VEEAM
IT JUST WORKS!™

Top 10 Best Practices für VMware-Datenverfügbarkeit

Eric Siebert
VMware vExpert

AVAILABILITY
for the Always-On Enterprise™

Zusammenfassung

Backups für virtuelle Maschinen (VMs) zu erstellen erscheint auf den ersten Blick vielleicht nicht besonders kompliziert. Wenn man allerdings ins Detail geht, stellt man fest, dass die Sache keineswegs so einfach ist, wie es zuerst aussieht. Die Sicherung physischer Speicher ist relativ unkompliziert: Man installiert einfach eine Agentensoftware auf einem Server und fügt sie zum Backup-Zeitplan hinzu. Ganz anders bei VM-Backups. Für wirklich effiziente Backups sind Techniken und Features nötig, die speziell für virtuelle Umgebungen entwickelt wurden. Werden VMs beim Backup und bei der Wiederherstellung wie physische Server behandelt, werden Ressourcen verschwendet und Backup-Fenster unnötig verlängert. Virtualisierung bringt umwälzende Veränderungen im Rechenzentrum mit sich. Daher sind auch völlig neue Verfahren und Methoden gefragt, um diese einzigartige Architektur und ihre Vorzüge optimal zu nutzen.

Die Virtualisierungsarchitektur bietet viele Vorteile für die Sicherung und Wiederherstellung von Servern. Sie verändert die herkömmlichen Techniken für Server-Backups mithilfe von Virtualisierungs-Features, mit denen verbesserte und effizientere Backup- und Wiederherstellungsprozesse realisiert werden. Zudem bietet sie mehr Flexibilität und Optionen zur Backup-Erstellung, VM-Wiederherstellung und Implementierung von Disaster Recovery (DR). In diesem Whitepaper geben wir Ihnen 10 Tipps, die Sie bei der Implementierung von Backup- und Wiederherstellungslösungen in einer virtuellen Umgebung unterstützen. Wir stellen geeignete Verfahren, Techniken und Konfigurationen vor und zeigen Ihnen, wie Sie Features von Veeam® Backup & Replication™ optimal nutzen, um von einer ganz neuen Dimension von Backup-Lösungen zu profitieren.

1 – Backup-Generierung auf VMware-Infrastrukturebene

Bei VM-Backups sollten Sie nicht an dem Verfahren festhalten, das Sie von der Sicherung Ihrer physischen Server gewohnt sind. Physische Server werden in der Regel über eine Agentensoftware gesichert, die im Gastbetriebssystem des Hosts installiert ist. Der Backup-Server stellt eine Verbindung zur Agentensoftware her, um die Daten daraus zu kopieren. Das funktioniert zwar auch mit einer VM, aber dann wird die Virtualisierungsebene völlig außer Acht gelassen. Die Backup-Erstellung ist damit ineffizient und wertvolle Host-Ressourcen werden verschwendet. Die beste Methode ist die Erstellung von VM-Backups auf Virtualisierungsebene. Dafür brauchen Sie eine Backup-Anwendung, die speziell für Virtualisierung entwickelt und optimiert wurde.

Eine solche Backup-Anwendung kann das Betriebssystem der VM beim Backup-Prozess völlig unberührt lassen. Stattdessen kann die Anwendung direkt eine Verbindung zum virtuellen Festplattendateisystem der VM herstellen und dieses sichern. So vermeiden Sie eine übermäßige Ressourcenauslastung in der VM und negative Auswirkungen auf die VM-Workloads während der Backup-Erstellung. Auch die Last auf die Ressourcen im Host kann so reduziert oder ganz vermieden werden. Sie können mehr VMs gleichzeitig sichern und dem Host stehen mehr Ressourcen für VM-

Workloads zur Verfügung. Zusätzlich sollte Ihre Backup-Lösung die VMware vSphere APIs for Data Protection nutzen, die Features wie Change Block Tracking integriert. Der Hypervisor kann damit tracken, welche Festplattenblöcke zwischen Backup- oder Replikationszyklen geändert wurden, um den Backup-Vorgang zu beschleunigen.

Mit der zunehmenden Virtualisierung in Unternehmen sollte Ihre Backup-Lösung diese Faktoren berücksichtigen und auf VMware-Infrastrukturebene ansetzen. Veeam Backup & Replication wurde von Grund auf speziell zur Sicherung von VMware vSphere-Umgebungen entwickelt. Es ist vollständig in VMware integriert und wird für maximale Effizienz auf der Virtualisierungsebene ausgeführt.

2 – Sicherheit für VMs und unternehmenskritische Daten mit der 3-2-1-Regel

Ihre VMs und vor allem Ihre Daten sind überlebenswichtig für Ihr Unternehmen. Ein Verlust kann nicht toleriert werden. Backups sind die Versicherungspolice für Ihre Daten: Genau wie bei Versicherungen hoffen Sie, dass Sie niemals darauf angewiesen sein werden. Wenn doch, müssen sie ordnungsgemäß funktionieren. Und Sie müssen sich darauf verlassen können, dass alles, was Sie brauchen, wiederhergestellt werden kann. Bei der Wiederherstellung von Daten sind Fehler schlicht nicht akzeptabel. Wenn Ihre primäre Wiederherstellungsmethode aus irgendeinem Grund fehlschlagen sollte, brauchen Sie einen Backup-Plan. Viele Unternehmen testen ihre Backups nicht standardmäßig auf Wiederherstellbarkeit. Im Falle eines Datenverlusts muss daher unter Umständen auf einen Plan B oder sogar Plan C zurückgegriffen werden.

Mit der 3-2-1-Regel stellen Sie sicher, dass mehrere Möglichkeiten zur Wiederherstellung Ihrer Daten zur Verfügung stehen. Sie schließen damit eine einzige zentrale Fehlerstelle aus. Auch für Ihr Backup sollte ein Backup-Plan existieren für den Fall, dass es zu einem Problem mit einem Backup kommt.
So funktioniert die 3-2-1-Regel:

- **Sie brauchen mindestens drei Kopien für Ihre Daten** – zusätzlich zu Ihren Primärdaten sollten Sie also über mindestens zwei zusätzliche Backups verfügen. Sollten Schwierigkeiten mit einem Backup auftreten, können Sie auf ein anderes zurückgreifen.
- **Speichern Sie die Kopien auf zwei unterschiedlichen Speichermedien** – so stellen Sie sicher, dass ein Ausfall eines der Geräte die Wiederherstellbarkeit nicht beeinträchtigt. Sie könnten beispielsweise ein Backup auf Band sichern und ein anderes auf Festplatte oder einem andere Zielspeicher, etwa bei einem Cloud-Provider, auf einem USB-Gerät, im SAN/NAS-Speicher etc.
- **Bewahren Sie eine Backup-Kopie extern auf** – das ist der wichtigste Punkt. Sie verhindern so, dass bei einer Katastrophe vor Ort, wie einem Brand oder einer Überschwemmung, auf einmal sowohl Ihre Primärdaten als auch Ihre Backup-Kopien verloren gehen. Sie können Bandsicherungen an einen externen Speicherort verschicken, Ihre Backups in einer anderen Niederlassung replizieren oder auch in der Cloud speichern. Egal für welche Lösung Sie sich entscheiden, ausschlaggebend ist die ausreichend große physische Entfernung zwischen Ihren Backups.

Veeam Backup & Replication ist dafür ausgerichtet, die 3-2-1-Regel einzuhalten und Ihre Backups abzusichern.

3 – Sicherheit Ihrer Backup-Daten und Schutz vor Verlust

Ihre Backups dienen im Grunde als Kopie Ihres kompletten Rechenzentrums. Alles ist an einem Ort gespeichert (bzw. an mehreren, wenn Sie nach der 3-2-1-Regel vorgehen). Und selbstverständlich müssen Sie auch beim Backup-Ziel dafür sorgen, dass Ihre Daten geschützt sind, egal wo sich dieses befindet. Häufig wird viel Aufwand für den Schutz von Hosts, Netzwerken, Betriebssystemen und Anwendungen betrieben. Die Sicherheit Ihrer Backups dürfen Sie dabei allerdings nicht vergessen. Was tun Sie zum Schutz Ihrer Backups, die sich häufig außerhalb Ihrer normalen abgesicherten Bereiche befinden? Wenn sich jemand Zugang zu Ihren Backups verschafft, ist es für den Eindringling unter Umständen kein Problem, VMs wiederherzustellen und auf Anwendungen und Daten zuzugreifen. Eine solche Bedrohung kann von innerhalb oder außerhalb Ihres Netzwerks ausgehen, da die Dateien einfach über Netzwerkverbindungen kopiert oder in winzigen USB-Geräten entwendet werden können. Auch wenn Ihre Daten zusätzlich extern aufbewahrt werden – ob an einem anderen Standort oder in der Cloud – müssen Sie sich darauf verlassen können, dass dort jemand für deren Schutz sorgt.

Sie müssen sich vergewissern, dass Ihre Sicherheitsstrategie auch Ihre Backup-Repositories einschließt, um das Risiko, dass Ihre Daten in fremde Hände gelangen, auf ein Minimum zu reduzieren. Dazu haben Sie viele Möglichkeiten. Die vielleicht einfachste ist die Verschlüsselung Ihrer Backup-Repositories über Ihre Backup-Anwendung. Sie könnten außerdem die Daten hardwarebasiert verschlüsseln. Dafür nutzen Sie eine Hardware, die eine solche Verschlüsselung unterstützt, was allerdings sehr teuer sein kann. Zudem sollten Sie den Zugriff auf Ihre Daten-Repositories auf die nötigen Administratoren beschränken und deren Zugriff regelmäßig einer Überprüfung unterziehen. Bei Backups außerhalb Ihres Rechenzentrums an einem Standort oder bei einem Cloud-Provider müssen Sie sich mit Ihrem Serviceprovider abstimmen, um sicherzustellen, dass ausreichende Sicherheitsmechanismen für Ihre Daten vorhanden sind.

Veeam Backup & Replication bietet eine integrierte End-to-End-AES-Verschlüsselung mit 256-Bit. Sie können so Ihre Backup-Dateien und Daten quellseitig (während des Backups), bei der Übertragung und im Backup-Speicher verschlüsseln. Damit bleibt Ihr Unternehmen vor negativen Schlagzeilen aufgrund von Sicherheitsverletzungen verschont.

4 – Optimale Nutzung richtlinienbasierter Maßnahmen für eine intelligentere Datensicherung

Entscheiden Sie sich im Zweifelsfall lieber für den komplizierten oder den einfachen Weg? Wenn Sie immer den komplizierten Weg einschlagen, dabei aber keine besseren Ergebnisse erzielen, verschwenden Sie Ihre Zeit und Ressourcen und laufen Gefahr, Fehler zu machen und entscheidende Schritte zu vergessen. Das virtuelle Rechenzentrum ist komplex und voller versteckter Herausforderungen, die den Managementaufwand erhöhen, die Effizienz beeinträchtigen und unerwünschte Probleme und Ausfallzeiten verursachen können. Automatisierung und Virtualisierungsumgebungen gehören praktisch untrennbar zusammen, denn durch automatisierte Verfahren wird die Einhaltung von Compliance-Anforderungen vereinfacht, während der Managementaufwand sinkt und alles so reibungslos wie möglich abläuft. Ein kluger vSphere-Administrator sucht stets nach einer einfacheren statt einer komplizierteren Lösung. Automatisierung oder richtlinienbasierte Kontrollmechanismen sind dafür die richtige Methode und sorgen zudem für Konsistenz.

Mit Storage Policy-Based Management (SPBM) – das in VMware vSphere 5.5 mit VSAN und später für Shared Storage in vSphere 6.0 mit Virtual Volumes (VVols) eingeführt wurde – können Sie Storage-Anforderungen für VMs basierend auf dem Storage-Array-Feature oder Hardwarefunktionalitäten festlegen. SPBM sorgt für Automatisierung und stellt sicher, dass VMs mit den Storage-Ressourcen konform gehen und auf diese abgestimmt sind. Zum Schutz der VMs können Sie Richtlinien basierend auf bestimmten RAID-Ebenen oder andere Storage-Verfügbarkeitsattribute einrichten, die Ihren SLA-Anforderungen entsprechen. Ein weniger bekanntes Feature von vSphere, das Sie bei einer einfacheren und strukturierteren Interaktion mit VMs unterstützt, ist das Tagging-Feature. Damit lässt sich die Gruppierung Ihrer VMs anpassen. Sie können benutzerdefinierte Tags erstellen und VMs zuweisen und so VMs basierend auf nicht standardmäßigen vSphere-Containern gruppieren (z. B. nach Anwendung, Rolle, Standort, Abteilung etc.). Diese Funktion können Sie zusammen mit VMware vSphere-Features oder Anwendungen Dritter verwenden, um Aktionen für VMs mit bestimmten Tags auszuführen.

Veeam Backup & Replication bietet vollständige Unterstützung für vSphere-Tags. Verwenden Sie sie beispielsweise zur Konfiguration von Backup-Jobs, so dass Sie Backup-Optionen für VMs je nach zugewiesenem Tag effizienter an Ihre Anforderungen anpassen können.

5 – Auswirkungen, die neue vSphere-Features und -Architekturen auf die Datensicherung haben

VMware entwickelt vSphere entsprechend der „Software-Defined Datacenter"-Vision kontinuierlich weiter. Es gibt immer wieder viele neue Features und Architekturen, die die Arbeitsweise mit vSphere grundlegend verändern. Das betrifft insbesondere den Storage-Bereich in vSphere. So hat VMware neue vSAN- und VVols-Storage-Architekturen eingeführt, die den herkömmlichen VMFS-Datastore ersetzen sollen. Auch der Netzwerkbereich wird stetig weiterentwickelt. Neueste Trends sind die neue NSX-Netzwerkarchitektur und Hyper-Converged Infrastrukturen wie EVO:Rail, mit denen Server, Storage und Netzwerke zu einem einzigen Appliance-Modell zusammengeführt werden sollen. Sie fragen sich vielleicht, wie sich all diese Änderungen auf Ihren Ansatz für Datensicherungslösungen auswirken. Sind die bestehenden Verfahren jetzt nicht mehr angemessen oder ineffizient? Welche Änderungen sollten Sie vornehmen, um sich diesen Neuerungen in vSphere anzupassen?

Seit vSphere 5.5 macht vSAN aus dem serverseitigen Speicher ein so genanntes „Shared Storage Array", das auf viele ESXi-Hosts verteilt werden kann. Da sich das SAN innerhalb eines Servers befindet, sind die Storage-Ressourcen dem Host viel näher, was positiv für die VM-Workloads ist, da der I/O-Pfad verkürzt wird. Die Kehrseite der Medaille ist jedoch, dass Backup-Prozesse zu einer erheblich höheren Host-Auslastung führen und damit die Performance insgesamt beeinträchtigen können. Zur möglichst effizienten Datenaufnahme ist außerdem eine veränderte Backup-Logik nötig. Dafür könnten Sie QoS-Steuerungen (Quality of Service) nutzen, die den Backup-Betrieb drosseln und sicherstellen, dass die Backup-Anwendung für vSAN konsistent ausgeführt wird. Mit den VVols in vSphere 6.0 sind in der neuen Storage-Architektur jetzt viele neue Komponenten zwischen Host und Storage-Array geschaltet, die allerdings für die meisten Backup-Anwendungen völlig transparent sind, d. h. von diesen nicht berücksichtigt werden. vSAN und VVols bieten außerdem einige neue APIs, so dass Sie sicherstellen müssen, dass Ihre Backup-Anwendung diese Features unterstützt und möglichst effizient nutzen kann.

Mit Veeam Backup & Replication genießen Sie die Gewissheit, dass Sie sowohl mit vSAN als auch mit VVols optimal aufgestellt sind. Die neuesten vSphere APIs werden effizient genutzt und in die neuen Storage-Architekturen integriert, so dass Sie bestmöglich von der erweiterten intelligenten Backup-Logik und der optimalen virtuellen Proxy-Auswahl profitieren.

6 – So nutzen Sie die Cloud optimal als Teil Ihrer Datensicherungsstrategie

Die Cloud dient als externe Erweiterung Ihres virtuellen Rechenzentrums, die Sie optimal als Alternative zu allem, was intern ausgeführt wird, nutzen können. Bei der Datensicherung kann die Cloud als externes Repository dienen. Sie kommen so ohne ein eigenes Wiederherstellungsrechenzentrum aus, dessen Verwaltung extrem teuer sein kann. Die Cloud empfiehlt sich in den meisten Fällen zwar nicht als primäres Speicherziel für Backups, kann aber eine bestehende Primär-Backup-Lösung in einem Layer-Modell perfekt ergänzen, da sie die Erstellung mehrerer Kopien für Ihre Backups unterstützt (3-2-1-Regel). Die meisten Backup- und Cloud-Anbieter ermöglichen eine sehr einfache Integration zwischen internen Rechenzentren und Anwendungen einerseits und Cloud-basierten Infrastrukturen und Services andererseits, so dass Sie unkompliziert Ihre Daten in die Cloud und zurück übertragen können.

Bei Ihrer Cloud-Strategie sollten Sie kurzfristige Backups, die intern vor Ort gespeichert, sowie langfristige Backups, die extern in der Cloud aufbewahrt werden, berücksichtigen. Statt die Cloud nur als statischen Speicher für Ihre VMs zu nutzen, könnten Sie sie außerdem als aktiven Speicher, d. h. als Replikationsziel einsetzen, aus dem Sie Ihre VMs bei Bedarf auch starten können. Die Cloud bietet viele Möglichkeiten und ist eine perfekte Ergänzung Ihrer Datensicherungsstrategie. Denken Sie bei der Wahl eines Cloud-Providers daran, dass sich die Kosten in der Regel nach der Ressourcennutzung richten. Für Sie sollte klar nachvollziehbar sein, welche Kosten durch die Backup- und Wiederherstellungsverfahren anfallen, die ressourcenintensiv sein können. Relevant sind dabei vor allem die Ingress- und Egress-Kosten (für ein- bzw. ausgehenden Datenverkehr). Die Übertragung Ihrer Daten in die Cloud kann beispielsweise relativ preiswert sein, während die Rückübertragung großer Datenmengen u. U. recht teuer ist.

Unabhängig davon, für welche Cloud-Strategie Sie sich entscheiden, bietet Ihnen Veeam Cloud Connect eine vollständig integrierte, schnelle und sichere Möglichkeit zur Sicherung und Wiederherstellung in die Cloud und aus der Cloud. Ohne die Kosten und die Komplexität für die Verwaltung einer externen Infrastruktur können Sie so Ihre Backups in einem externen Speicher sichern.

7 – Zuverlässige Einhaltung aller Anforderungen zum Schutz Ihrer geschäftskritischen Anwendungen

Beim Schutz Ihrer geschäftskritischen Anwendungen können Sie sich keinerlei Pannen erlauben. Schließlich kann jeder einzelne Fehler extrem kostspielig sein. Sie müssen alle nötigen Vorkehrungen zur Sicherung Ihrer Anwendungen treffen, um jederzeit eine 100 %ige Wiederherstellbarkeit zu gewährleisten. Besonders heikel sind Backups und Wiederherstellungen in Verbindung mit Datenbank- und E-Mail-Anwendungen, denn hier sind ganz spezielle Anforderungen einzuhalten. Einer der kritischsten Schritte im Backup-Prozess ist das so genannte „Quiescing“ (Stilllegung). Diese Funktion stellt sicher, dass die in einer VM ausgeführten Daten und Anwendungen für das Backup in einen korrekten Zustand versetzt werden, so dass die Wiederherstellung später keine Probleme macht. Das Quiescing versetzt eine VM temporär in den Ruhezustand. Alle ausstehenden Schreibvorgänge und Daten im Arbeitsspeicher können so auf Festplatte geschrieben werden, bevor das Backup startet. Erfolgt das VM-Backup ohne vorheriges Quiescing, kann es vorkommen, dass bei der Wiederherstellung einige Daten beschädigt oder unbrauchbar sind, da geöffnete Dateien nicht korrekt verarbeitet werden konnten.

Eine weitere spezielle Technik bei Datenbank-Backups ist die „Truncation" (oder Verkürzung) der Transaktionsprotokolle. In diesen Protokollen werden alle Transaktionen und Modifikationen an einer Datenbank aufgezeichnet, die ggf. zur Wiederherstellung einer Datenbank dienen können. Transaktionsprotokolle müssen regelmäßig verkürzt werden, damit diese im Laufe der Zeit nicht ausufern. Eine solche Verkürzung kann nach Abschluss eines erfolgreichen Datenbank-Backups erfolgen, da das Backup die Funktion eines Wiederherstellungspunkts übernehmen kann. Die Transaktionsprotokolle, die nach dem Backup vorhanden sind, können so lange zur Wiederherstellung verwendet werden, bis das nächste Backup abgeschlossen ist.

Eine weitere wichtige Anforderung sind granulare Wiederherstellungen. Sie bieten die Möglichkeit, nur einen bestimmten Teil der Daten wiederherzustellen, statt eine vollständige Datenbank oder einen kompletten E-Mail-Objektspeicher. Sollen beispielsweise nur einige Datensätze aus einer Datenbank oder nur eine einzige E-Mail aus einer Mail-Datei wiederhergestellt werden, ohne die ursprünglichen Dateien zu überschreiben, muss Ihre Backup-Anwendung eine granulare Wiederherstellung unterstützen.

Veeam Backup & Replication bietet vollständige Unterstützung für anwendungs- und transaktionskonsistente Backups, die garantieren, dass Ihre geschäftskritischen Daten korrekt gesichert werden. Außerdem unterstützt diese Lösung die Protokoll-Truncation mit anwendungskonsistenter Image-Verarbeitung. Im Bedarfsfall ermöglichen die Veeam Explorer™ ganz unkompliziert die Wiederherstellung einzelner Objekte für häufig genutzte Anwendungen, wie Microsoft Active Directory, Exchange und SQL Server.

8 – Zahlreiche Wiederherstellungsoptionen für VM-Backups auf Festplattenebene

Für maximale Effizienz werden in einer virtuellen Umgebung Backups auf Image-Ebene auf einer virtuellen Festplatte erstellt. Im Geschäftsalltag müssen allerdings häufig nur bestimmte Objekte innerhalb einer VM wiederhergestellt werden und nicht die gesamte VM. Was also, wenn einzelne Dateien oder Anwendungselemente wiederhergestellt werden sollen? Bei einem Backup auf Image-Ebene haben Sie Einblick in das Festplatten-Image, da es von der Backup-Anwendung gemountet und über das Dateisystem des Betriebssystems innerhalb des Image aufgerufen werden kann. So können Sie die Dateien im Image anzeigen und genau die benötigten einzelnen Dateien wiederherstellen. Außerdem können Sie Datastores auf Anwendungsebene aufrufen, wie Datenbanken oder E-Mail-Dateien. Die Wiederherstellung einer riesigen Datenbank kann aufwendig und komplex sein. Mit dem Aufruf einzelner Dateien können Sie dagegen kleinere E-Mail-Volumen oder wenige Datensätze wiederherstellen. Ihre Backup-Anwendung muss daher das Anwendungsdateiformat kennen, damit Sie genau die benötigten Objekte darin finden und wiederherstellen können.

Neben Datenbanken und E-Mails müssen häufig auch einzelne Anwendungsobjekte aus Microsoft Active Directory (AD), einer wichtigen Komponente jeder Windows-Infrastruktur, wiederhergestellt werden. In der Regel sollen nicht die vollständige AD-Struktur und alle Daten aus Active Directory wiederhergestellt werden. Es ist deshalb besonders wichtig, die Struktur nicht zu beschädigen. Für eine solch sensible Wiederherstellung muss die Backup-Anwendung in der Lage sein, nativ auf AD zuzugreifen und darin zu navigieren, um gelöschte Objekte im ursprünglichen Verzeichnis wiederherzustellen. Mit Image-basierten Backups sind also abhängig von den jeweiligen Anforderungen viele Möglichkeiten denkbar. Egal ob eine vollständige VM, eine bestimmte VM auf einer virtuellen Festplatte, eine oder mehrere Dateien innerhalb einer VM, eine einzelne E-Mail oder ein Objekt einer Datenbank wiederhergestellt werden soll – Ihre Backup-Anwendung sollte alle Voraussetzungen erfüllen, die an diese granularen Wiederherstellungsszenarios gestellt werden.

Mit Veeam Backup & Replication ist das kein Problem. Unterstützt werden 47 unterschiedliche Wiederherstellungsszenarios, von VM-Gruppen in einer vApp über eine vollständige VM bis hin zu einzelnen Dateien und Objekten auf Anwendungsebene, so dass Sie so gut wie alle Anforderungen in Sachen Wiederherstellung problemlos bewältigen.

9 – Optimierte Backup-Nutzung – lassen Sie Backup-Repositories für sich arbeiten

Backups sind vergleichbar mit einem Versicherungsschutz: Sie sind eine fortlaufende Investition, die Geld kostet. Sie brauchen diesen Schutz zwar, erhalten aber erst dann etwas zurück, wenn der Schadensfall eintritt. In virtualisierten Umgebungen erstellen Sie häufig Backups von Festplatte zu Festplatte oder arbeiten optional mit Bandsicherungen. Ihre VM-Backups belegen auf Ihren Ziel-Repositories wertvollen Festplattenspeicher und verbrauchen Ressourcen – und bleiben dabei völlig ungenutzt. Indem Sie Ihre VMs allerdings auf Festplatte speichern, verfügen Sie über historische Kopien, die Sie sehr sinnvoll verwenden können. Stellen Sie sich vor, Sie bräuchten schnell eine Sandbox-Umgebung, um ein Anwendungs-Upgrade zu testen, oder eine isolierte Umgebung für Testzwecke oder zur Fehlerbehebung: Backup-Kopien eignen sich perfekt dafür. Sie können sie als eigenes virtuelles Netzwerk isolieren und damit beliebig für jeden denkbaren Zweck nutzen, ohne Beeinträchtigung Ihrer Produktivumgebung.

Veeam bietet diese Möglichkeit mit Veeam Backup & Replication. Dort wird ein Virtual Lab erstellt, das den Backup-Server als NFS-Server nutzt, wobei die Backup-Repositories als Storage-Geräte dienen. Jeder ESXi-Host kann eine Verbindung zum Virtual Lab herstellen und die VM-Backups im Repository aufrufen. Die Backup-Images sind schreibgeschützt und alle Änderungen daran werden später wieder verworfen. Die aktiven VMs im Repository werden vom übrigen Netzwerk isoliert und über eine spezielle Routing-Appliance außerhalb des Netzwerks aufgerufen. So können Sie Ihre Backups auch automatisch auf Wiederherstellbarkeit prüfen. Wir haben bereits die 3-2-1-Regel angesprochen. Veeam bietet sogar eine 3-2-1-0-Regel. „0“ steht dabei für „0 Fehler“ – das Ergebnis der automatischen Prüfung auf Wiederherstellbarkeit für jedes Backup mit Veeam SureBackup® und Sure Replica.

Indem Sie Ihre Backups neben gelegentlichen Wiederherstellungen auch für andere Zwecke einsetzen, maximieren Sie den Ertrag aus Ihren Backup-Investitionen und profitieren zugleich von einem wirklich funktionierenden Versicherungsschutz.

10 – Verhindern Sie Engpässe – machen Sie Ihre Hausaufgaben

Die Kapazitätsplanung für Ihre Backups ist enorm wichtig. Denn nur so können Sie die Aufbewahrungsrichtlinie zuverlässig einhalten, die Sie sich selbst auferlegt haben oder zu der Sie nach Compliance-Vorgaben verpflichtet sind. Die Kapazitätsplanung Ihrer Backup-Repositories ist nicht einfach, da virtuelle Umgebungen durch einen VM-Wildwuchs oft sehr schnell immer größer werden. Wissen Sie, wie lange Ihre aktuelle Kapazität noch ausreicht? Wissen Sie, welche Folgen eine Erweiterung um fünf weitere VMs hat? Bei einem Engpass fallen entweder nicht geplante Kosten für eine Erweiterung an oder Sie müssen Abstriche bei Ihren Aufbewahrungsrichtlinien machen. Beides gilt es zu vermeiden. Sie müssen also berechnen, wann Sie für Ihr vorgesehenes Backup-Repository den Storage erweitern müssen – und das kann ganz schön diffizil sein. Aufgaben in der Backup-Mathematik sind leider ungleich schwerer zu lösen als die Frage zur Kapazitätsplanung für herkömmliche Speicher, denn es fließen viele Faktoren in die Berechnung ein. Dazu gehören beispielsweise Backup-Komprimierungsverhältnisse, Aufbewahrungszeiträume, Häufigkeit und Änderungsraten für inkrementelle Backups. Hier sind Sie auf eine intelligente Backup-Anwendung angewiesen, die diese Rechenaufgaben für Sie erledigt.

Veeam ONE™ bietet umfassende Analyse- und Monitoring-Funktionen für VMware vSphere-Infrastrukturen, mit denen potenzielle Probleme aufgedeckt werden, die die Performance Ihrer Backups und Produktivanwendungen beeinträchtigen könnten. Veeam ONE benachrichtigt Sie, wenn der Backup-Speicherplatz eine bestimmte Schwelle erreicht. Es kann den Schätz-Report „VM Change Rate Estimation“ generieren, der Ihre VM-Änderungsrate automatisch analysiert und den potenziell erforderlichen Speicherplatz für Ihr Backup-Repository berechnet.

Backups brauchen mehr als nur ein System, auf dem sie gespeichert werden – sie benötigen zudem ausreichend Host-Ressourcen, damit sie innerhalb des gewünschten Backup-Fensters ausgeführt werden können. Der Report „Datastore Performance Assessment“ hilft bei der Beurteilung der Datastore-Performance, um potenzielle Probleme zu erkennen, die während der Backup-Prozesse aufgrund zu hoher Latenz- oder IOP-Werte auftreten können. Diese Informationen sind hilfreich bei der Definition von Latenz-Schwellenwerten zur Optimierung der Backup-Verarbeitungs-Performance, Erhöhung der Effizienz bei der Ressourcenauslastung und Minimierung der Auswirkungen auf Produktiv-Workloads. Veeam ONE ist eine ideale Ergänzung zu Veeam Backup & Recovery und bietet Ihnen den vollständigen transparenten Einblick, den Sie für eine funktionierende Backup-Umgebung benötigen.

Der Autor

Eric Siebert kann als IT-Branchenveteran, Referent, Autor und Blogger aufeine mehr als 25-jährige Erfahrung zurückblicken. Seit 2005 befasst er sich schwerpunktmäßig mit dem Bereich Virtualisierung. Er hat mehrere Bücher veröffentlicht, darunter den kürzlich von Pearson Publishing herausgegebenen Titel „Maximum vSphere", sowie Hunderte Artikel und Whitepapers für Tech Target und VMware-Partner. Auf seiner eigenen VMware-Info-Website unter „vSphere-land.com" veröffentlicht er zudem regelmäßig Wissenswertes rund um VMware. Eric Siebert ist häufig als Referent auf Branchenkonferenzen und Events anzutreffen, etwa auf der VMworld, und seit dem Programmstart im Jahr 2009 anerkannter vExpert von VMware.

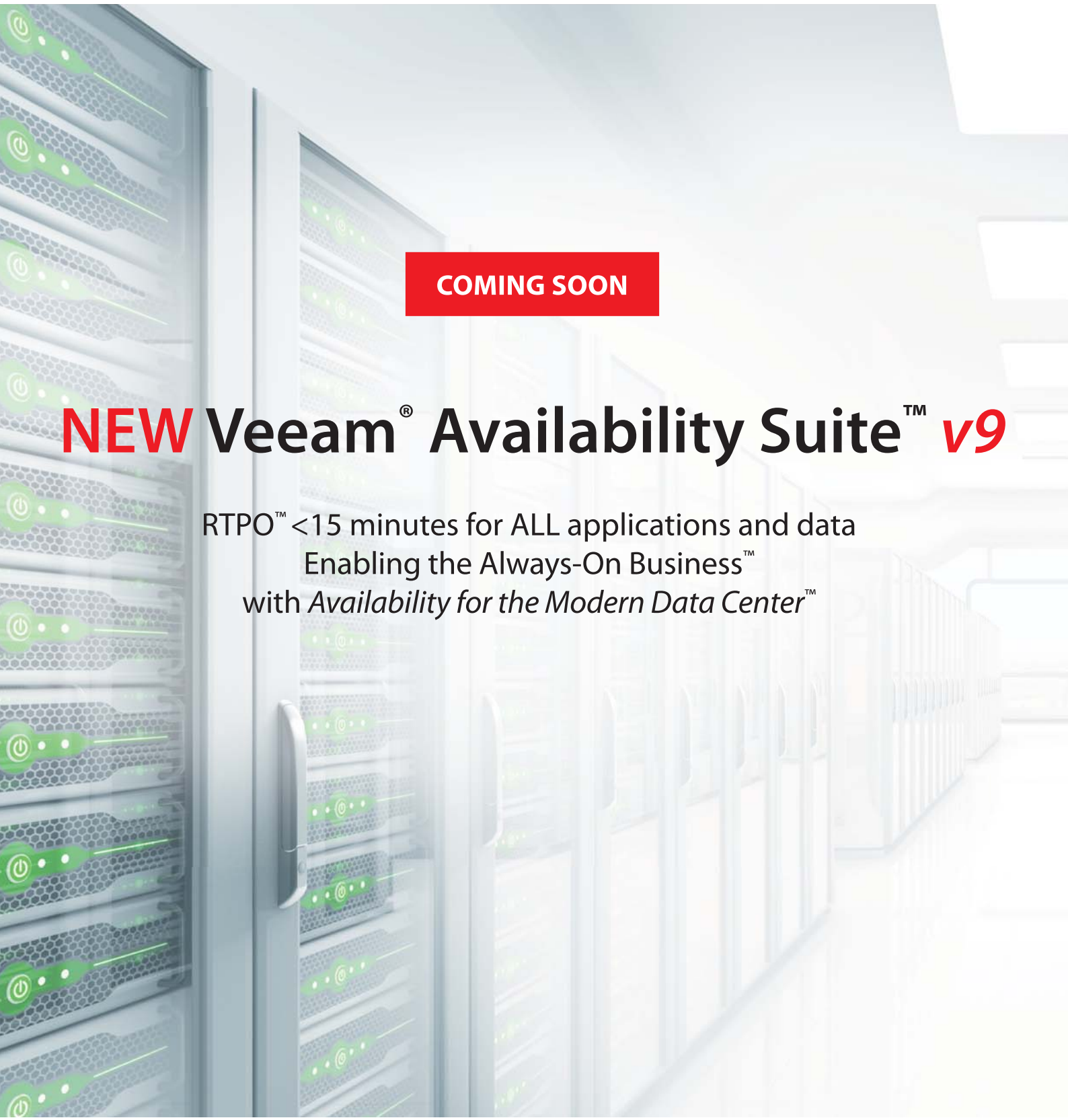
Über Veeam Software

Veeam® kennt die neuen Herausforderungen, denen sich Unternehmen weltweit in Sachen Always-On Business™ für einen Geschäftsbetrieb rund um die Uhr (24/7/365) stellen müssen. Daher bietet Veeam als erster Anbieter auf dem Markt *Availability for the Modern Data Center*™ und unterstützt Unternehmen dabei, Wiederherstellungszeiten und -punkte (RTPO™) von weniger als 15 Minuten für alle Anwendung und Daten zu erzielen. Dafür stellen wir eine völlig neue Lösung bereit, die High-Speed Recovery, Vermeidung von Datenverlust, Verified Protection, Risikominimierung und vollständige Transparenz ermöglicht. Die Veeam Availability Suite™, die Veeam Backup & Replication™ beinhaltet, nutzt Virtualisierungs-, Storage- und Cloud-Technologien optimal aus, so dass Unternehmen mit modernen Rechenzentren Zeit sparen, Risiken minimieren und Investitions- und Betriebskosten erheblich senken können.

Veeam wurde im Jahr 2006 gegründet und hat derzeit ein Netzwerk von 30.500 ProPartnern und mehr als 145.500 Kunden weltweit. Der Hauptsitz von Veeam befindet sich in Baar in der Schweiz, darüber hinaus hat das Unternehmen Niederlassungen in der ganzen Welt. Mehr erfahren Sie unter https://www.veeam.com/.

VEEAM
IT JUST WORKS!™

AVAILABILITY™
for the Modern Data Center



COMING SOON

NEW Veeam® Availability Suite™ v9

RTPO™ <15 minutes for ALL applications and data
Enabling the Always-On Business™
with *Availability for the Modern Data Center*™

To learn more, visit **www.veeam.com**