Disaster Recovery as a Service

Leitfaden für Käufer

AUF EINEN BLICK

Einen On-Premises-Standort als Disaster Recovery-Ziel bereitzustellen, ist komplex, teuer und unzuverlässig. Eine Disaster Recovery as a Service-Lösung, die nahtlos auf Basis einer globalen Public Cloud bereitgestellt wird, bietet integrierte Vorteile wie Cloud-Ökonomie, Zuverlässigkeit, Anwenderfreundlichkeit und die nötige Flexibilität, um auf seltene, aber unvorhersehbare Zwischenfälle reagieren zu können. Deshalb ist sie ein ideales DR-Ziel.

WICHTIGE ÜBERLEGUNGEN

1. Welche RTOs werden für die einzelnen Anwendungen benötigt?
2. Bietet der Service eine zuverlässige Infrastruktur für den DR-Standort sowie Failover-Automatisierung und -Orchestrierung?
3. Wie würde sich der Plattformwechsel von Anwendungen gestalten?
4. Können unterbrechungsfreie DR-Tests durchgeführt werden?
5. Ist der Service im Vergleich zu bestehenden alternativen DR-Lösungen kosteneffizient?

Viele Unternehmen implementieren eine Disaster Recovery(DR)-Lösung, weil ihnen die Wichtigkeit bewusst ist oder um behördliche Vorschriften einzuhalten. Einen separaten On-Premises-Standort als DR-Ziel zu betreiben, ist arbeitsintensiv und erfordert erhebliche Investitionen für Bereitstellung und Wartung. Insbesondere aufgrund der seltenen Nutzung derartiger Bereitstellungen ist dies ungünstig. Wenn Disaster Recovery as a Service (DRaaS) dagegen in einer elastischen Public Cloud mit integrierter Automatisierung ausgeführt wird, werden ungenutzte Hardware sowie Wartungsaufgaben reduziert. Zudem wird die Bereitstellung bei einem DR-Ereignis vereinfacht und die Zuverlässigkeit der DR-Lösung durch unterbrechungsfreie Tests erhöht.

On-Premises-DR-Lösungen sind häufig teuer und erfordern tiefgreifende Kenntnisse für Bereitstellung, Wartung und Betrieb. Außerdem muss der volle Preis für DR-Stellfläche, -Hardware und -Software bezahlt werden, obwohl diese Ressourcen nur genutzt werden, wenn das primäre Rechenzentrum ausfällt. Deshalb fällt es IT-Entscheidungsträgern schwer, Investitionen in derartige Initiativen zu rechtfertigen. Nach der Bereitstellung einer DR-Lösung muss diese zudem getestet werden, was oftmals aufwändig und mit Unterbrechungen verbunden ist. Das Ergebnis ist ein geringeres Maß an Schutz, das Unternehmen für ihre geschäftskritischen Anwendungen in Kauf nehmen müssen, wenn es zu einem Zwischenfall kommt. Um diese Herausforderungen zu bewältigen, setzen viele Unternehmen auf die Public Cloud. Dieser Leitfaden soll Unternehmen wichtige Faktoren darlegen, die beachtet werden sollten, wenn die Public Cloud als DR-Lösung in Erwägung gezogen wird.

Gartner zufolge bieten DRaaS-Anbieter eine hervorragende Möglichkeit für Unternehmen, die sich von Rechenzentrumsabläufen lösen und dabei Geld sparen möchten. DRaaS-Preise betragen üblicherweise zwischen 30% und 50% von dem, was der Aufbau vergleichbarer Funktionen kosten würde.[1]

1. Faktor: Für einzelne Anwendungen benötigte RTOs

Zwar können Unternehmen durchaus alle eigenen Anwendungen schützen, aber dies wird u.U. sehr teuer. Stattdessen sollten sie ihre Anwendungen anhand der entsprechenden Recovery Time Objectives (RTOs) kategorisieren. Dieser Wert gibt die akzeptable Wartezeit an, bis die Anwendung wieder online ist. Einige DRaaS-Lösungen bieten RTOs von Minuten, andere von Stunden oder Tagen.

Die RTO-Werte richten sich nach den unterschiedlichen Unternehmensanforderungen. Umsatzgenerierende Anwendungen dürfen selten für längere Zeit ausfallen. HR-Anwendungen dagegen brauchen meist 8 Stunden oder mehr, bis sie wieder online sind, ohne dass dabei das Business merklich betroffen ist. Je strenger die RTO-Anforderungen für Anwendungen sind, desto teurer ist entsprechend auch die Wiederherstellung dieser Anwendungen innerhalb des erforderlichen Zeitrahmens. Unternehmen sollten deshalb den Schutz geschäftskritischer Anwendungen priorisieren. Falls anschließend ausreichend Budget verbleibt, können dann weniger wichtige Anwendungsklassen geschützt werden. Der gewünschte RTO-Wert sollte zentraler Faktor bei der Auswahl einer Cloud-basierten DRaaS-Lösung sein.

Abgesehen von den RTOs sollten Unternehmen auch darauf achten, ob sie innerhalb kurzer Zeit verschiedene Wiederherstellungspunkte überprüfen können, wenn sie eine Recovery nach einem Ransomware-Angriff durchführen. Auf diese Weise wird eine schnelle Wiederherstellung von Anwendungen nach einem Ransomware-Angriff sichergestellt.

DISASTER RECOVERY-LÖSUNGEN IN DER ÜBERSICHT

Nur Daten-Backup

Bei diesen Lösungen werden die Unternehmensdaten an einem sekundären On-Premises-Standort oder in der Cloud repliziert. Dadurch sind Unternehmen jedoch nicht vor längeren Ausfallzeiten im Rahmen von Zwischenfällen geschützt, denn dann steht keine Infrastruktur zum Ausführen von Anwendungen bereit. Außerdem können keine unkomplizierten DR-Tests durchgeführt werden und nach dem Kauf der Infrastruktur stehen zahlreiche manuelle Aufgaben an.

Automatisierte DR zu einem On-Premises-Standort oder einer Co-Location

Bei diesen Lösungen fällt weniger manueller Aufwand an. Jedoch muss erhebliches Kapital in Stellfläche, Hardware und Software investiert werden, obwohl diese Ressourcen nur selten genutzt werden. Zudem gestaltet sich die Skalierung schwieriger.

Automatisierte DR zu Rechenzentren von DRaaS-Anbietern

Diese Lösungen bieten die meisten Vorteile automatisierter DR zu On-Premises-Standorten sowie eine günstigere Kostenstruktur, die der seltenen Nutzung des DR-Ziels entspricht.

Kunden, die sich für derartige Lösungen interessieren, sollten sich über die Zuverlässigkeit der entsprechenden DR-Infrastruktur sowie die finanzielle Sicherheit des DRaaS-Anbieters informieren.

Automatisierte DR zu globalen Clouds größter Skalierung

Diese Lösungen bieten die meisten Vorteile automatisierter DR zu On-Premises-Standorten sowie eine günstigere Kostenstruktur, die der seltenen Nutzung des DR-Ziels entspricht.

Kunden, die derartige Lösungen nutzen, profitieren aufgrund der zuverlässigen Infrastruktur, globalen Verfügbarkeit und finanziellen Stabilität des Mega-Cloud-Anbieters von einem geringeren Risiko. Bei einigen dieser Lösungen müssen Kunden jedoch einen Plattformwechsel ihrer Anwendungen vornehmen.

2. Faktor: Zuverlässige Infrastruktur für einen DR-Standort sowie Failover-Automatisierung und -Orchestrierung

Daten in der Cloud zu sichern, ist relativ einfach. Wenn Unternehmen sich jedoch ausschließlich auf Backups verlassen, entstehen durch die Möglichkeit von Zwischenfällen erhebliche Risiken. Wenn nur Daten in die Cloud kopiert werden, müssen Unternehmen eine vollständige Umgebung einrichten, Computing-Instanzen erstellen, Daten auf die richtigen Cloud-Storage-Geräte verschieben und Networking einrichten. Viele dieser Aufgaben gehen mit hohem manuellem Aufwand einher und kosten viel Zeit. Bei Anwendungen mit einem RTO ab zwei Tagen stellt dies kein Problem dar. Umsatzgenerierende Anwendungen müssen in der Regel jedoch schneller wiederhergestellt werden.

Unternehmen sollten für wichtigere Anwendungen Cloud-basierte Services wählen, die Orchestrierung und Automatisierung des DR-Failovers bieten. Diese Services stellen gemäß eines zuvor festgelegten Runbooks eine DR-Umgebung bereit. Dabei werden erforderliche Knoten gestartet, VMs in der ihren Abhängigkeiten entsprechenden Reihenfolge hochgefahren, Skripts ausgeführt und IP-Netzwerke automatisch zugewiesen – alles mit äußerst geringem manuellem Aufwand. So wird die rechtzeitige Ausführung kritischer Anwendungen sichergestellt, um bei Zwischenfällen die Auswirkungen auf das Business möglichst zu reduzieren.

Disaster Recovery as a Service ist bei vielen Anbietern erhältlich. Umfang und Reifegrad von DRaaS-Lösungen variieren jedoch. So mangelt es bei vielen Anbietern im Gegensatz zu den größten Cloud-Anbietern an Skalierbarkeit, Zuverlässigkeit, finanzieller Stabilität sowie an der globalen Verfügbarkeit. Die Zuverlässigkeit der DR-Infrastruktur sollte ebenfalls als zentraler Faktor betrachtet werden. Denn Unternehmen müssen sich im entscheidenden Augenblick, wenn es zu einem Ausfall des eigenen primären Rechenzentrums kommt, auf DR-Lösungen verlassen können.

3. Faktor: Komplikationsgrad bei der VM-Formatkonvertierung

Viele der modernen Anwendungen, die auf Microservices basieren, sind hinsichtlich der Public Cloud, auf der sie ausgeführt werden, unabhängig. In zahlreichen Unternehmen noch immer stark vertretene herkömmliche Anwendungen werden dagegen normalerweise als VM bereitgestellt. Je nach Hypervisor liegen unterschiedliche VM-Formate vor und viele Public Clouds unterscheiden sich bezüglich ihrer VM-Formate von den On-Premises-Umgebungen in Unternehmen. Um Anwendungen, die für einen bestimmten Hypervisor geschrieben und bereitgestellt wurden, auf einem anderen Hypervisor zu verwenden, muss das VM-Datenträgerformat konvertiert werden. Die VM-Formatkonvertierung ist meist ein langwieriger, komplexer Vorgang, dessen Abschluss mehrere Monate in Anspruch nehmen kann. Während dieses Vorgangs sind die entsprechenden Unternehmensanwendungen vor Zwischenfällen nicht geschützt.

4. Faktor: Erfordernis von DR-Tests ohne Unterbrechungen

Ein DR-Plan wird nicht nur einmal erstellt. Rechenzentren sind dynamisch. Vorhandene Anwendungen werden aktualisiert oder ersetzt und mit der Zeit werden zusätzliche Anwendungen bereitgestellt. Dadurch ergibt sich eine Abweichung des ursprünglichen DR-Plans von einem effektiven DR-Plan, der mit Anwendungsänderungen Schritt halten kann.

Um diesen Missstand zu verhindern, müssen Unternehmen ihren DR-Plan regelmäßig überprüfen – quartalsweise gemäß Best Practices. Da es sich bei diesen Tests nicht um echte Zwischenfälle handelt, sollten die währenddessen ausgeführten Unternehmensanwendungen nicht in Mitleidenschaft gezogen werden. Die Tests sollten unterbrechungsfrei erfolgen. Unternehmen müssen mühelos DR-Failover-Verfahren in einer sich ständig ändernden IT-Umgebung definieren, pflegen und testen können.

Einige Unternehmen sind zudem gesetzlich verpflichtet, DR-Tests durchzuführen und deren Ergebnisse im Rahmen von Audits vorzulegen. Ideale DRaaS-Lösungen sollten Kunden umfassende, unterbrechungsfreie Tests sowie dazugehörige Reports bereitstellen.

DISASTER RECOVERY AS A SERVICE (DRAAS) – ANWENDUNGSBEREICHE

Ersteinführung einer DR-Lösung
Für Unternehmen, die nur über Backups verfügen oder noch keinen DR-Plan erstellt haben

Erweiterung vorhandener DR-Pläne
Einige Unternehmen besitzen bereits eine DR-Lösung On-Premises, schützen damit jedoch nur wenige Workloads. Mit DRaaS können diese Kunden ihre restlichen Workloads in der Cloud schützen, ohne dabei vorhandene DR-Pläne zu verändern.

Ersetzen der vorhandenen DR-Lösung
Einige Unternehmen müssen die interne Stellfläche reduzieren bzw. auf die Cloud umsteigen. DRaaS stellt eine naheliegende Lösung dar, um einen On-Premises-DR-Standort in die Cloud zu verschieben.

DR über mehrere Cloud-Regionen hinweg
Selbst in den größten Public Clouds kommt es zu Ausfällen, wodurch DR auch für Kunden relevant ist, die Anwendungen in der Cloud ausführen. Mit einer DRaaS-Lösung können Kunden die eigenen Anwendungen über mehrere Cloud-Regionen hinweg schützen.

RESSOURCEN

VMware Cloud on AWS – Website

VMware Cloud Disaster Recovery-Website

VMware Site Recovery-Website

Weitere Informationen finden Sie in den Dokumenten *VMware Cloud on AWS – Lösungsübersicht* und *VMware Cloud on AWS – Gesamtbetriebskosten*.

Sehen Sie sich informative Demos, Übersichtsvideos, Webinare und Kundenfeedback an: *VMware Cloud on AWS auf YouTube*

Lesen Sie unsere aktuellen *Blog-Beiträge zu VMware Cloud on AWS*

Folgen Sie VMware auf Twitter *@vmwarecloudaws* und verwenden Sie das Hashtag #VMWonAWS.

TECHNISCHE RESSOURCEN

VMware Cloud Tech Zone

Erste Schritte mit VMware Cloud on AWS

5. Faktor: Kosteneffizienz im Vergleich zu bestehenden alternativen DR-Lösungen

DRaaS-Lösungen benötigen Storage-Komponenten in stabilem Zustand, um die zu schützenden Daten zu speichern. Damit Unternehmen ihre Kosten optimieren können, ist ein hocheffizienter Storage-Layer in der Cloud erforderlich, um diese Daten zu speichern. Um die Kosten noch weiter zu reduzieren, sollten Unternehmen in der Lage sein, die Infrastruktur in der Cloud nur dann hochzufahren, wenn sie während eines DR-Tests oder eines Failover-Ereignisses benötigt wird.

Schließlich sollten Unternehmen sich beispielsweise folgende Fragen stellen: Muss die DRaaS-Lösung bei einem Failback immer alle Daten wiederherstellen oder lässt sie optimiertes Failback zu? Wie sehen Preis und Kennzahl der zu schützenden Daten aus? Welche Egress-Gebühren erhebt der Cloud-Anbieter bei der Übertragung der Daten in die/aus der Cloud-Infrastruktur? Diese Faktoren haben einen erheblichen Einfluss auf die DR-Kosten.

Fazit

Unternehmen, die Disaster Recovery as a Service über die Public Cloud bereitstellen möchten, sollten bei der DR-Strategie einige wichtige Faktoren beachten. Ein gutes DRaaS-Angebot zeichnet sich durch Bereitstellung der RTOs aus, die für geschäftskritische Anwendungen erforderlich sind. Außerdem sollten Orchestrierung und Automatisierung des Failover-Vorgangs sowie unterbrechungsfreie Tests bereitgestellt werden. All das sollte idealerweise ohne Erfordernis eines Plattformwechsels von Anwendungen erfolgen und auf Basis einer zuverlässigen Public Cloud ausgeführt werden. Und schließlich sollte DRaaS Kunden dabei unterstützen, ihre DR-Kosten zu optimieren.

VMware bietet zwei firmeneigene DRaaS-Lösungen an, die in VMware Cloud on AWS unterstützt werden:

VMware Cloud Disaster Recovery bietet eine bedarfsorientierte Disaster Recovery, die als einfach zu bedienende SaaS-Lösung mit den wirtschaftlichen Vorteilen der Cloud bereitgestellt wird. Sie kombiniert kosteneffizienten Cloud-Storage mit einfachem, SaaS-basiertem Management für IT-Resilienz im erforderlichen Maßstab. Kunden profitieren von einem konsistenten VMware-Betrieb über Produktions- und DR-Standorte hinweg und einem Failover-Kapazitätsmodell für Disaster Recovery-Ressourcen (DR) mit bedarfsorientierten Preisen. VMware Cloud Disaster Recovery kann eine sehr breite Palette von IT-Services kosteneffizient mit schnellen Recovery-Funktionen schützen (On-Demand-DRaaS).

Mit VMware Site Recovery™ for VMware Cloud™ on AWS profitieren Kunden von einem vollständigen DR-Service. VMware Site Recovery kann unternehmenskritische IT-Services schützen, die einen sehr niedrigen RPO und RTO benötigen (Hot DRaaS). Site Recovery stellt für Kunden eine globale, zuverlässige Infrastruktur mit den vertrauten Oberflächen von vSphere und vCenter bereit. Dabei sind keine Plattformwechsel erforderlich. Mit VMware Site Recovery Manager™ (SRM), einer vielfach bewährten DR-Lösung, können Kunden Failover, Failback und Neuzuweisung von IP-Netzwerken orchestrieren und automatisieren sowie unterbrechungsfreie Tests mit ausführlichen Reports durchführen.

Weitere Informationen
VMware Cloud Disaster Recovery und *VMware Site Recovery*

1. Gartner: „Reduce Costs and Piggyback DR Investments“, 29. Mai 2020

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Zweigniederlassung Deutschland Willy-Brandt-Platz 2 81829 München Tel.: +49 89 370 617 000 Fax: +49 89 370 617 333 www.vmware.com/de