netgo techpaper

Cyber-Resilienz

Ransomware Protection

mit Veeam v12 and HPE StoreOnce

Ransomware Protection

mit Veeam v12 and HPE StoreOnce

Datenwachstum, Verfügbarkeit, Verteilte Systeme – viele Unternehmen stehen vor großen Herausforderungen, wenn es um ihre Daten geht. Besonders, da Angriffe auf Infrastrukturen stetig zunehmen und Administratoren vor die Frage stellen, wie die kontinuierlich wachsenden Datenmengen effizient und gut geschützt abgelegt werden können.

Veeam hat mit der Version 12 der Data Plattform viele Neuerungen gebracht, die das Ziel verfolgen, Daten möglichst sicher vor Angreifern abzulegen. Eine dieser Neuerungen betrifft die Integration der StoreOnce Backup Appliances, die aus der engen Zusammenarbeit von HPE und Veeam entstanden ist.

Data Immutability:
HPE + Veeam = Better together

Schon lange hat sich die 3-2-1-1-0 Regel in der Sicherungsstrategie bewährt. Die Empfehlung lautet, mindestens drei Kopien der Daten auf mindestens zwei verschiedenen Medien Aufzubewahren und dabei mindestens eine der Kopien an einem anderen Standort aufzubewahren sowie eine Kopie offline oder immutable. Die Anfertigung und Ablage dieser Backups beruhigt zwar das Gewissen – aber damit ist die Datensicherung noch lange nicht abgeschlossen: Die Backups sollten in regelmäßigen Abständen nach einem Standardverfahren geprüft werden, damit sichergestellt ist, dass diese auch fehlerfrei sind.

Immutable Backups, also Backups die unveränderlich und nicht löschbar aufbewahrt werden, sind ein wichtiger Teil der Backup-Strategie. Denn Angreifer können ansonsten Backups ebenso angreifen wie produktive Daten. Durch das sich stetig verändernde Verhalten der Cyberkriminellen ist es zudem wichtig, Backups über einen längeren Zeitraum hinweg aufzubewahren – schließlich lässt sich oftmals nicht sagen, wie lange ein Angreifer sich bereits im System aufhält. Oftmals vergehen bis zu 90 Tage, bis Anwender bemerken, dass sich Unbefugte in der Infrastruktur aufhalten.

In dem Fall ist es natürlich ungünstig, wenn Backups dann lediglich für einen Monat aufbewahrt werden und es keine sauberen Wiederherstellungspunkte gibt. Eine Lösung für die sichere Aufbewahrung bietet Veeam in Verbindung mit HPE.

What’s new with HPE StoreOnce and Veeam v12?

Mit erscheinen der Version 12 ist die Möglichkeit dazugekommen, Backups auf HPE StoreOnce Systemen ebenfalls Immutable, also in diesem Fall unlöschbar, aufzubewahren.

HPE StoreOnce Systeme zeichnen dabei verschieden Vorteile aus:

- Anbindung via Catalyst Protocol (Ethernet and FC): Der Zugriff auf die Backup-Stores ist nur über die Catalyst API möglich und für normale Clients oder Server unsichtbar
- Deduplizierung: Die bewährte Source-Side Deduplizierung der Catalyst Stores bietet eine Bandbreitenschonende und Effiziente Aufbewahrung der Backups, sodass diese auch langfristig und Platzsparend aufbewahrt werden können
- Skalierung: HPE StoreOnce Appliances gibt es von klein bis groß, virtuell, in der Cloud und als Hardware. Der individuelle Bedarf im Hinblick auf Kapazität und Datendurchsatz bestimmen das einzusetzende Modell
- Ransomware Protection: Dual Authorization sowie Objekt-Level Immutability

Für Nutzer von StoreOnce Systemen ab Generation 4 kann diese Funktionalität in Verbindung mit Veeam v12 ohne weitere Anschaffung genutzt werden. Dafür müssen lediglich einige Voraussetzungen erfüllt werden:

- StoreOnce OS ab 4.3.2
- Dual Authorization muss aktiviert und konfiguriert sein
- Die Maximale Beibehaltung der vom ISV gesteuerten Unveränderbarkeit von Daten muss konfiguriert sein
- Forward Incremental Backups oder GFS Backups müssen genutzt werden

Anschließend ist eine Aktivierung für neue oder noch aktive Backup-Ketten möglich.

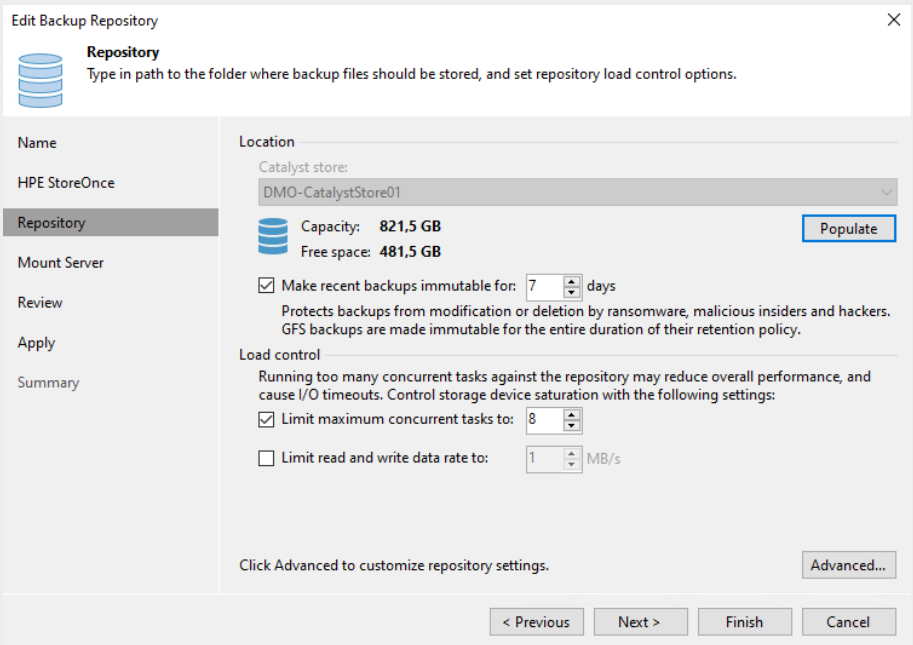

Bild: Immutability aktivieren

Durch das Aktivieren der Immutability-Funktionalität lassen sich Backups für den eingestellten Zeitraum der Aufbewahrung nicht mehr löschen. Lediglich die Metadaten, die sich mit jedem Backuplauf ändern, können gelöscht werden. Die Backups bleiben aber wiederherstellbar.

Die Immutability lässt sich dabei in der Backup Übersicht prüfen:

Files:

Name	Data Size	Backup Size	Deduplication	Compression	Date	Immutable Until
VM-MGMT-VC01.vm-84021D2023-08-03T233016_D62F.vib	9,85 GB	9,86 GB	1,0 x	1,0 x	03.08.2023 23:30:16	11.08.2023

Bild: Immutability

Und auch der Härtetest zeigt, dass die Backups sich nicht löschen lassen:

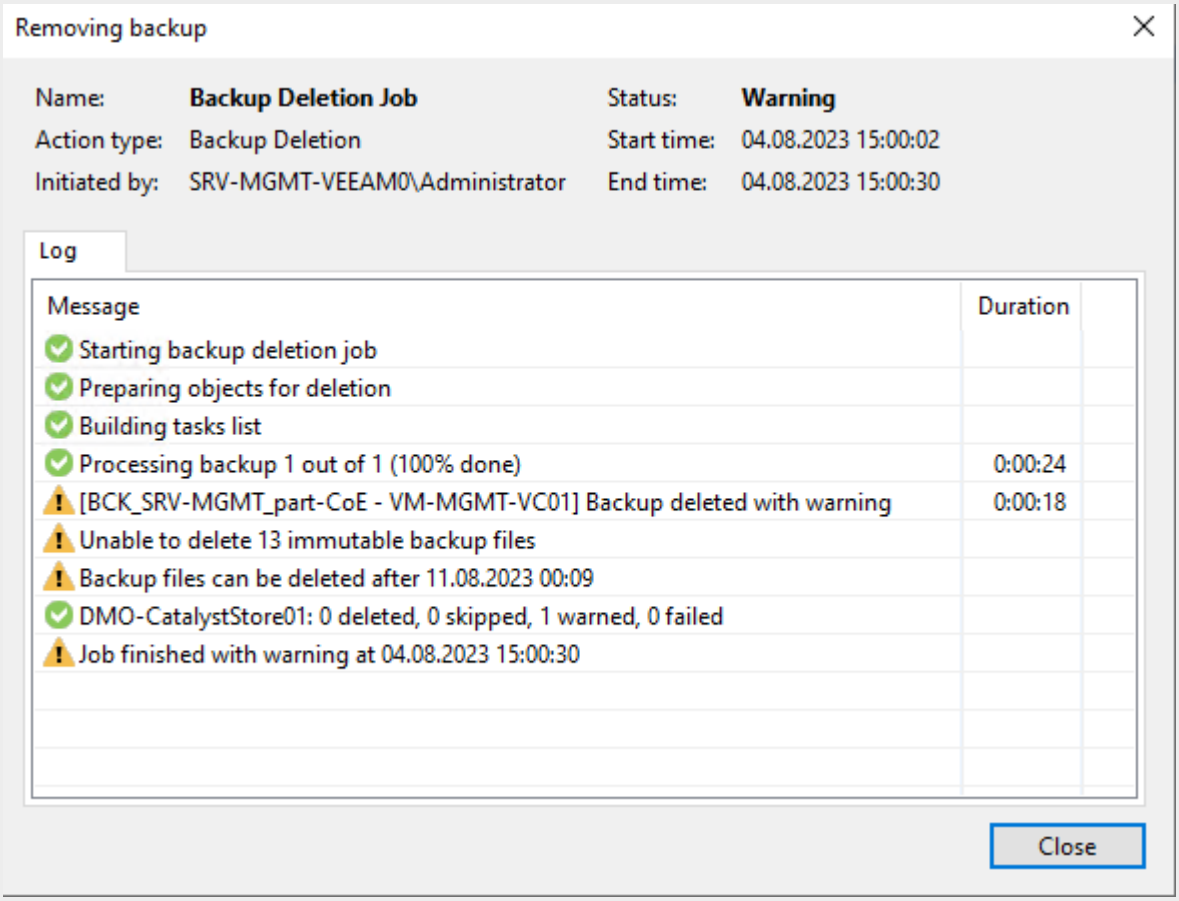

Bild: Löschen vereitelt

Durch die Nutzung der GFS-Aufbewahrung können Backups auch unabhängig von der primären Kette für Monate oder gar Jahre immutable aufbewahrt werden. Hier spielt die StoreOnce und oder ihre effiziente Deduplizierung ihre Karten voll aus.

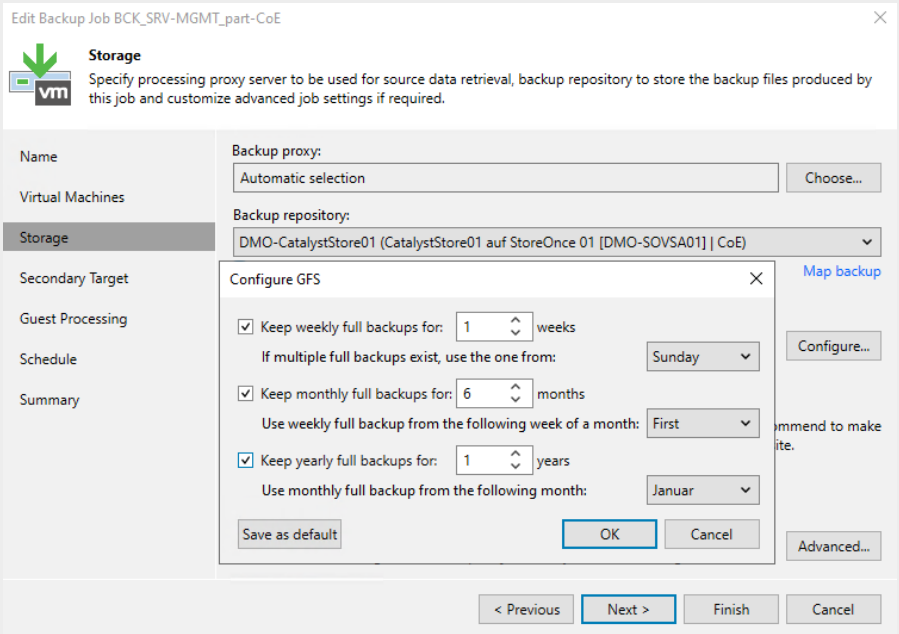

Bild: GFS Optionen

Damit auch bei Angriffen auf die StoreOnce selbst nicht der gesamte Catalyst Store mitsamt aller Backups gelöscht werden kann, gibt es für destruktive oder kritische Vorgänge auf dem System den Compliance Modus, welcher sich durch Dual Authorization aktivieren lässt. Dual Authorization funktioniert dabei wie ein Vier-Augen-Prinzip, was bedeutet, das immer zwei Benutzer benötigt werden, um kritische Vorgänge wie Löschvorgänge oder das Herabsetzen der ISV-Aufbewahrung zu verändern.

Im Einsatz bedeutet das, wenn ein Administrator – oder ein Angreifer mit Administrator Credentials – sich an der StoreOnce zu schaffen macht und versucht den gesamten Backup-Bestand zu löschen, wird dafür ein weiterer Benutzer benötigt, der diese Änderungen bestätigt. Werden die Änderungen nicht bestätig, werden diese nicht durchgeführt. Dual Authorization geht dabei ein Stück weiter als Multi-Faktor-Authentifizierung, wo eine einzelne Person in der Lage wäre alle Daten alleine zu löschen.

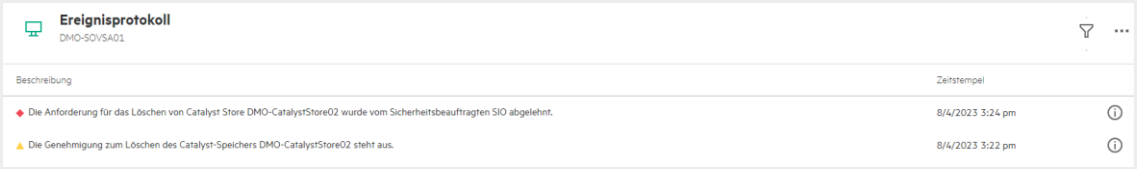

Bild: Löschvorgang abgelehnt

Durch die neuen Funktionalitäten, lassen sich Backups also nicht mehr nur lange sondern auch gut geschützt vor potentiellen Angreifern aufbewahren.

HPE und Veeam können dabei auf eine lange Innovationshistorie zurückschauen, die nun seit zwölf Jahren besteht. Nahezu jedes HPE Storage-Produkt ist nativ in Veeam integriert, umso unter anderem auch Storage-Snapshots effektiv zu orchestrieren und Backups anfertigen zu können.

Welche Integrationen für Sie in Frage kommen, bestimmen wir gerne im Rahmen unserer Veeam-Workshops mit Ihnen, damit Ihre Daten bestmöglich
abgesichert sind.