Whitepaper
Veeam as a Service
Uptime Backup auf Basis Veeam B&R

1. Funktionsweise

Uptime IT bietet Backuplösungen basierend auf Veeam Backup & Replication oder IBM Spectrum Protect an. In diesem Whitepaper wird die auf Veeam B&R basierende Lösung beschrieben.
Veeam Backup & Replication ist eine plattformübergreifende Lösung zur Datensicherung und Replikation kompletter virtueller Maschinen (VMs). Dazu gehört auch die Wiederherstellung der VMs, deren Konfiguration, virtueller Festplatten, einzelner Dateien oder Anwendungsobjekte.
Zentraler Bestandteil des Systems ist die Serverkomponente (Veeam Server), welche Dienste zur Datensicherung anbietet und die Sicherungen auf den Speichersystemen verwaltet. Die Verwaltungsinformationen werden in einer zentralen Datenbank gespeichert.
Auf den VMs, deren Daten gesichert werden sollen, müssen keine speziellen Clientkomponenten installiert werden (Agentless Backup).

Die folgenden Funktionen von Veeam B&R können in Uptime Backup as a Service genutzt werden:

- Sicherung kompletter VMs für alle von VMware unterstützte Betriebssysteme.
- Schnappschuss-Technik (VMware tools quiescence, zusätzlich VSS für Windows) für geringstmöglichen Einfluss auf den laufenden Betrieb.
- Deduplizierung und Kompression je Backup-Job zur Verringerung des Backup-Volumens.
- Applikationsspezifische Sicherungsprozessierung für unterstützte Windows-Systeme und -Anwendungen (Active Directory, SQL Server, Exchange Server, Sharepoint).
- Backup-Verfahren Forever Incremental. Dabei werden nach der erstmaligen Vollsicherung nur noch inkrementelle Sicherungen durchgeführt, d.h. nur geänderte Datenblöcke der VM gesichert. Die Änderungen zur vorherigen Sicherung werden in separaten Dateien gespeichert (forward incremental backup file). Nach Ablauf der Aufbewahrungsfrist wird die Vollsicherung mit der ältesten inkrementellen Sicherung zu einer neuen Vollsicherungsdatei zusammengeführt.
- Kopieren der Sicherungen an einen zweiten Standort zum Zwecke des Katastrophenschutzes.
- Replikation von VMs auch in schneller Folge (near Continuous Data Protection) an zweiten Standort um schnelles Wiederanlaufen des Betriebes nach einem Rechenzentrumsausfall zu ermöglichen.
- Wiederherstellung kompletter VMs für alle von VMware unterstützte Betriebssysteme.
- Wiederherstellung einzelner VM-Dateien (Konfiguration, Logdateien usw.)
- Wiederherstellung einzelner virtueller Festplatten.

2. Struktur

Uptime Backup as a Service mit Veeam B&R unterliegt folgender Struktur:

- Uptime
  - RZ-Standort
    - Veeam Server
      - Sicherungs-Job
        - Aufbewahrungsregeln
        - Zeitplan
        - Sicherungsobjekte (alle VMs in einem Container, einzelne VMs)
      - Kopier-Job
        - Aufbewahrungsregeln
        - Zeitplan
        - Zu kopierende Objekte (alle oder ausgewählte VMs eines bereits bestehenden Backups)
      - Replikations-Job
        - Aufbewahrungsregeln
        - Zeitplan
        - Replikationsobjekte (alle VMs in einem Container, einzelne VMs)

3. Planung einer Datensicherung

3.1. Standardsicherung

Der Standardfall ist eine einmal tägliche Sicherung aller vApps mit den VMs der dem Kundenvertrag zugeordneten Uptime Cloud Organisation mit Ausnahme der vShield Edge Appliances, die vom VMware Cloud Director verwaltet werden. (Die Uptime Cloud-Konfiguration, d.h. Benutzer, Rechte, Firewall-Regeln sowie Mediendateien und vApp-Templates in den Katalogen können mit Veeam B&R nicht gesichert werden.)
Die Sicherung findet in einem Zeitfenster von 22:00 bis 06:00 Uhr statt.
Tägliche Sicherungen sowie Sicherungen von VMs, die vom Host gelöscht wurden, werden 14 Tage lang aufbewahrt.
Es wird VMware tools quiescence verwendet, um eine konsistente Sicherung zu erhalten. (Diese sorgt dafür, dass sich Dateisysteme nicht ändern, während der Schnappschuss für die Sicherung erstellt wird. Dies

schließt auf unterstützten Windows-Systemen einen VSS-Schnappschuss mit ein.)
Es wird VMware Changed Block Tracking (CBT) verwendet, um kurze Backupzeiten zu gewährleisten.
Die Backups werden einmal täglich in das sekundäre Backup-Storage an einen zweiten RZ-Standort kopiert.

3.2. Individuelle Sicherung

Bezüglich der Aufbewahrungszeit ist es Uptime IT nicht möglich, eine einheitliche Empfehlung zu geben, da die Anforderungen der Auftraggeber sehr unterschiedlich sein können. Uptime IT bietet daher die Möglichkeit der individuellen Sicherung.
Mit der individuellen Sicherung kann der Auftraggeber seine eigene, individuelle Risiko-betrachtung als Grundlage verwenden und bei der Sicherung berücksichtigen. Zusammen mit Uptime IT können dann abweichende Aufbewahrungszeiten (z.B. als Vorsorge gegen über viele Monate schlafende Ransomware oder zu forensischen Zwecken), kürzere Sicherungszyklen (z.B. für Datenbanken), oder andere Sicherungsstrategien (GFS) definiert werden.
Sind auf Grund einer solchen Betrachtung Abweichungen vom Standardverfahren gewünscht, wird ein Backup Recovery Agreement (BRA) zwischen dem Auftraggeber und Uptime IT geschlossen. Darin werden folgende Dinge festgelegt:

- Welche VMs sollen gesichert werden?
- Welche virtuellen Festplatten der VMs sollen gesichert werden?
- Wann soll gesichert werden?
- Wie häufig soll gesichert werden?
- Wie viele Versionen einer gesicherten VM sollen aufbewahrt werden?
- Wie lange sollen die gesicherten VMs aufbewahrt werden, nachdem diese vom Host gelöscht wurden?
- Müssen bestimmte Dienste auf den VMs heruntergefahren werden, um eine konsistente Sicherung zu erreichen?
- Ist eine applikationsspezifische Prozessierung erforderlich, d.h. müssen z.B. Transaktionslogs nach erfolgreicher Sicherung abgeschnitten werden?
- Ist es erforderlich, Transaktionsprotokolle von SQL-Servern regelmäßig (z.B. stündlich) zu sichern?

Sind diese Festlegungen getroffen und die Konfiguration erfolgt, läuft der Sicherungsvorgang in der Regel automatisch ab. Abweichend hiervon sind manuelle Sicherungen möglich, die bei Uptime IT beauftragt werden können.

3.3. Wartungsslot

Bei der Planung der Datensicherung ist zu berücksichtigen, dass Uptime IT einen Zeitslot benötigt, um Wartungsarbeiten am System durchführen zu können oder Auswertungen vorzunehmen. Diese Arbeiten finden täglich zwischen 06:00 Uhr und 08:00 ohne weitere Ankündigungen statt. In dieser Zeit sind keine Sicherungen möglich und möglicherweise kein Restore.

4. Einrichtung einer Datensicherung

Um eine Standardsicherung für ein System einzurichten, ist es lediglich erforderlich, auf dem Veeam-Server einen Backup-Job einzurichten, der zu sichernde VMs, den Zeitplan sowie einige weitere Einstellungen festlegt. Dies wird von Uptime IT durchgeführt. Mit der Uptime IT Standardsicherung werden auch VMs gesichert, die erst zu einem späteren Zeitpunkt hinzugefügt wurden.
Auf den zu sichernden VMs muss lediglich eine aktuelle Version der VMware Tools installiert werden. Dies wird vom Auftraggeber ausgeführt.
Während der ersten Sicherung durch Veeam B&R dürfen für die zu sichernde VM keine VMware-Schnappschüsse existieren, damit CBT für die VM eingeschaltet werden kann.
Im Falle einer individuellen Sicherung ist es bei Verwendung einer applikationsspezifischen Prozessierung erforderlich, Zugangsdaten für das Gastsystem der zu sichernden VM auf dem Veeam-Server zu hinterlegen. Müssen z.B. Dienste heruntergefahren werden, um eine konsistente Sicherung zu erreichen, wird ein Pre-Freeze- und Post-Thaw-Script auf dem Veeam-Server hinterlegt (siehe auch Kapitel 5 „Ablauf einer Datensicherung“).

5. Ablauf einer Datensicherung

Eine automatische Datensicherung läuft in diesen Schritten ab:

1. Ist der im Zeitplan festgelegte Zeitpunkt erreicht, wird der Sicherungsjob sofort gestartet, falls die maximale Anzahl parallel laufender Jobs noch nicht erreicht ist, im anderen Fall in die Warteschlange eingereiht.
2. Eine Liste der zu sichernden VMs wird erstellt. Diese kann sich bei jeder Sicherung ändern, falls ein VMware-Container (Ordner, Resource Pool, Storage, Data Center) als Sicherungsquelle festgelegt ist.
3. Die VMs werden der Reihe nach abgearbeitet:
   a. Wenn im Backup-Job „CBT verwenden“ eingeschaltet ist (Standardeinstellung), dann CBT für die VM einschalten. Voraussetzung hierfür ist, dass aktuell keine VMware-Schnappschüsse für die VM existieren.
   b. Die VM wird mittels VMware Tools „eingefroren“. Dabei wird zuerst ein evtl. auf dem Veeam-Server hinterlegtes Pre-Freeze-Script ausgeführt. Auf Windows-Systemen wird hier ein VSS-Schnappschuss angelegt.
   c. Ein VMware-Schnappschuss wird erstellt.
   d. Die VM wird mittels VMware Tools wieder „aufgetaut“. Danach wird ein evtl. auf dem Veeam-Server hinterlegtes Post-Thaw-Script ausgeführt. Auf Windows-Systemen wird hier der VSS-Schnappschuss wieder aufgelöst.
   e. Die Konfigurationsdateien der VM werden gesichert.
   f. Die virtuellen Festplatten der VM werden gesichert soweit im Backup-Job festgelegt

(Standard ist die Sicherung aller Festplatten). Dabei wird direkt über das SAN auf die Daten zugegriffen und CBT genutzt (bei Standardeinstellung). Die Daten werden dedupliziert und komprimiert (bei Standardeinstellung).

g. Der VMware-Schnappschuss wird wieder aufgelöst.

4. Die Vollsicherung wird mit der ältesten inkrementellen Sicherung zu einer neuen Vollsicherungsdatei zusammengeführt, sofern die Höchstanzahl aufzubewahrender Versionen überschritten ist.
5. Ein Bericht wird erstellt und per E-Mail an Uptime IT verschickt.

Sollte während der Sicherung das Ende des Zeitfensters erreicht werden, so wird der Job abgebrochen und als fehlerhaft berichtet.
Zeitlich unabhängig von der Datensicherung läuft einmal täglich ein Job, der die Backups vom primären in den sekundären Backup-Storage kopiert.

6. Aufbewahrung gesicherter VMs

Für die gesicherten VMs werden Aufbewahrungsregeln in jedem Backup-Job definiert. Hier wird festgelegt, wie viele Backup-Versionen und wie lange Backups gelöschter bzw. inzwischen von der Sicherung ausgenommener VMs aufbewahrt werden sollen.
Die Datenbereiche für gelöschte VMs werden aus den bestehenden Backupfiles nach Ablauf der Aufbewahrungsfrist aus technischen Gründen nicht entfernt, jedoch als frei markiert. Daraus folgt, dass sich das Datenvolumen in diesem Fall nicht oder nur geringfügig vermindert. Die freien Bereiche werden wiederverwendet, bevor sich das Backupfile vergrößert.

7. Wiederherstellungsszenarien

7.1. Wiederherstellung einer VM (Instant Recovery)

- Für die schnellstmögliche Wiederherstellung einer einzelnen VM.
- Kein Zugriff durch Uptime IT auf das Gastsystem notwendig.
- Nach der initialen Bereitstellung der VM auf dem Veeam-Server kann diese mit Performance-Einschränkungen bereits benutzt werden.
- Die Migration der VM in den Production Store kann dann im laufenden Betrieb erfolgen.

7.2. Wiederherstellung einer VM (Standardverfahren)

- Normale Wiederherstellung einer oder mehrerer VMs.
- Kein Zugriff durch Uptime IT auf das Gastsystem notwendig.
- Falls die Originalmaschine noch existiert, darf diese nicht laufen, sofern am Originalort bzw. -Netzwerk wiederhergestellt wird.
- Während der Wiederherstellung können die VMs nicht benutzt werden.

7.3. Wiederherstellung von VM-Dateien

- Wiederherstellung von VM-Dateien (z.B. Konfiguration).
- Kein Zugriff durch Uptime IT auf das Gastsystem notwendig.
- Während der Wiederherstellung am Originalort können die betroffenen VMs nicht benutzt werden.

7.4. Wiederherstellung von virtuellen Festplatten der VMs

- Kein Zugriff durch Uptime IT auf das Gastsystem notwendig.
- Die wiederhergestellten Festplatten können an andere VMs und/oder andere Geräte-IDs gehängt werden (z.B. als zweite Platte parallel zum Original).
- Während der Wiederherstellung können die Festplatten nicht benutzt werden.

7.5. Wiederherstellung einzelner Dateien

- Wiederherstellung einzelner Dateien direkt in das Gastsystem bei unterstützten Dateisystemen.
- Zugriff durch Uptime IT auf das Gastsystem notwendig.
- Voraussetzung ist der Netzwerkzugriff vom Veeam_Server aus auf das Gastsystem. Dazu sind ggf. vom Kunden entsprechende Firewallregeln zu definieren.

7.6. Wiederherstellung von applikationsspezifischen Elementen

- Wiederherstellung von Exchange-Elementen, SQL-Server-Tabellen, -Views, -Datenbanken, Active-Directory-Elementen
- Zugriff durch Uptime IT auf das Gastsystem notwendig.
- Voraussetzung ist der Netzwerkzugriff vom Veeam_Server aus auf das Gastsystem. Dazu sind ggf. vom Kunden entsprechende Firewallregeln zu definieren.
- Voraussetzung ist eine entsprechende applikationsspezifische Prozessierung.

8. Überwachung und Benachrichtigung

Jede geplante Datensicherung wird von Uptime IT darauf überwacht, ob der Sicherungsvorgang im geplanten Zeitfenster stattgefunden hat und ob es während der Sicherung Fehler gegeben hat. Sollte es zu Fehlern gekommen sein, wird an den Auftraggeber eine E-Mail mit Detailinformationen gesendet.
Uptime IT bemüht sich die Mails so zu versenden, dass sie zu Arbeitsbeginn des Auftraggebers vorliegt.
Wird eine definierte Sicherung erneut nicht durchgeführt, unabhängig von den Gründen, erhält der Auftraggeber bei jedem Auftreten eine entsprechende Benachrichtigung. Diese Benachrichtigungen sind vom Auftraggeber zu sichten, zu bewerten und bei Bedarf sind vom Auftraggeber Maßnahmen zu ergreifen oder

einzuleiten, um ggf. mit Hilfe von Uptime IT die Sicherung wieder in Gang zu setzen oder anders dafür zu sorgen, dass die Meldungen unterbleiben.
Ist eine Datensicherung fehlgeschlagen gibt es auch keinen Recovery Point.
Uptime IT hat wiederholt festgestellt, dass nicht behobene Fehler zu einem dramatischen Anstieg des gesicherten Datenvolumens führen können. Es liegt daher im natürlichen Interesse des Auftraggebers Fehler umgehend zu beheben, bzw. bei der Behebung mitzuwirken.
Uptime IT behält sich vor, Benachrichtigungen auszusetzen, wenn ein Fehler über einen Zeitraum von mind. 14 Tagen regelmäßig auftritt, aber nicht behoben werden kann, weil

- dieser nicht im Verantwortungsbereich von Uptime IT liegt,
- die Mitwirkung des Auftraggebers nicht erfolgt.

In diesen Fällen wird Uptime IT den Kunden auf das Ende der Benachrichtigungen aufmerksam machen. Uptime IT übernimmt keine Haftung, für Folgen, die aus dieser Situation entstehen wie z.B. ein erhöhtes Datensicherungsvolumen. Dies gilt ausdrücklich auch wenn durch diese Situation Benachrichtigungen zu schwerwiegenderen, behebbaren Fehlern unterbunden wurden und/oder eine andere Fehlerbehebung nicht stattfinden kann.
Die Anzahl der gesicherten VMs und das Datenvolumen für jeden Backup-Job werden täglich erfasst und gespeichert. Aus den gesammelten Daten wird monatlich eine Abrechnung erstellt.

9. Sicherheit

9.1. Zugriff auf Gastsysteme

Für die Standardsicherung wird kein Zugang zu den Gastsystemen der zu sichernden VMs benötigt.
Im Falle einer individuellen Sicherung werden bei Verwendung einer applikationsspezifischen Prozessierung Zugangsdaten für das Gastsystem der zu sichernden VM auf dem Veeam-Server hinterlegt.

9.2. Verschlüsselte Dateisysteme

Auf den zu sichernden VMs können verschlüsselte Dateisysteme verwendet werden, um unbefugten Zugriff auf die Daten zu verhindern, auch wenn sie mit Veeam B&R gesichert wurden. Uptime IT unterstützt derzeit keine verschlüsselten Backups.

10. Optimierung der Datensicherung

Um die Datensicherung zu optimieren, werden folgende Mechanismen eingesetzt:

10.1. Kompression

Zu sichernde Daten werden standardmäßig komprimiert, um das Sicherungsvolumen zu verringern.

10.2. Sicherung von geänderten Blöcken

Die Sicherung von geänderten Blöcken kann das Transfer- und auch das Sicherungsvolumen verringern. Bei der ersten Sicherung wird die VM komplett gesichert. Bei nachfolgenden Sicherungen werden nur die Blöcke der VM-Dateien gesichert, die sich seit der letzten Sicherung verändert haben. Hierzu wird bevorzugt das VMware Changed Block Tracking (CBT) verwendet. Fehlen die Voraussetzungen hierfür, so verwendet Veeam B&R seinen eigenen prüfsummenbasierten Mechanismus. Dieser muss jedoch alle Blöcke der VM-Datei lesen, was zu einer schlechteren Performance führt.

10.3. Deduplizierung

Bei der Deduplizierung werden identische Blöcke nur einmal je Backup-Job gesichert, um so das Sicherungsvolumen zu verringern.

10.4. Auslassung von ungenutzten Datenblöcken

Bei der Sicherung von Windows-VMs werden auf deren virtuellen Festplatten Datenblöcke ausgelassen, die nie genutzt wurden oder zu gelöschten bzw. Auslagerungsdateien gehören. Damit wird das Sicherungsvolumen nochmals verringert.

11. Unterstützte Funktionen

Sicherung und Wiederherstellung von VMs, VM-Dateien, Virtuellen Festplatten		
Alle in der Uptime Cloud unterstützten Betriebssysteme / Versionen		
Wiederherstellung einzelner Dateien		
Betriebssystem	*Dateisystem*	*Unterstützung*
Microsoft Windows	FAT, FAT32	V
	NTFS	VU
	ReFS	V
Linux	ext2, ext3, ext4	VU
	ReiserFS	V
	JFS	V
	XFS	V
	Btrfs	V
BSD	UFS, UFS2	-
Mac	HFS, HFS+	-
Novell OES	NSS	-
Solaris	UFS	-
	ZFS (except any pool versions of Oracle Solaris)	-

Applikationsspezifische Prozessierung und Wiederherstellung (ab Microsoft Windows Server 2008)	
Applikation	*Unterstützung*
Active Directory auf Microsoft Windows Server 2008	VU
Active Directory auf Microsoft Windows Server 2008 R2	VU
Active Directory auf Microsoft Windows Server 2012	VU
Active Directory auf Microsoft Windows Server 2012 R2	VU
Active Directory auf Microsoft Windows Server 2016	VU
Active Directory auf Microsoft Windows Server 2019	VU
Active Directory auf Microsoft Windows Server 2022	V
Microsoft Exchange 2010 SP1, SP2 oder SP3	V
Microsoft Exchange 2013	V
Microsoft Exchange 2016	VU
Microsoft Exchange 2019	VU
Microsoft SQL Server 2005 SP4	V
Microsoft SQL Server 2008 SP4	V
Microsoft SQL Server 2008 R2 SP3	V
Microsoft SQL Server 2012 SP4	V
Microsoft SQL Server 2014 SP3	V
Microsoft SQL Server 2016 SP2	VU
Microsoft SQL Server 2017	VU
Microsoft SQL Server 2019	VU
Microsoft SharePoint 2010	V
Microsoft SharePoint 2013	V
Microsoft SharePoint 2016	V
Microsoft SharePoint 2019	V
Oracle 11*	V
Oracle 12*	V
Oracle 18*	V
Oracle 19*	V
Oracle 21*	V

* Oracle Datenbanken jeweils gemäß Versionskompatibilitätsmatrix auf Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019, 2022, CentOS 5 oder neuer, RedHat 5 oder neuer, Oracle Linux 5 oder neuer. SUSE Linux Enterprise 11, 12, 15

Legende:
VU = offiziell von Veeam unterstützt und von Uptime IT getestet
V = offiziell von Veeam unterstützt und von Uptime IT bisher nicht getestet
- = offiziell von Veeam unterstützt, jedoch bei Uptime IT nicht verfügbar