

TECHNICAL WHITE PAPER

Ransomware Remediation with Veeam and Pure

Rely on powerful ransomware mitigation with Pure FlashArray//C and Veeam Backup & Replication.

Contents

Introduction3

The Rising Threat of Ransomware3

Pure Storage FlashArray//C4

 Data Reduction..... 4

 FlashArray Snapshots 4

 SafeMode™ Snapshots 5

 Proactive Alerts 5

 Integration with Veeam Universal Storage API 5

SafeMode Operational Impact.....6

Protecting the Veeam Repository6

 How to Protect Your Data..... 6

 How to Recover Your Data 8

 Import Option 1..... 10

 Import Option 212

Improving Veeam Backup and Recovery Performance with Snapshots..... 14

 How to Enable Snapshots..... 14

 How to Recover with Snapshots.....15

Conclusion 16

Additional Resources 17



Introduction

Many organizations are on a journey to transform into data-driven organizations. Analytic processes created to derive strategic, data-driven decisions depend on easily consumable data. Protecting data is fundamental to developing the modern data center and serves as the foundation of digital transformation.

At Pure Storage®, we believe maintaining data availability and ransomware protection should not sacrifice the elements of the modern data center. Pure FlashArray™ (specifically FlashArray//C) and Veeam Backup & Replication work together to improve the performance of your backups and guard against ransomware attacks.

The Rising Threat of Ransomware

Cybercriminals have long realized the importance of data. And since the early 2000s, they've explored different tactics to attack organizations. In an article published in October 2016, the United States Department of Justice estimated that an average of 4,000 ransomware attacks occurs daily across all vertical industry. This figure represented a 300% increase in ransomware activity compared to the same point the year before.

Just five years later, Cybersecurity Ventures estimates that the global cost of ransomware-related damages will reach \$20 billion in 2021, compared to their estimated damages of \$11.5 billion in 2019 and \$8 billion in 2018.

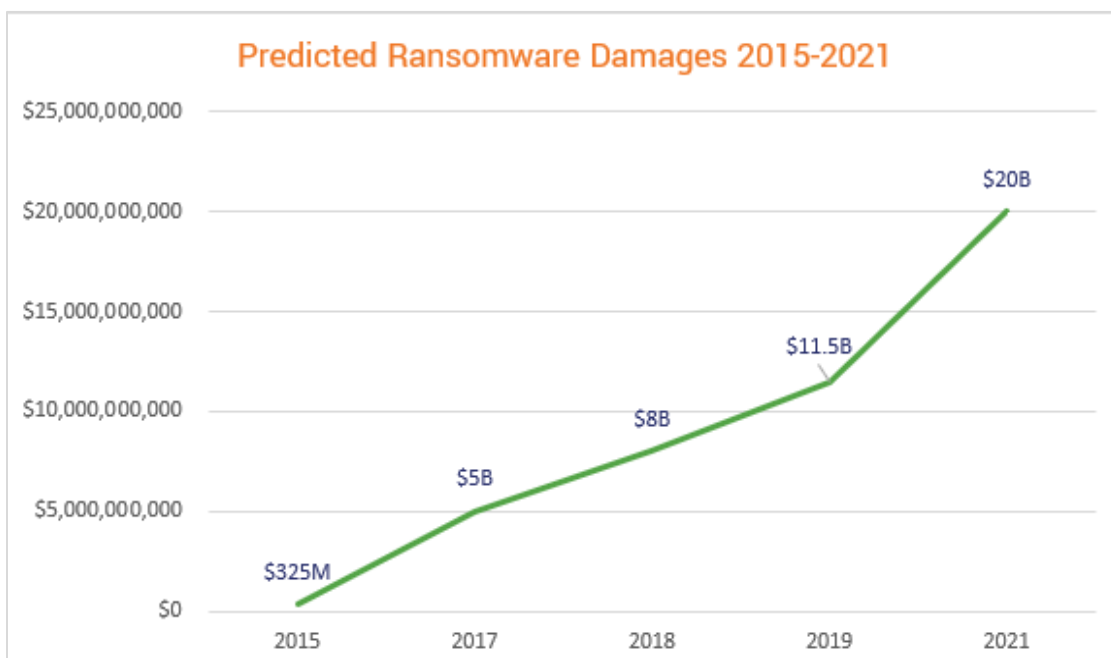


Figure 1. Tracking the predicted growth of ransomware, Cybersecurity Ventures.¹



A primary defensive strategy to protect against ransomware attacks is to back up everything. However, since the backup environment itself is prone to ransomware attacks, additional infrastructure is typically needed. A second copy to tape is another tactic, but doing so comes at the cost of agility, performance, and availability, which are primary features of a modern data center. Depending on regulatory and business guidelines, Write Once Read Many (WORM) object storage may provide an option. However, while WORM storage offers advantages to tape in a ransomware situation, recovery time objectives (RTOs) can be at risk because you need to import objects back into the backup system.

Pure Storage FlashArray//C

Pure built the FlashArray family for the modern data center. FlashArray//X is well recognized for its high-performance, sub-millisecond response time, robust data reduction capabilities, deployment and management simplicity, built-in protection features such as ActiveCluster™ synchronous replication, and deep integration with the leaders in the data protection space.

Introduced in September 2019, FlashArray//C is the industry's first capacity-optimized, all-QLC NVMe array. Built to bring consistent 2- to 4-millisecond response time, FlashArray//C delivers data reduction capabilities with tier one reliability at disk economics. This capability makes FlashArray//C an ideal use case as a target for data protection software like Veeam Backup & Replication.

Today's modern data centers need a platform like FlashArray//C. Spinning disk and even hybrid arrays can't meet agility expectations, data reuse, data protection, and most importantly, quick recovery if needed. Because FlashArray//C is based on the same platform as FlashArray//X, it inherits all the features and functionalities provided by the Purity//FA Operating Environment.

Data Reduction

Data reduction at Pure is designed to be “always-on.” FlashArray reduces data in five ways:

1. Pattern removal identifies and removes repetitive binary patterns, including zeroes. In addition to capacity savings, pattern removal reduces the volume of data to be processed by the dedupe scanner and compression engine.
2. High-performance, inline deduplication operates on a very-granular, 512-byte aligned, variable block size ranging from 4KB to 32KB. Only unique blocks of data are saved on flash, removing duplicates that fixed-block architectures might miss.
3. Inline compression reduces data to use less capacity than the original format. Append-only write layout and variable addressing optimize compression savings by removing the wasted space that fixed-block architectures introduce.
4. Post compression provides additional, heavier-weighted compression algorithms applied post-process to increase the efficiency savings on data that was already compressed.
5. Copy reduction allows for copying data on a FlashArray to only involve metadata. Leveraging the data reduction engine, Purity provides instant pre-deduplicated copies of data for snapshots, clones, replication, and xCopy commands. This has interesting new implications like instant and space-saving migration from VMFS VMs to new vVOLS in VMware.

FlashArray Snapshots

FlashArray snapshots are immutable, point-in-time images of one or more volumes. Immutability means FlashArray snapshots cannot be directly accessed by hosts or have their contents modified at all. Essentially, snapshots are copies of a source volume's metadata content pointers. As a result, creating snapshots is extremely fast and space-efficient—initially consuming no added capacity and completed in about the same time it takes to complete a single I/O. Volumes can be deleted or



modified without affecting their corresponding automated snapshot and snapshot history. Snapshots are typically used to create new volumes and can be used to “roll back” to an earlier point in time on existing volumes. In a ransomware attack, the fast restore and clone capabilities of snapshots can help minimize operational recovery as part of ransomware remediation or when cleaning out malware, viruses, and rootkits. There is nothing faster for restore than a metadata operation.

SafeMode™ Snapshots

FlashArray's default behavior protects administrators from accidental deletion of volumes, snapshots, protection groups, and other array objects for 24 hours. Deleted objects are retained on FlashArray in the “eradication-pending” bin. At the end of the eradication period, each object and any related content in the “eradication-pending” bin is completely removed.

SafeMode extends the core immutability protection that snapshots provide to help with scenarios where array administrative credentials have been compromised. Enabling SafeMode triggers three changes to array behavior for administrative users:

- Disabling the ability to eradicate volumes and snapshots from the destroyed items bucket
- Introducing an adjustable Eradication Timer from 24 hours up to 30 days
- Disabling the ability to shorten the Protection Group retention period

Since ransomware attackers typically infiltrate an environment weeks or months before they start encrypting data, they often focus on compromising the means of data protection by targeting backups and snapshots. FlashArray snapshots and SafeMode protection focus on providing a copy of the data before the point of encryption. Once the attacker starts encrypting, organizations usually quickly notice as applications start going offline.

Proactive Alerts

Ransomware attacks commonly lead to an increase in FlashArray capacity consumption and to a decrease in the data reduction rate. FlashArray's remote telemetry reporting and alerting mechanisms monitor space consumption and help with early ransomware detection.

Integration with Veeam Universal Storage API

The Pure Storage plug-in for Veeam further improves backups. High transactional virtual environments are particularly sensitive to backup operations. Utilizing hardware snapshots eliminate VM stun issues that contribute to very low RTOs.

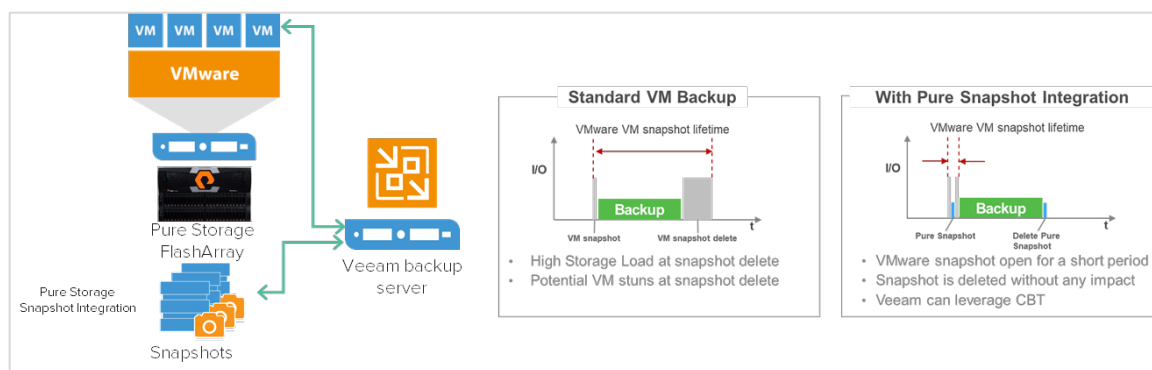


Figure 2. Pure Storage snapshot integration with Veeam Backup & Replication.



SafeMode Operational Impact

Enabling SafeMode on FlashArray has a system-wide impact. The SafeMode eradication timer protects both volumes and protection groups. Consequently, you can delete volumes no longer needed or manually created snapshots, but their space will not be reclaimed back into the free space pool until the eradication timer expires. If the FlashArray//C is also hosting other applications other than Veeam repositories, it's essential to plan. Keep in mind the lag time between deleting volumes or manually created snapshots and when their capacity is available in the free space pool.

Protecting the Veeam Repository

A repository is a storage location where Veeam keeps backup files of NAS, physical servers, and virtual machines (VMs). Veeam backup files are completely portable and require no external metadata (such as a central catalog) to be recoverable.

Veeam's best practice guide states a repository should be highly resilient since it is hosting customer's data. One way to do this is to create multiple copies of the repository. However, in the event of a ransomware attack, all repository copies could also be at risk. There is also the possibility that it could take a long time to recover from the other copies.

When FlashArray//C is set up with a protection group schedule to take periodic snapshots of the repository volumes, it creates a series of immutable point-in-time snapshots retained for a configurable retention period set up by the protection group. When SafeMode is enabled, these snapshots are further protected from destruction even from those with admin privileges.

If ransomware strikes, you can quickly use the SafeMode protected repository snapshots—drastically reducing RTOs—and start to recover your environment. Some data loss should be expected because the latest snapshot might have occurred during or after the attack.

How to Protect Your Data

As stated earlier, the encryption phase of a ransomware attack is detected quickly due to applications going offline or data becoming unavailable. Most Pure customers choose snapshot schedules of 7 to 14 days with SafeMode eradication timeout values of the same. While Pure cannot give a recommendation guaranteed for every customer environment, the key formula is based on how soon the encryption phase of an attack would be detected (usually hours to days at most). Just be sure to have data in snapshots that go back to a point-in-time before the attacker started the encryption processes.

Enabling SafeMode requires opening a case with Pure Support. An authorized representative of your company will work with Pure Support to set up authorization, enable SafeMode on the FlashArray, and configure the eradication timer. Once set, emptying the eradication bin or changing the eradication timer can only be changed by working with Pure Support. If an admin or an attacker tries to eradicate the snapshot, a message will be displayed, stating eradication is disabled (Figure 3).

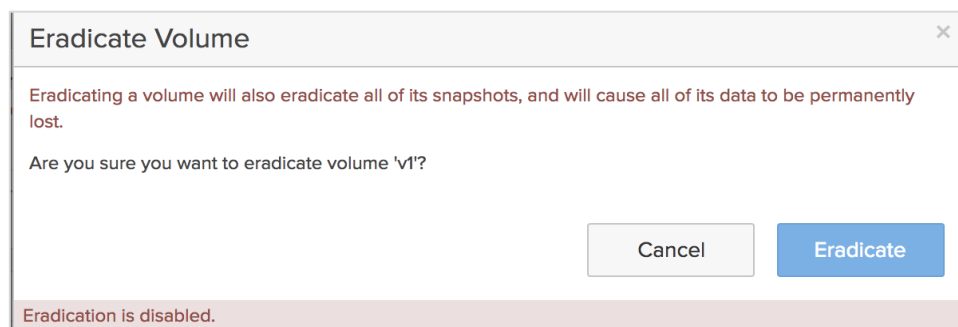


Figure 3. Volume eradication is disabled when SafeMode snapshots are enabled.



To protect Veeam repositories, set up a protection group to take periodic snapshots. You can use the Purity//FA GUI, secure shell, or REST API (please see the Additional Resources section below for CLI and API guides). The following are the steps using Purity//FA:

1. Create a Protection Group.

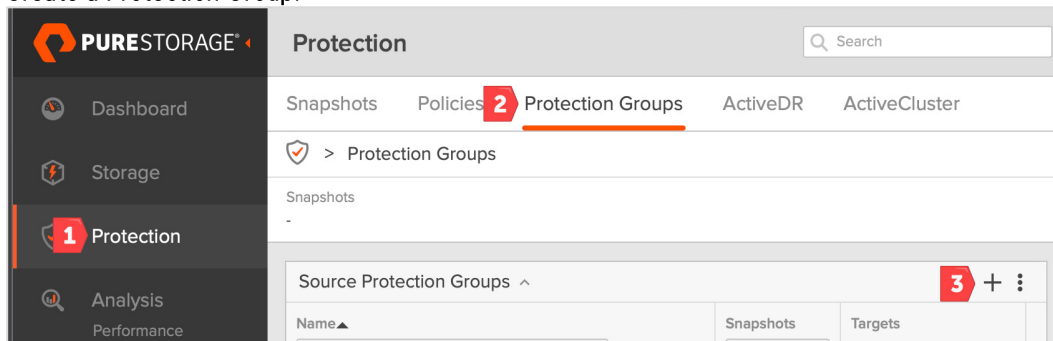


Figure 4: Creating a Protection Group using Purity//FA

2. Add member(s) to the Protection Group. This could be Veeam Repository Volume, Veeam Repository Server, or the Host Group housing repository volumes.

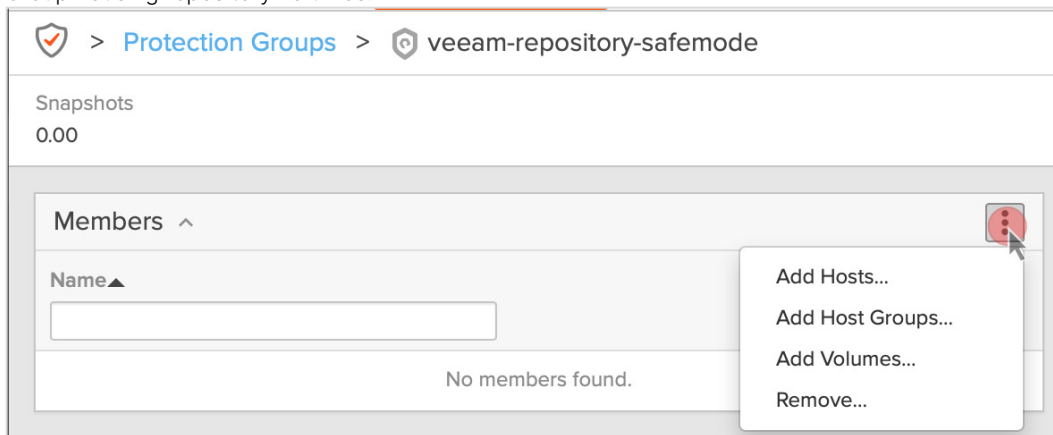


Figure 5: Adding members to the Protection Group

3. Set up snapshot schedule. In this case, we're creating a snapshot of the Veeam Repository every day at noon as it's outside the backup window (6:00 PM–6:00 AM). Doing so ensures we have a snapshot of last night's backup. The snapshots will be retained for two weeks. For environments with a 24-hour backup window, depending on how aggressive the protection strategy is, it's best to create a couple of snapshot schedules, where each will capture backups that occurred the previous 12 hours. Once the snapshot schedule is enabled, Purity//FA immediately starts the snapshot process.



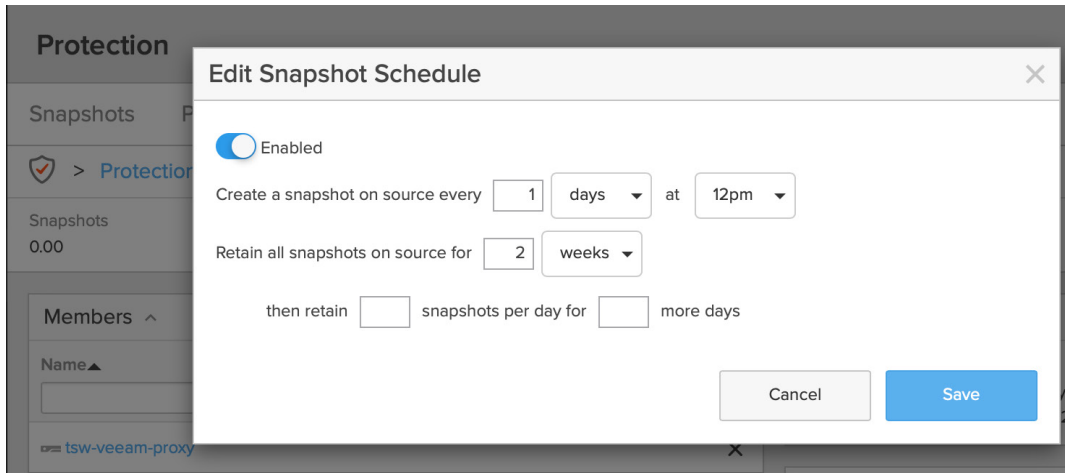


Figure 6. Set the snapshot schedule outside the backup window.

How to Recover Your Data

The ransomware recovery process typically starts with creating a “clean room,” in which the operating system running Veeam software has been declared to be clean from ransomware binaries with updated antivirus/malware software. Next, we need to identify which snapshot to use for recovery.

Again, we’ll use Purity//FA GUI to perform recovery tasks, but you can also use CLI and REST. One of the main signatures of ransomware is a significant reduction in deduplication. Purity//FA displays volume and snapshot sizes in terms of their unique data. Therefore, you can see this pattern on the Purity//FA GUI and CLI. Figure 7 shows a screenshot of the “purevol” command. This example shows the Veeam repository volume in normal operation with 8:1 data reduction, as the VMs.

```
Sat Feb 20 19:11:05 PST 2021
```

| Name | Size | Thin Provisioning | Data Reduction | Total Reduction | Unique | Snapshots | Total |
|----------------------------|------|-------------------|----------------|-----------------|---------|-----------|---------|
| tsw-veeam-safemode-2T-Repo | 2T | 28% | 8.0 to 1 | 11.1 to 1 | 238.16M | 1.75M | 239.91M |

```
root@sn1-c60r3-d06-20-ct0:~#
```

Figure 7. Screenshot of the “purevol” command.

However, after simulating a ransomware attack, running the same “purevol” command shows a very different picture (Figure 8) as data reduction dropped to a 1.9:1 ratio. Also of note is the significant growth of unique data from 238MB to almost a terabyte. Besides deduplication being significantly lower, the sizes of the combined snapshots are also considerably larger.

```
pureuser@sn1-c60r3-d06-20> purevol list tsw-veeam-safemode-2T-Repo -space
```

| Name | Size | Thin Provisioning | Data Reduction | Total Reduction | Unique | Snapshots | Total |
|----------------------------|------|-------------------|----------------|-----------------|---------|-----------|-------|
| tsw-veeam-safemode-2T-Repo | 2T | 6% | 1.9 to 1 | 2.0 to 1 | 914.75G | 755.52G | 1.63T |

```
pureuser@sn1-c60r3-d06-20>
```

Figure 8. Telltale signs of a ransomware attack.

It’s worth noting that you can also quickly glance at a historical graph of the repository volume (Figure 9). This graph shows the total volume consumption that includes data and snapshots. You can reach this view from FlashArray Purity//FA GUI, Analysis Tab, then choosing the desired volume.



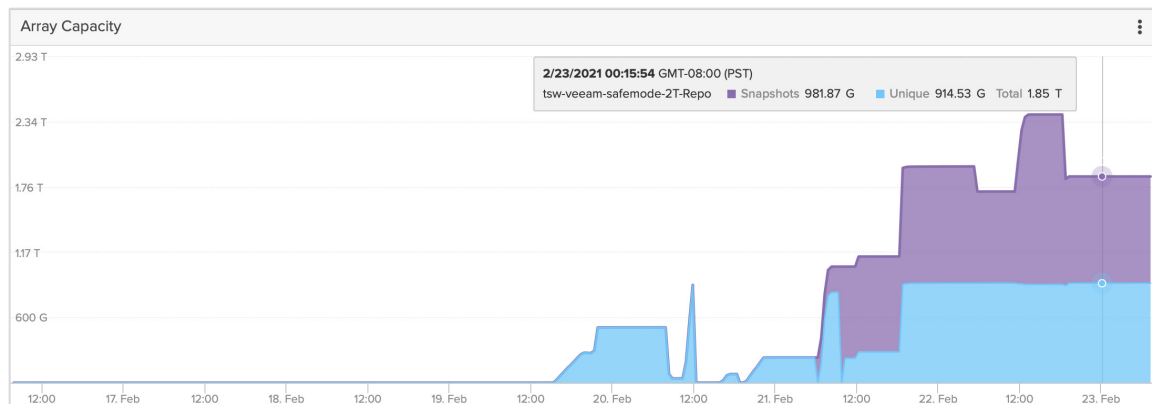


Figure 9. Example of the Veeam repository volume.

Figure 10 shows the daily repository snapshot for a little over a week. Looking at the most recent snapshots, the sizes are significantly larger than the previous trend of daily snapshots, which reflect all notable changes from the day before.

| Volume Snapshots ^ | | | |
|---|---------------------|----------------------|--------------------|
| General | | Transfer | 1-10 of 11 < > + ⋮ |
| Name | Created | Snapshots | |
| <input type="text"/> | All | <input type="text"/> | |
| veeam-repository-safemode.11.tsw-veeam-safemode-2T-Repo | 2021-02-22 12:00:00 | 755.51 G | ransomware |
| veeam-repository-safemode.10.tsw-veeam-safemode-2T-Repo | 2021-02-21 12:00:00 | 730 M | ransomware |
| veeam-repository-safemode.9.tsw-veeam-safemode-2T-Repo | 2021-02-20 12:00:00 | 1.55 M | ransomware |
| veeam-repository-safemode.8.tsw-veeam-safemode-2T-Repo | 2021-02-19 12:00:00 | 764.40 K | Candidate |
| veeam-repository-safemode.7.tsw-veeam-safemode-2T-Repo | 2021-02-18 12:00:00 | 42.47 K | |
| veeam-repository-safemode.6.tsw-veeam-safemode-2T-Repo | 2021-02-17 12:00:00 | 77.08 K | |
| veeam-repository-safemode.5.tsw-veeam-safemode-2T-Repo | 2021-02-16 12:00:00 | 68.13 K | |
| veeam-repository-safemode.4.tsw-veeam-safemode-2T-Repo | 2021-02-15 12:00:00 | 174.16 K | |
| veeam-repository-safemode.3.tsw-veeam-safemode-2T-Repo | 2021-02-14 12:00:00 | 250.69 K | |
| veeam-repository-safemode.2.tsw-veeam-safemode-2T-Repo | 2021-02-13 12:00:00 | 35.11 K | Oldest snap |
| Destroyed (2) v | | | |

Figure 10. Analyzing the daily repository snapshot report.

Looking at the three most recent snapshots (marked with red arrows), it's clear to see significant changes to the snapshots compared to the previous six days. Skipping to the snapshot marked with a green arrow called "candidate," it appears to be the most suitable for restore, as its size is in line with the trend observed over previous snapshots. We still have to verify the snapshot is clean, but this should be the starting point.

Due to the speed and performance of FlashArray snapshots, the "restore speed iteration" can also be dramatically increased by quickly choosing another snapshot if one previously selected does have encrypted data. From Purity//FA, select **Protection > Protection Group > Source Protection Group Snapshots**. Then select the desired snapshot and click Copy Snapshot (Figure 11).





Figure 11. Volume Snapshot screen.

This option will allow you to create a volume from the snapshot. You will be prompted to choose a name for the volume, making it available to be mapped to Veeam Repository Server (Figure 12). Once mapped, the administrator should perform virus and malware scans on the volume before importing the backups.

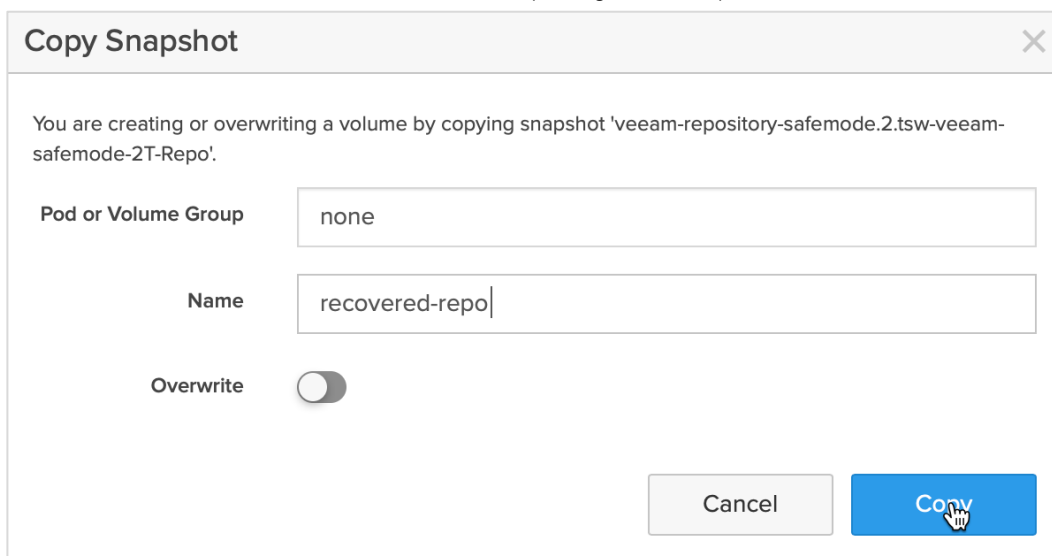


Figure 12. Copying the selected snapshot.

Import Option 1

Since this is a new Veeam server, there is no repository configuration to import. Therefore, we will create a new repository on the mapped snapshot volume, then scan the repository for existing backups. From the Veeam management interface (under the "BACKUP INFRASTRUCTURE" section), add a new repository (Figure 13). Then follow the wizard to create a repository as normal.



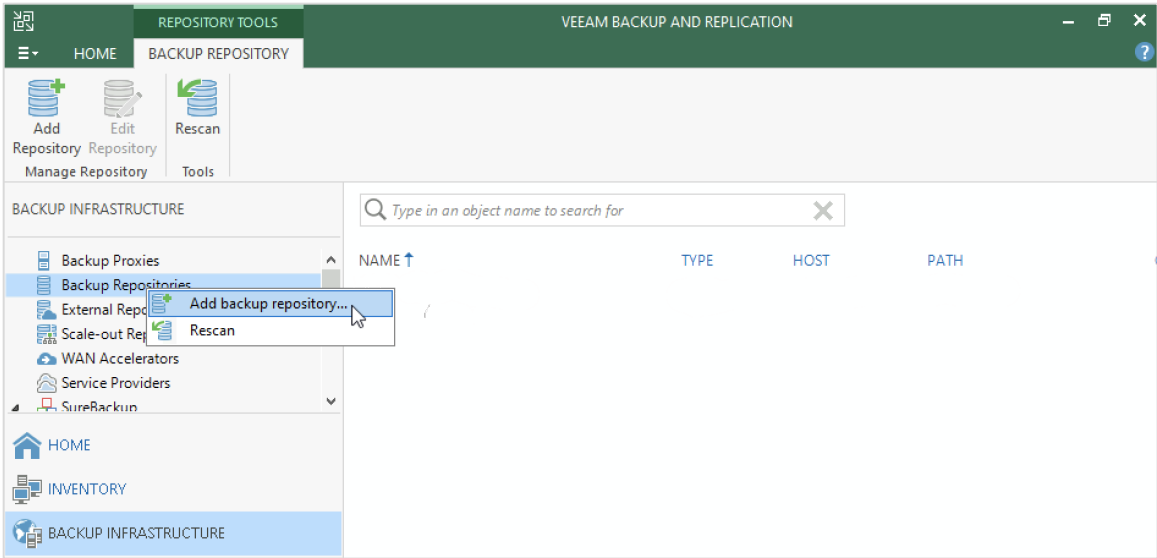


Figure 13. Adding a new backup repository in Veeam.

It's important to check the option “Search Repository for existing backups and import them automatically” checkbox (Figure 14), located in the preview section of the “Add backup repository” wizard.

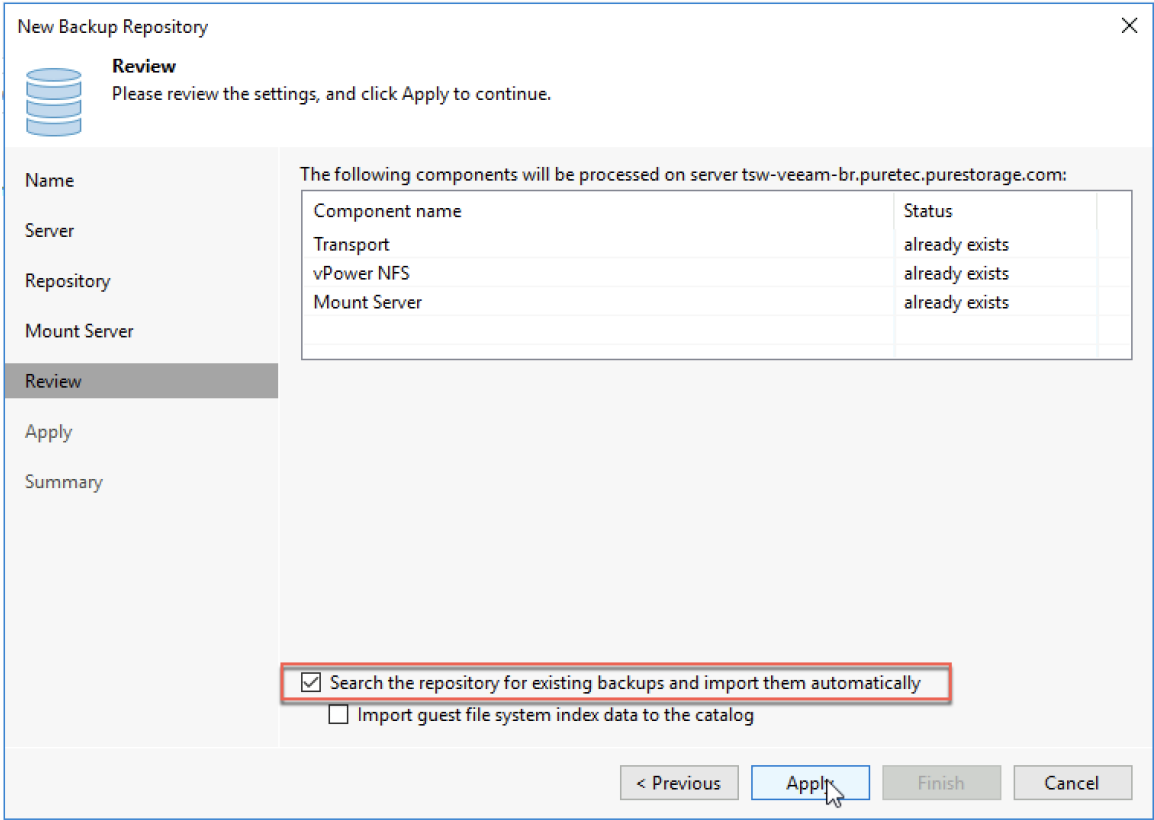


Figure 14. Review options when creating new backup repositories.

Once the Wizard is complete, the new repository is added to the Backup Infrastructure (Figure 15).



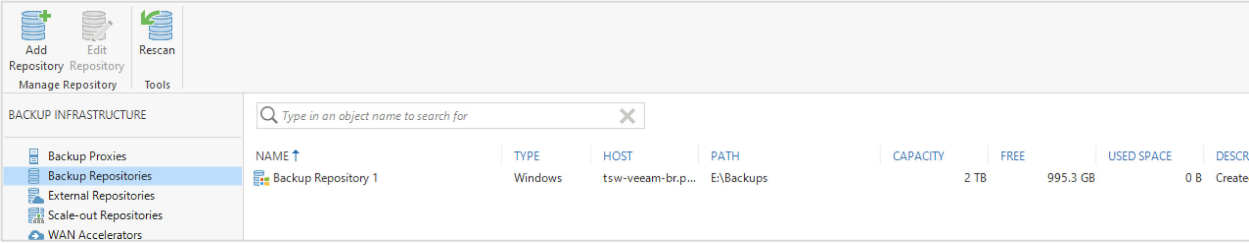


Figure 15. A new repository added to the Backup Infrastructure.

Import Option 2

Since scanning the repository volume for viruses can take a long time, you may first need to restore a handful of important services like DNS, Active Directory, and E-Mail as quickly as possible before recovering the rest of the infrastructure. We can import individual backup jobs that include the VMs or physical server backups needed for restore for these purposes. Then we can start the restore process while ensuring the antivirus scan is enabled so as you scan, you restore. This feature is called Secure Restore. From the Veeam management interface, under the “Home” section, then “Import Backup” Action (Figure 16).

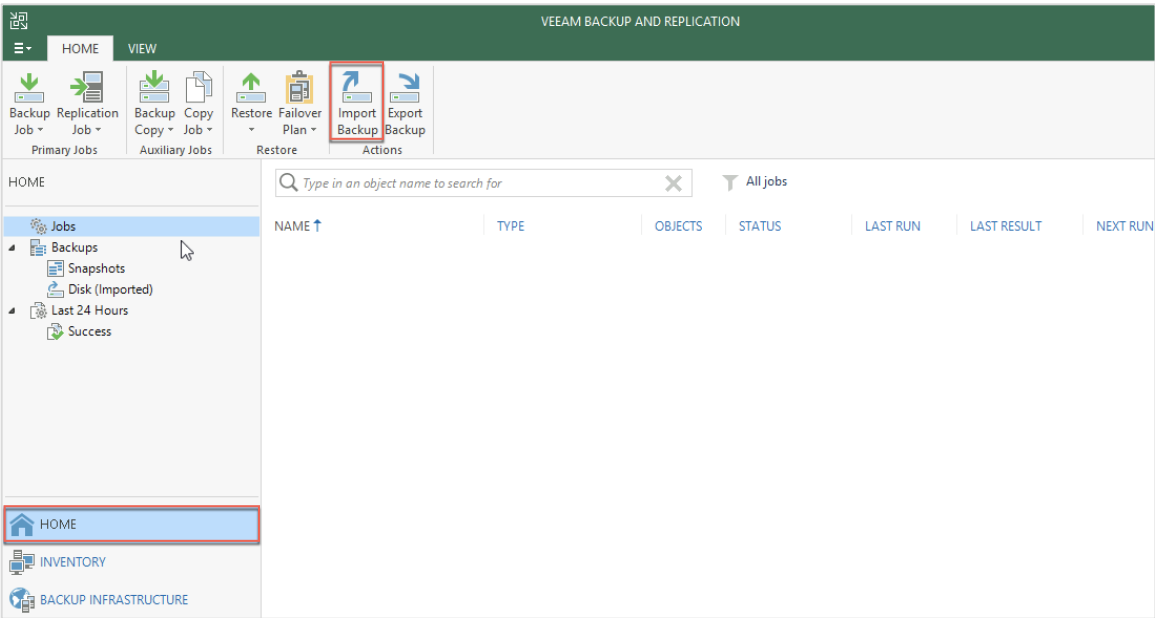


Figure 16. Importing backups from the Veeam console.

You will be prompted to specify which backup to import. Since this option allows you to point directly to the backup job, you may need to repeat this process once per backup Job (Figure 17).



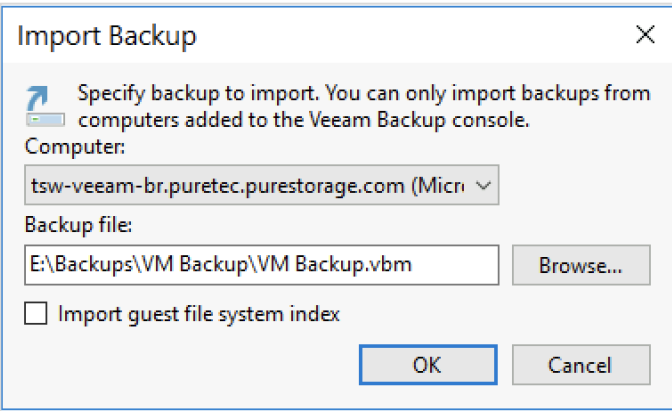


Figure 17. Importing the backup.

Once Veeam scans the disk, a new shortcut for the recovered (Imported) backups is displayed (Figure 18).

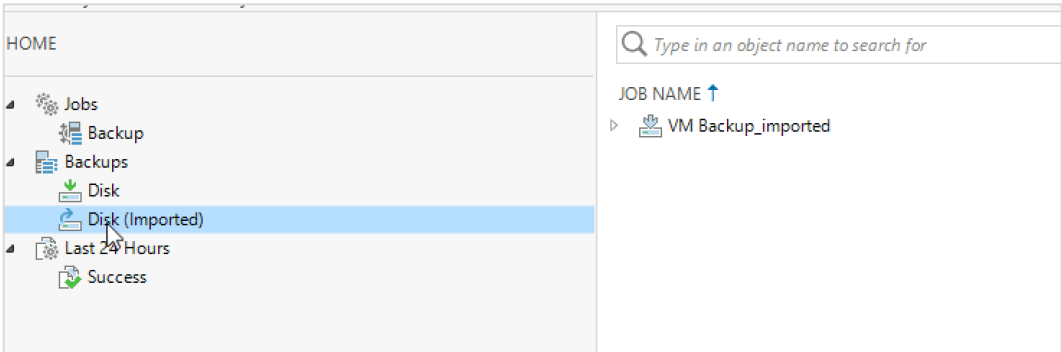


Figure 18. A new shortcut for recovered backups.

Run the antivirus scanning tools during restore. If this is a VM, you can disable network adapters for extra checks if necessary (Figure 19).

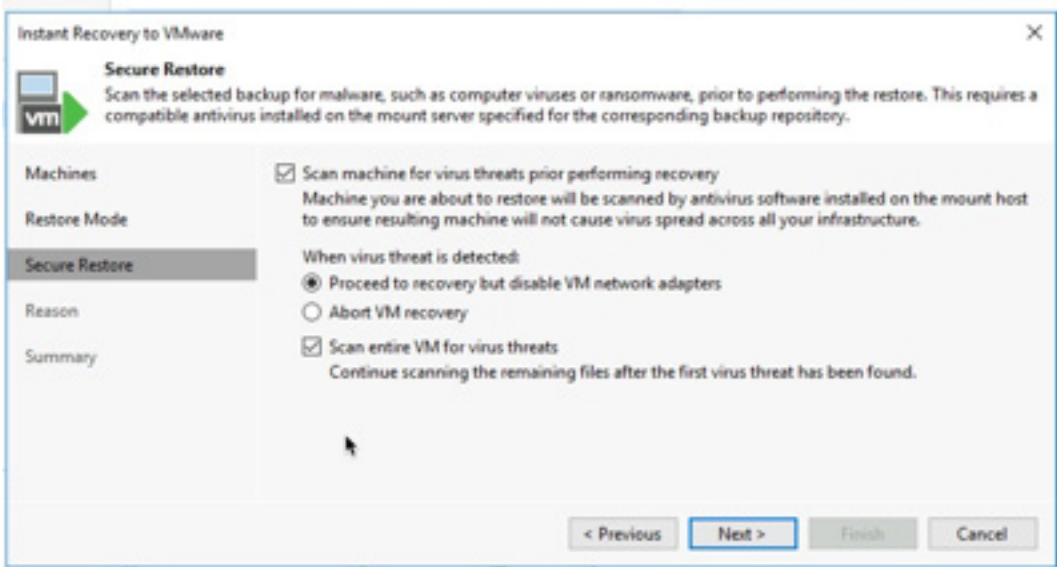


Figure 19. Disabling network adapters.



Improving Veeam Backup and Recovery Performance with Snapshots

Hardware snapshots are a very effective way to improve data protection tasks, especially in high transactional environments. FlashArray integration with the Veeam Universal API effectively improves backup and recovery times. The Veeam orchestration layer manages consistency with the application. Snapshot creation orchestrates directly by reading the snapshot data into the repository before offloading backup workloads from production. Similarly, if hardware snapshots are enabled during recovery as a second copy, all recovery options are also available through hardware snapshots, for example, Instant VM Recovery.

How to Enable Snapshots

Enabling hardware snapshots as a second copy can be achieved from within the Backup Job Configuration wizard (Figure 20). Under “Configure secondary backup destination for this job” > Next > Click on “Add” and select “Pure Storage Snapshot” (Figure 21). The default hardware snapshot retention is 14 days, which is recommended.

Edit Backup Job [VM Backup]

Storage
Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.

Name
Backup proxy: Automatic selection [Choose...]

Virtual Machines
Backup repository: FlashArray-C-2T-Repo (Created by TSW-VEEAM-BR\Administrator at 2/5/2021 10:2) [Map backup]

Storage
Retention policy: 2 restore points [i]

Secondary Target
☐ Keep certain full backups longer for archival purposes [Configure...]
GFS retention policy is not configured

Guest Processing
☒ **Configure secondary backup destinations for this job**
Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Schedule
Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings. [Advanced]

Summary
< Previous Next > Finish Cancel

Figure 20. Enabling hardware snapshots as a second copy.

Edit Backup Job [VM Backup]

Secondary Target
Use the backups produced by this job to satisfy backup requirement by archiving backups to tape, or efficiently creating remote backups and replicas over WAN.

Name
Secondary destination jobs:

| Name | Type | Free |
|------|------|------|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Virtual Machines
Jobs
Pure Storage Snapshot [Remove]

Storage

Secondary Target

Guest Processing

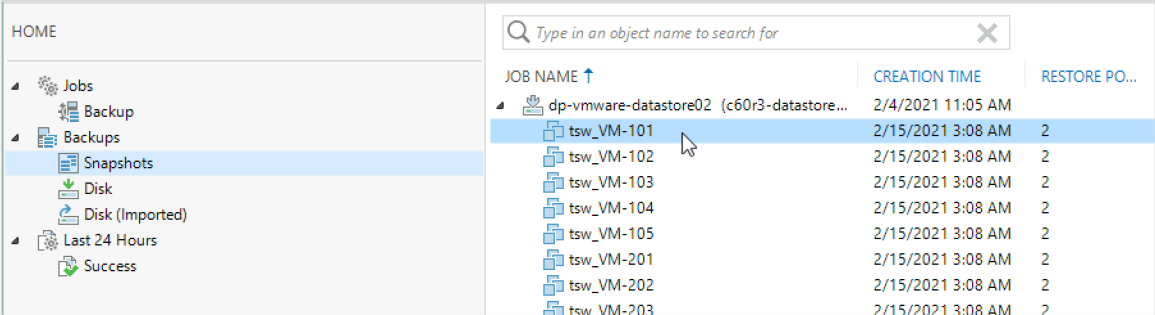
Schedule
THROU

Figure 21. Editing the Backup Job.



How to Recover with Snapshots

Once the backup job is run, a new shortcut to “Snapshots” is created. Inside the “Snapshots” folder, you’ll see a list of all VMs included in the hardware snapshots—including a date/time stamp of the latest snapshot—as well as how many restore points are available (Figure 22).



The screenshot shows the Veeam Backup & Replication console. On the left, the 'Snapshots' folder is selected under 'Backups'. The main pane displays a table of VMs with columns for Job Name, Creation Time, and Restore Points.

| JOB NAME ↑ | CREATION TIME | RESTORE PO... |
|--|-------------------|---------------|
| dp-vmware-datastore02 (c60r3--datastore... | 2/4/2021 11:05 AM | |
| tsw_VM-101 | 2/15/2021 3:08 AM | 2 |
| tsw_VM-102 | 2/15/2021 3:08 AM | 2 |
| tsw_VM-103 | 2/15/2021 3:08 AM | 2 |
| tsw_VM-104 | 2/15/2021 3:08 AM | 2 |
| tsw_VM-105 | 2/15/2021 3:08 AM | 2 |
| tsw_VM-201 | 2/15/2021 3:08 AM | 2 |
| tsw_VM-202 | 2/15/2021 3:08 AM | 2 |
| tsw_VM-203 | 2/15/2021 3:08 AM | 2 |

Figure 22. List of all VMs included in the hardware snapshots, including date/time stamps.

You achieve recovery by selecting which VM(s) you want to recover. Figure 23 shows an option to perform Instant VM Recovery.

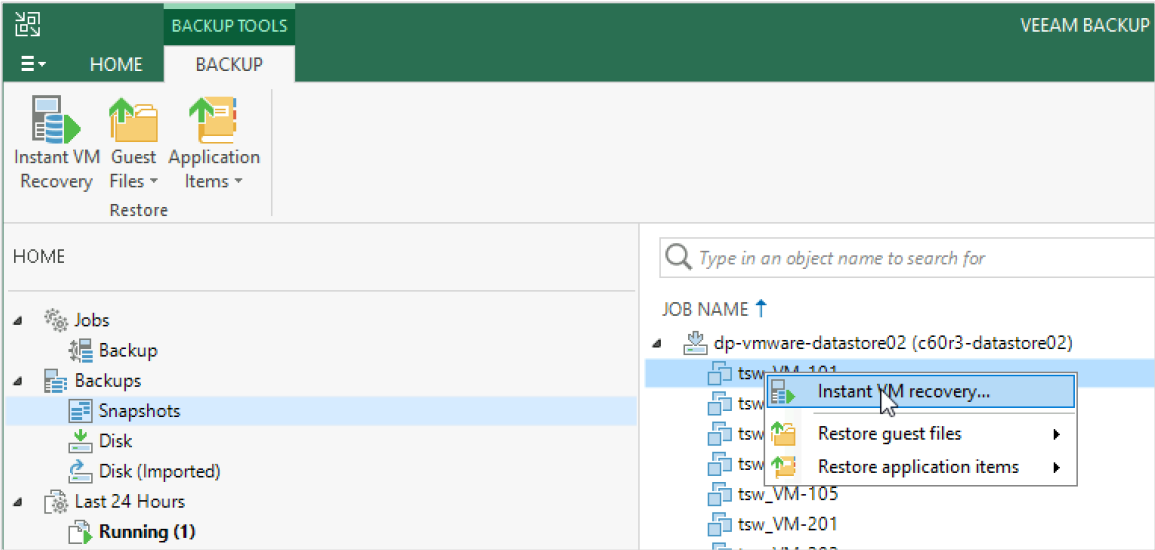


Figure 23. Instant VM Recovery.

Clicking on the “Point” button will allow you to select which recovery point from which you want to recover.

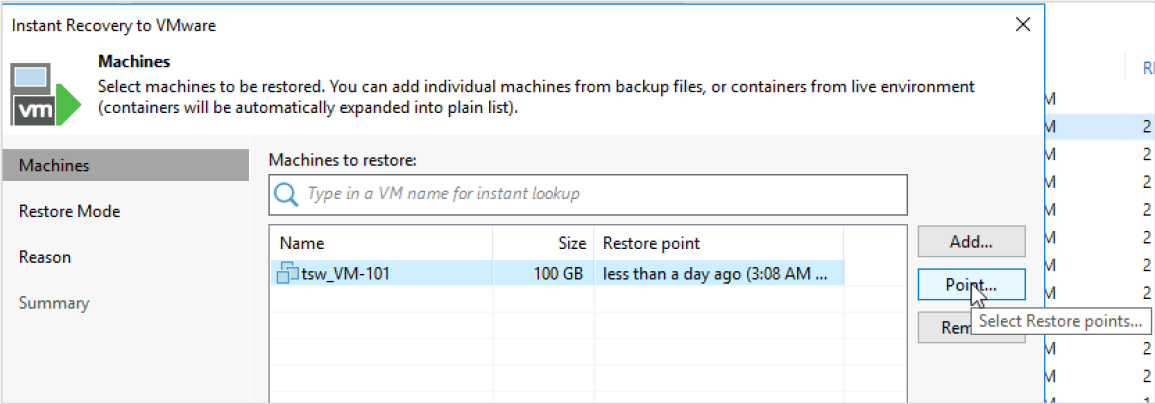


Figure 24. Selecting the VM for recovery.



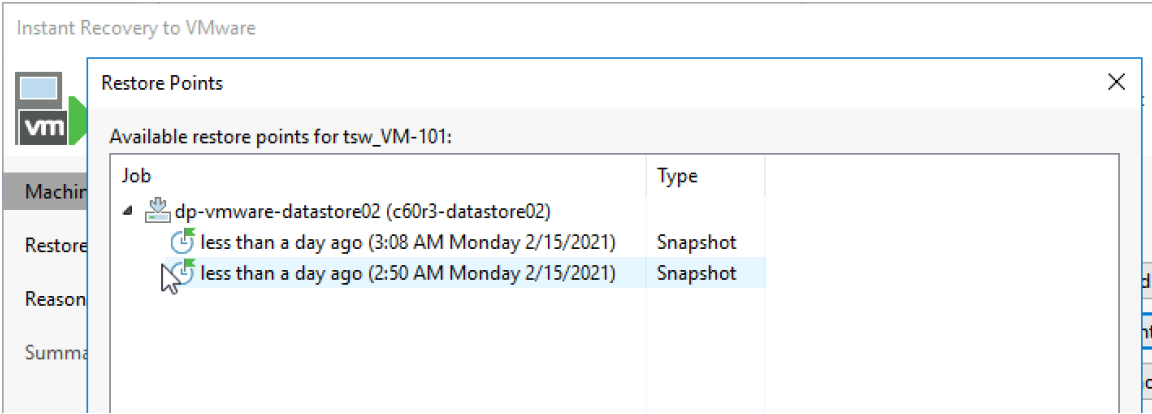


Figure 25: Selecting the recovery point.

This union of orchestrated hardware snapshots and Veeam backups provides the agility and responsiveness to deliver the Always-On infrastructure availability.

Conclusion

Modern IT business objectives require continuous data availability. Organizations need to recover from data, application, and system loss with minimal or zero downtime. That is vastly different from yesterday's backup solutions built on legacy architectures.

Achieving these objectives requires modern data protection software and fast storage media. Until FlashArray//C, data protection solutions using traditional disk were forced to compromise performance and features for an economically viable solution. Today, with FlashArray//C, you don't have to compromise dollars per GB, performance, or ransomware mitigation features like SafeMode. FlashArray//C offers an NVMe, all-flash experience at spinning disk economics. The combination of Veeam Backup & Replication and FlashArray//C with SafeMode not only provides needed agility and performance but adds resilience and streamlined recovery following ransomware attacks, malware onslaught, viruses, and administrative mistakes.



Additional Resources

Next Steps

- Learn more about [FlashArray//C](#).
- Download the FlashArray//C [User Guide](#) (login required).
- Learn more about [Pure and Veeam solutions](#).

Supporting Information

- [Veeam Backup & Replication User Guide for VMware vSphere](#).
- [Veeam Backup & Replication Best Practices](#)
- [Veeam and Pure Storage Integrated Deployment Guide](#)
- [U.S. Justice Department Cybersecurity and Ransomware related articles](#)
- [Cybersecurity Ventures Cost of Ransomware](#)

¹ [Global Ransomware Damage Costs Predicted to Reach \\$20 Billion by 2021](#), Steve Morgan, *Cybersecurity Magazine*

©2021 Pure Storage, the Pure P Logo, and the marks on the Pure Trademark List at <https://www.purestorage.com/legal/productenduserinfo.html> are trademarks of Pure Storage, Inc. Other names are trademarks of their respective owners. Use of Pure Storage Products and Programs are covered by End User Agreements, IP, and other terms, available at: <https://www.purestorage.com/legal/productenduserinfo.html> and <https://www.purestorage.com/patents>

The Pure Storage products and programs described in this documentation are distributed under a license agreement restricting the use, copying, distribution, and decompilation/reverse engineering of the products. No part of this documentation may be reproduced in any form by any means without prior written authorization from Pure Storage, Inc. and its licensors, if any. Pure Storage may make improvements and/or changes in the Pure Storage products and/or the programs described in this documentation at any time without notice.

THIS DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. PURE STORAGE SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Pure Storage, Inc.
650 Castro Street, #400
Mountain View, CA 94041

purestorage.com

800.379.PURE

