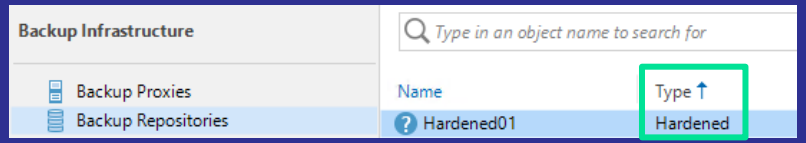
Enable log off for inactive users!

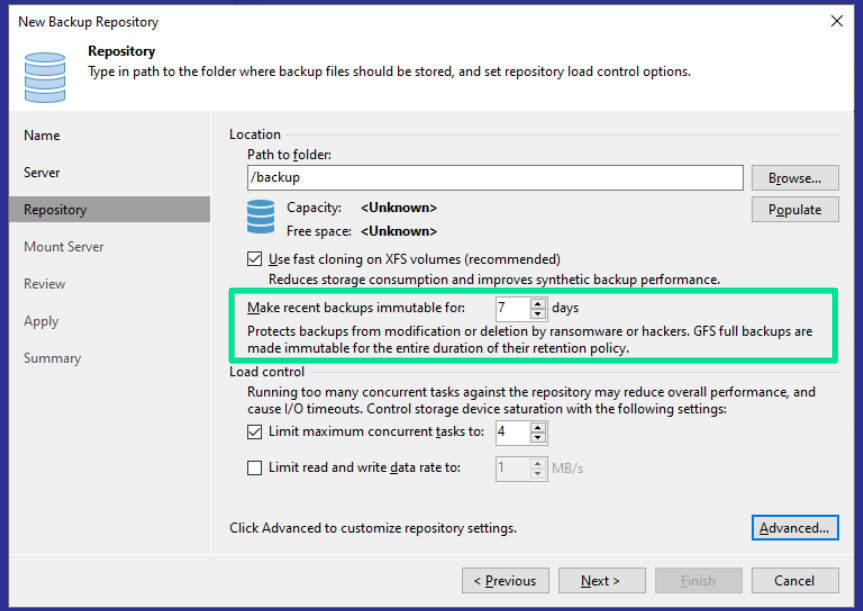




Secure backups = clean restore







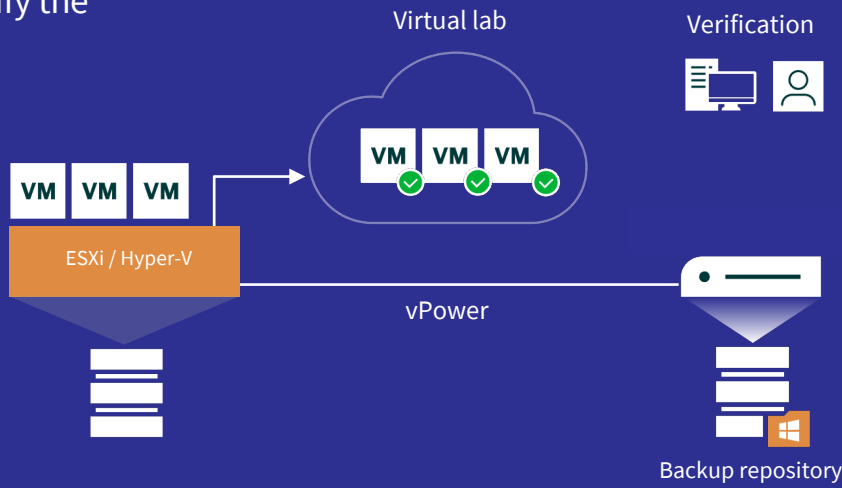
A tested backup is a valid restore

With **SureBackup®** technology, you can automatically verify the recoverability of every backup!

1. VMs are mounted in an isolated virtual environment.
2. Testing of your choosing is performed against the backup.
3. Reports are compiled and sent directly to your mailbox.

Bonus: Veeam Data Integration API

Effortlessly enable data mining, data classification, security analysis, data forensics, eDiscovery and more directly from an instantly mounted backup



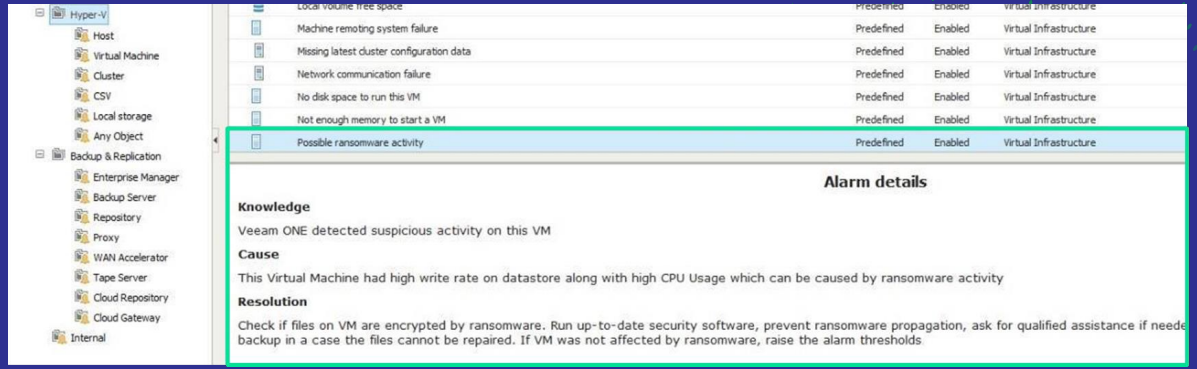
Create virtual lab → Create application groups → Create SureBackup job(s) → Specify tests within the jobs → Schedule SureBackup jobs → Receive verification report

Detect threats early

Out-of-the-box reporting enables visibility for proactive management and recovery success detect abnormal backup sizes

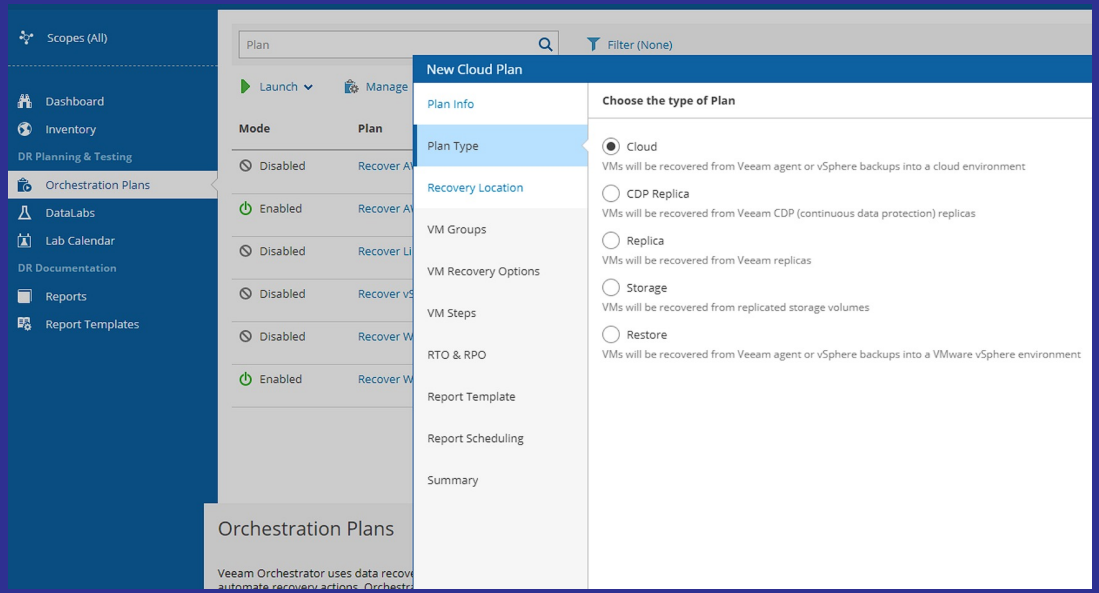
Status	Time	Source	Ty...	Name
Warning	9:23:24 PM	SoBR - Synology & Wasabi		Backup repository connection failure
Error	9:20:03 PM	This object (VEEAM)		Suspicious incremental backup size
Error	9:20:03 PM	Job "42u.local" (VM "DC-02")		Incremental backup size of "DC-02" (**68.0%**) created by "42u.local" job is below the configured threshold (70.0%) Incremental backup creation time 2022-11-07 03:00:27 (UTC-5:00)

Alert on possible ransomware activity



Cloud DR

- Make using cloud as a true DR location a reality with direct recovery to Microsoft Azure.
- Eliminate errors by automating and orchestrating testing in an isolated sandbox.
- Guarantee clean recovery with the most recent, threat-free recovery point.



StrategicResearch@veeam.com

Ransomware Trends 2022

1,000 organizations that suffered at least one attack

- CISO, SecOps, IT Ops, backup personas.
- Attack source, targets, pervasiveness.
- Remediation methods & lessons learned.

http://vee.am/RW22

Salesforce Protection Trends 2022

800 orgs managing SFDC across US, EU and APJ

- Salesforce Devs/Admins & backup personas.
- Drivers & sentiments toward backing up SFDC.

http://vee.am/SF22

Cloud Protection Trends for 2023

1,700 using at least one IaaS, SaaS or PaaS

- 3 XaaS, IT Ops, and backup admin personas.
- Backup drivers/methods for IaaS/PaaS/SaaS.
- Adoption drivers for BaaS & DRaaS.

http://vee.am/CPT23

Data Protection Trends 2023

4,200 unbiased organizations across 28 countries

- Macro data protection drivers/trends.
- Real-world downtime stats, DX considerations.
- Cyber-strategies, containers and BC/DR.

http://vee.am/DPR23


Thank you
VEEAMON 2023