Disaster Recovery as a Service – Leitfaden für Käufer

AUF EINEN BLICK

Einen On-Premises-Standort als Disaster Recovery-Ziel bereitzustellen, ist teuer und komplex. Diese Disaster Recovery as a Service-Lösung wird nahtlos auf Basis einer globalen Public Cloud bereitgestellt und ist dank integrierter Vorteile ein ideales DR-Ziel.

WICHTIGE ÜBERLEGUNGEN

1. Welche RTOs werden für die einzelnen Anwendungen benötigt?
2. Werden Failover-Automatisierung und -Orchestrierung durch den Service bereitgestellt?
3. Wie würde sich der Plattformwechsel von Anwendungen gestalten?
4. Können unterbrechungsfreie DR-Tests durchgeführt werden?
5. Wie zuverlässig ist die Infrastruktur des DR-Standorts?

Viele Unternehmen implementieren eine Disaster Recovery (DR)-Lösung, weil ihnen der Stellenwert bewusst ist oder um Compliance mit gesetzlichen Richtlinien sicherzustellen. Wenn ein zusätzlicher On-Premises-Standort als DR-Ziel bereitgestellt wird, geht dies mit Aufwand und Investitionen für Bereitstellung und Wartung einher. 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, können ungenutzte Hardware sowie Wartungsaufgaben reduziert werden. Zudem wir die Bereitstellung bei Zwischenfällen vereinfacht und dank unterbrechungsfreier Tests ergibt sich eine zuverlässige Lösung.

DR-Lösungen, die in On-Premises-Umgebungen bereitgestellt werden, 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. Neben der Bereitstellung von DR-Lösungen müssen auch die Tests beachtet werden, die oftmals aufwändig und mit Unterbrechungen verbunden sind. Das Ergebnis ist ein geringeres Maß an Schutz, das Unternehmen für die eigenen geschäftskritischen Anwendungen in Kauf nehmen müssen, wenn es zu einem Zwischenfall kommt. Um diese Herausforderungen zu bewältigen, greifen viele Unternehmen zur Public Cloud. Dieser Leitfaden soll Unternehmen wichtige Faktoren darlegen, die beachtet werden sollten, wenn die Public Cloud als DR-Lösung geprüft wird.

DISASTER RECOVERY-LÖSUNGEN IN DER ÜBERSICHT

1. **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.
2. **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.
3. **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 im Klaren sein.
4. **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 äußerst großen Cloud-Anbieters. Bei einigen dieser Lösungen müssen Kunden jedoch einen Plattformwechsel der eigenen Anwendungen vornehmen.

1. Faktor: Für einzelne Anwendungen benötigte RTOs

Zwar können Unternehmen auch alle eigenen Anwendungen schützen, aber dies kann sehr teuer werden. Stattdessen sollten Unternehmen die eigenen Anwendungen anhand der entsprechenden Recovery Time Objectives (RTOs) kategorisieren. Dieser Wert gibt die akzeptable Wartezeit an, bis die Anwendung wieder online sein muss. Einige DRaaS-Lösungen bieten RTOs von Minuten, andere Stunden oder Tage.

Je nach Unternehmen müssen unterschiedliche RTO-Werte angefordert werden. 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 zur Auswahl einer Cloud-basierten DRaaS-Lösung als zentraler Faktor herangezogen werden.

2. Faktor: Automatisierung und Orchestrierung des Failovers

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 manuell 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 bereitstellen. 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 (DRAAS) – ANWENDUNGSBEREICHE

1. **Ersteinführung einer DR-Lösung**
   Für Unternehmen, die nur über Backups verfügen oder noch keinen DR-Plan erstellt haben
2. **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.
3. **Ersetzen der vorhandenen DR-Lösung**
   Einige Unternehmen müssen die interne Stellfläche reduzieren bzw. „die Cloud einführen“. DRaaS stellt eine naheliegende Lösung dar, um einen On-Premises-DR-Standort in die Cloud zu verschieben.
4. **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.

3. Faktor: Komplexität des Plattformwechsels von Anwendungen

Viele der modernen Anwendungen, die auf Mikroservices 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 ein Plattformwechsel der VMs vorgenommen werden. Plattformwechsel sind meist langwierige, komplexe Projekte, deren Abschluss Unternehmen mehrere Monate kosten 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. Denn Rechenzentren sind dynamisch. So werden vorhandene Anwendungen 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 den eigenen 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.

Einige Unternehmen sind zudem gesetzmäßig zum Durchführen von DR-Tests und zur Präsentation der Ergebnisse im Rahmen von Audits verpflichtet. Ideale DRaaS-Lösungen sollten Kunden umfassende, unterbrechungsfreie Tests sowie dazugehörige Berichte bereitstellen.

5. Faktor: Zuverlässigkeit der Infrastruktur des DR-Standorts

Disaster Recovery as a Service ist bei vielen Anbietern erhältlich. Die von DRaaS-Anbietern gebotene Skalierung und Erfahrung variiert 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 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.

RESSOURCEN

Weitere Informationen zu unserem Service finden Sie auf der Website zu VMware Cloud on AWS.

Weitere Informationen zu Disaster Recovery as a Service, Demo-Videos und mehr finden Sie auf der Website zu VMware Site Recovery.

Lesen Sie die Dokumente 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 die neusten Beiträge im Blog zu VMware Cloud on AWS.

Folgen Sie uns auf Twitter @vmwarecloudaws und erwähnen Sie uns mittels #VMWonAWS.

Legen Sie jetzt mit VMware Cloud on AWS los: https://cloud.vmware.com/vmc-aws/get-started

Lesen Sie die technische Dokumentation zu VMware Cloud on AWS.

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.

Mit VMware Site Recovery™ for VMware Cloud™ on AWS profitieren Kunden von einem vollständigen DR-Service. 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 häufig bewährten DR-Lösung, können Kunden Failover, Failback und Neuzuweisung von IP-Netzwerken orchestrieren und automatisieren sowie unterbrechungsfreie Tests mit ausführlichen Berichten durchführen.

Weitere Informationen erhalten Sie unter cloud.vmware.com/de/vmware-site-recovery.

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