Zerto

a Hewlett Packard Enterprise company

Disaster Recovery Leitfaden

DISASTER RECOVERY LEITFADEN

EINLEITUNG

In der heutigen digital ausgerichteten Welt sind Unternehmen auf eine funktionierende Infrastruktur, Anwendungen und Daten angewiesen. Und das rund um die Uhr. Die Ausgaben für Ausfallzeiten und Datenverluste können Unternehmen in den Ruin treiben, wichtige öffentliche Dienste unzugänglich machen und sogar die nationale Sicherheit gefährden. Katastrophen, die IT-Ausfälle und Datenverluste mit sich bringen, reichen im Ausmaß von lokalen Cyberangriffen bis hin zu regionalen Naturkatastrophen. Für Unternehmen, die in den kommenden Jahrzehnten wettbewerbsfähig,erfolgreich und den Bedrohungen gewachsen sein wollen, sind durchdachte Sicherheits- und Resilienzstrategien von entscheidender Bedeutung.

Das Rechenzentrum hat sich weit über einen klimatisierten Raum mit Servern, Speicher- und Netzwerkgeräten hinaus entwickelt. Diese Komponenten werden heute von Software definiert und erweitern Daten über die vier Wände des Rechenzentrums hinaus. Die Daten wandern nicht nur in die Cloud, sondern auch an die Ränder der Netzwerke, wo sie direkt von Nutzern, Kunden, Studenten, Patienten und den digitalen Geräten, die unsere Unternehmen – und unser Leben – steuern, erfasst und verwendet werden.

Die digitale Transformation und das Datenwachstum haben sich in einem Tempo verändert, das schneller ist als die Fähigkeit vieler Disaster Recovery (DR) Lösungen, sich an die modernen Anforderungen an die Wiederherstellung anzupassen. Die meisten DR-Lösungen sind nach wie vor auf das physische Rechenzentrum ausgerichtet und nicht in der Lage, mit der Menge an Daten zu skalieren, die moderne Unternehmen inzwischen produzieren und nutzen.

In diesem Leitfaden liefern wir Ihnen Einblicke in die Herausforderungen, Anforderungen, Strategien und verfügbaren Lösungen für Datenschutz, insbesondere in modernen, digital-zentrierten Umgebungen. Wir erklären, welche Vorteile und Effizienzgewinne Zerto, ein Unternehmen von Hewlett Packard Enterprise, bietet und wie die Lösung im Vergleich zu anderen Technologien für Business Continuity/Disaster Recovery (BC/DR) abschneidet. Mit dem vorliegenden Leitfaden geben wir Unternehmen die richtigen Informationen an die Hand, mit denen sie eine optimale Datenschutz-Lösung für ihre Anforderungen bestimmen können. Wenn Sie beim Lesen des Leitfadens Fragen haben, kontaktieren Sie uns bitte unter info@zerto.com.

VERSUCHEN SIE ES SELBST

Zerto lässt sich in weniger als einer Stunde installieren und konfigurieren. Die simple, VM-basierte Replikation sorgt für RPO-Werte im Sekundenbereich und RTO-Werte im Minutenbereich. Navigieren Sie zu www.zerto.com/trial, um noch heute eine kostenlose Testversion herunterzuladen!

ABSCHNITT 1

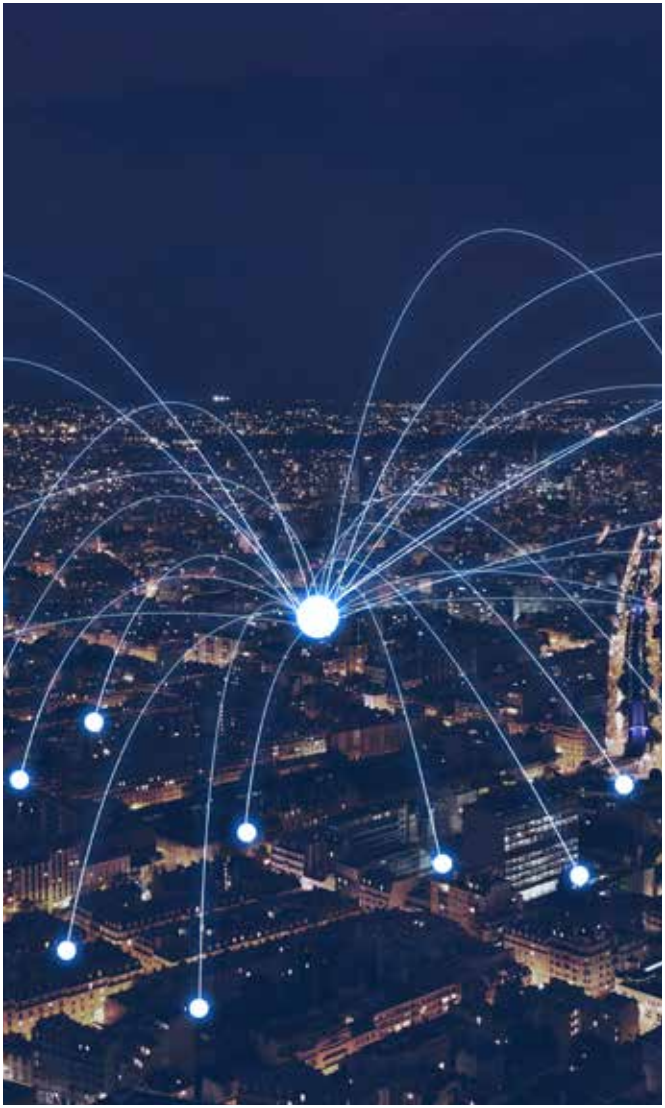
Disaster Recovery – Übersicht

Hinter fast jedem geplanten oder ungeplanten Ereignis kann sich eine Katastrophe verbergen, die die Geschäftsfähigkeit von Unternehmen bedroht. Zur Aufrechterhaltung des Betriebs benötigen Unternehmen eine solide DR-Strategie, die sich auf zwei Hauptziele konzentriert:

Effektives Reagieren auf ungeplante Ereignisse wie Naturkatastrophen, Infrastrukturausfälle, Stromausfälle, Benutzerfehler, Ransomware, beschädigte Systeme und mehr.

Schutz von Daten bei geplanten Unterbrechungen wie bei Migrationen, Cloud-Einführungen, Konsolidierungen von Rechenzentren und mehr.

Eine gute DR-Strategie hilft nicht nur bei ungeplanten Ereignissen wie Katastrophen, sondern auch bei geplanten Unterbrechungen (wie z. B. geschäftsfördernden Initiativen). Die Herausforderung der IT besteht darin, für ausreichend Schutz zu sorgen, um reaktiv auf ungeplante Störungen reagieren zu können, und gleichzeitig durch proaktive Störungen Innovationen zu erlauben, um geschäftlichen Nutzen zu bringen.



Katastrophen in allen Formen und Ausmaßen

Es gibt zwei Hauptkategorien von Katastrophen: natürliche und vom Menschen verursachte Katastrophen.

Zu Naturkatastrophen gehören Erdbeben, Wirbelstürme, Tornados, Waldbrände und Überschwemmungen – Ereignisse, die sowohl größere als auch kleinere Störungen verursachen. Naturkatastrophen können kleine Gebiete betreffen (wie bei Tornados), aber auch ganze Regionen destabilisieren (wie bei Wirbelstürmen). Sie können so verheerend sein, dass sie ganze Standorte – oder sogar mehrere Standorte – in einer Region zerstören. Selbst wenn ein Rechenzentrum nicht direkt beschädigt wird, kann eine Naturkatastrophe zu Strom- und Kommunikationsausfällen führen.

Von Menschen verursachte Katastrophen sind noch vielfältiger. Dazu können z. B. Brände und Überschwemmungen gehören, aber auch subtilere Ereignisse wie Cyberangriffe oder ein versehentliches bzw. böswilliges Löschen von Daten. Da vom Menschen verursachte Katastrophen absichtlich oder unabsichtlich eintreten können, sind ihre Art und ihr Ausmaß schwer vorherzusagen. Einfache Fehlkonfigurationen oder ungeplante Umgebungsänderungen betreffen ggf. ein einzelnes Gebäude, während Ereignisse wie ein Stromausfall ganze Regionen in Mitleidenschaft ziehen können.

In letzter Zeit hat sich Ransomware als eine der bekanntesten von Menschen verursachten Katastrophen etabliert. Es hat sich gezeigt, dass Ransomware-Angriffe weitreichende Störungen verursachen, da sie sich auf Lieferketten auswirken und Versorgungsbetriebe beeinträchtigen. Diese Angriffe sind für Sicherheitsexperten, DR-Spezialisten und in gewissem Maße auch für die nationale Sicherheit Verantwortliche zu einem wichtigen Thema geworden.

Unabhängig von Größe oder Form der Katastrophe muss eine DR-Strategie darauf vorbereiten, schnell zu reagieren, sich zu erholen und den Betrieb fortzusetzen. Außerdem sollte eine DR-Lösung Optionen für eine schnelle Wiederherstellung nach jeder Art von Katastrophe (ob natürlich oder von Menschen verursacht, ob lokal oder regional) bieten.

Die Beziehung zwischen Disaster Recovery und Business Continuity

Business Continuity schließt mehr ein als DR allein. Business Continuity gewährleistet, dass der Geschäftsbetrieb niemals durch geplante oder ungeplante Ereignisse unterbrochen wird, was auch DR-Reaktionsstrategien für ungeplante Störungen einschließt. Beispiele für Business Continuity bei geplanten Ereignissen sind Workload-Migrationen oder geplante Wartungsarbeiten ohne Ausfallzeiten. Business Continuity kann auch dazu beitragen, Katastrophen abzuwenden. Betrachten Sie dazu folgendes Beispiel:

Ein abgelegenes Rechenzentrum befindet sich im Einzugsbereich eines Wirbelsturms, der in wenigen Tagen auf Land treffen könnte. Das DR-Team überträgt Anwendungen und Daten dieses Rechenzentrums im Failover-Verfahren an einen entfernten Standby-Standort, bis die Gefahr vorüber ist. Unabhängig davon, ob eine Katastrophe eintritt oder nicht, wird durch präventive Maßnahmen die Business Continuity gewährleistet.

Auch wenn Business Continuity über den Umfang von DR hinausgeht, sollte es nicht nötig sein, für beide Aspekte völlig unterschiedliche Tools zu verwenden. Eine gute DR-Lösung kann mit Funktionen wie Workload-Migration, unterbrechungsfreiem Patch-Testing und unterbrechungsfreiem Malware-Scanning auch die Anforderungen von Business Continuity erfüllen. Überlegen Sie, inwiefern die Möglichkeiten einer DR-Lösung über reine Disaster Recovery hinausgehen, damit Sie größtmöglichen Nutzen aus Ihrer Investition ziehen können.

Backups gehören nicht zur Disaster Recovery

Die Sicherung von Daten oder eines ganzen Systems ist ein Konzept, das es fast seit den Anfängen der IT gibt. Im Allgemeinen bedeutet Sichern das Replizieren von Daten auf einem anderen Gerät oder an einem anderen Ort zur langfristigen Aufbewahrung oder Einhaltung von Vorschriften. Die Zeiten, in denen ein Backup allein ausreichende DR-Fähigkeiten bot, sind jedoch längst vorbei. Herkömmliche Backups bieten keine adäquaten Werte hinsichtlich Wiederherstellungszeit (RTO) und Wiederherstellungspunkt (RPO), da sie in der Regel die Systemproduktion beeinträchtigen und nur in regelmäßigen Abständen (alle paar Stunden oder einmal pro Tag) durchgeführt werden. Die Zeit, die für die tatsächliche Wiederherstellung von Daten aus dem Backup benötigt wird, kann jedoch Tage oder gar Wochen betragen.

Backup-Dienste haben in den letzten zwei Jahrzehnten versucht, Wiederherstellungszeiten und Wiederherstellungspunkte zu verbessern, doch erfüllen Backups noch immer nicht den Wiederherstellungsbedarf moderner Unternehmen, die ihre Dienste rund um die Uhr betreiben. Backups sind ein notwendiger Bestandteil einer IT-Umgebung, sollten aber um eine DR-Lösung ergänzt werden, um die Lücken zu füllen, die ein Backup nicht schließen kann.

Die Kosten von Ausfallzeiten und Datenverlusten

Während und nach einer Katastrophe können Ausfallzeiten und Datenverluste für Unternehmen extrem kostspielig werden. Bereits viele Unternehmen mussten ihre Türen für immer schließen, weil Katastrophen ihren Ruf, ihre Produktivität und ihre Umsätze irreparabel beschädigt haben. Ausfallzeiten und Datenverluste sind jeweils mit eigenen Kosten verbunden. Manchmal aber ist ein Datenverlust die Ursache für Ausfallzeiten, wie das bei Ransomware-Angriffen oft der Fall ist.

Ausfallzeiten

Vom Online-Shopping über Bankgeschäfte bis hin zum Streaming von Unterhaltungsdiensten erwarten wir heute, dass Dienste rund um die Uhr verfügbar sind. Selbst Unternehmen mit eingeschränkten Öffnungszeiten wie Restaurants oder Friseursalons verlassen sich bei Terminvereinbarungen und Reservierungen häufig auf digitale Dienste, von denen Kunden und Inhaber erwarten, dass sie jederzeit verfügbar sind.

Ausfallzeiten während der Betriebsstunden oder Hauptproduktionszeiten können kostspielige Unterbrechungen hinsichtlich Produktivität, Diensten und Transaktionen zur Folge haben. Dabei kann jede geplante oder ungeplante Ausfallzeit Produktivitäts- und Geschäftseinbußen sowie Verluste und eine Verschlechterung des Rufs zur Folge haben.

Datenverluste

Datenverluste, die sich in Minuten, Stunden oder Tagen bemessen, können für Unternehmen extrem kostspielig sein, vor allem, wenn die betroffenen Daten Produktivität, geistiges Eigentum oder wichtige Geschäftstransaktionen darstellen. Außerdem können Datenverluste zusätzliche Ausfallzeiten verursachen, wenn wichtige Systeme ohne aktuelle Daten nicht mehr richtig funktionieren.

Studien verschiedener Institute zeigen, dass Zahl und Kosten von Datenverlusten von Jahr zu Jahr steigen. Eine Business-Continuity-Strategie, die Verfügbarkeit sicherstellt, Datenverluste verringert und die Produktivität in jeder kompromittierenden Situation maximiert, ist für jedes Unternehmen eine unerlässliche digitale Sicherheitsstrategie. Die Frage ist nicht, ob eine Katastrophe eintreten wird, sondern *wann*.

FOLGEN VON DATENSTÖRUNGEN

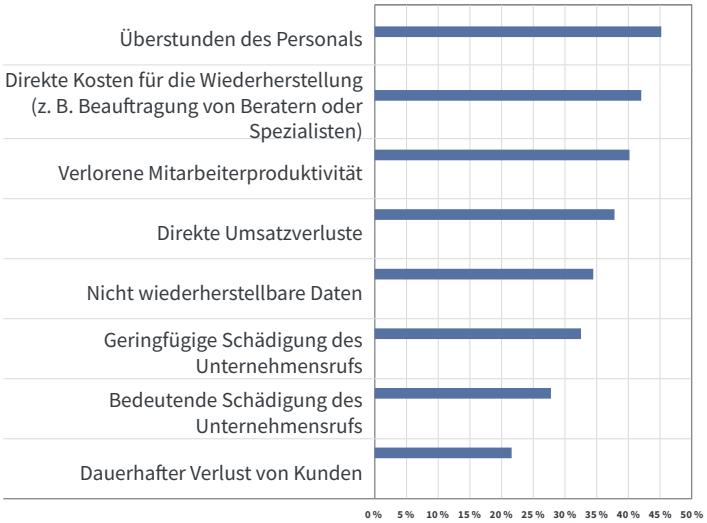


Abbildung 1. Als Hauptgrund für Datenverluste nannten Umfrageteilnehmer die Lücke zwischen einzelnen Backups. Unregelmäßige, periodische Backup-Lösungen sind nicht dazu geeignet, Datenverluste zu verhindern.

Quelle: IDC's Worldwide State of Data Protection and Disaster Recovery Survey, gesponsert von Zerto, Januar 2022

RTO und RPO für ungeplante Ausfallzeiten

Die Wiederherstellung im Katastrophenfall wird mit zwei Arten von Zielen ausgedrückt: Wiederherstellungszeit (RTO) und Wiederherstellungspunkt (RPO).

- Der RTO-Wert ist die Zeitspanne, die ein Unternehmen beeinträchtigt sein kann, ohne nennenswerte Verluste oder Risiken zu erleiden. RTO-Werte sind von Lösung zu Lösung sehr unterschiedlich, wobei viele Backup-Lösungen Tage oder sogar Wochen zur Wiederherstellung von Systemen benötigen.
- Der RPO-Wert ist der letzte Zeitpunkt, von dem Daten wiederhergestellt werden können. Herkömmliche Backup- oder Snapshot-Technologien haben RPO-Werte von nur 15 Minuten oder aber bis zu 24 Stunden.

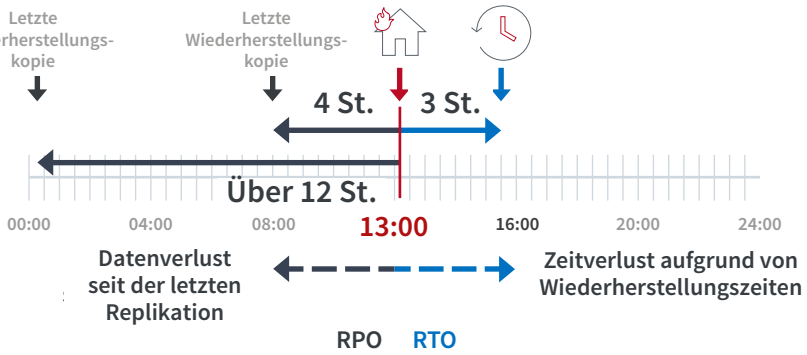
In einer modernen, digital ausgerichteten Welt müssen sowohl RTOs als auch RPOs so niedrig wie möglich sein. Sie dürfen nicht mehr in Stunden ausgedrückt werden, sondern müssen sich auf Minuten oder Sekunden belaufen. Viele Unternehmen konzentrieren sich auf RTOs, um nach einer Katastrophe den Betrieb so schnell wie möglich wieder aufzunehmen. Doch wird die Unfähigkeit, den Datenverlust zu reproduzieren – der RPO-Wert – ein Unternehmen noch lange nach einer Katastrophe beschäftigen.

ANWENDUNGSFÄLLE FÜR RTO UND RPO

RPO

Jedes Unternehmen, das an der Börse notiert ist, muss Regeln für Datensicherheit einhalten; Datenverluste führen zu Einbußen bei Umsätzen, Ruf und Unternehmenswert.

Ein Onlineshop, bei dem vier Stunden Daten verloren gehen, hat am Ende möglicherweise verärgerte Kunden, die sich fragen, warum ihre gekauften Waren nicht ankommen.



RTO

Wenn Systeme in einem Transportunternehmen für ein paar Stunden ausfallen, können Lieferungen und Abholungen nicht sinnvoll geplant werden, was enorme Folgen für die ohnehin schon unter Druck stehenden Umsätze hat.

Komplexe robotergestützte Produktionsprozesse, die nach einem Hardware- oder Softwarefehler ausfallen, verursachen enorme Produktivitäts- und Umsatzverluste.

Abbildung 2. RPOs und RTOs wirken sich in verschiedenen Unternehmen und Branchen unterschiedlich aus und können sowohl Produktivität als auch Umsatz beeinträchtigen. Beide Werte zu messen und zu definieren ist sehr wichtig, um den DR-Bedarf richtig einschätzen und abdecken zu können.

ABSCHNITT 2

Schlüsselüberlegungen zu einer Disaster-Recovery-Strategie

Bei der Entwicklung einer DR-Strategie müssen Sie viele Faktoren berücksichtigen, insbesondere bei der Auswahl der geeigneten Lösung zur Umsetzung Ihrer Strategie. Wenn Sie diese Faktoren verstehen, ist Ihr Unternehmen auf den Ernstfall vorbereitet.

Erzielen optimaler RTO- und RPO-Werte

Die beiden wichtigsten Faktoren im DR-Verfahren sind eine schnelle Wiederherstellung des Betriebs und die Vermeidung von Datenverlusten. Sowohl RTO (die Zeit, die benötigt wird, um das System wieder zum Laufen zu bringen) als auch RPO (die Menge der verlorenen Daten) sollten so niedrig wie möglich sein. Möglicherweise haben Sie genau definierte SLAs, die Sie mit Ihren RTOs und RPOs erreichen müssen. Doch unabhängig von Ihren SLAs gilt: Je besser Ihre RTOs und RPOs sind, desto weniger Zeit und Geld werden Sie im Katastrophenfall verlieren.

Die besten RTOs werden im Minutenbereich gemessen. Das können Sie auf zwei Arten erreichen:

1. Bei einem teilweisen oder begrenzten Ausfall des Primärsystems können Sie Daten und Systeme sofort aus einem lokalen Replikat wiederherstellen. Unabhängig davon, ob es sich bei dem lokalen Replikat um ein Backup, einen Snapshot oder ein CDP-Journal handelt, werden Daten mit der DR-Strategie sofort wieder in die Produktion eingespeist und der normale Systembetrieb ohne weitere Verzögerung wieder aufgenommen. Bei dieser Methode müssen der ursprüngliche Standort und dessen Systeme für die Wiederherstellung verfügbar sein.

2. Bei Szenarien, in denen der primäre Standort und dessen Systeme nicht verfügbar sind, ist ein Failover auf einen warmen Standort zur Wiederherstellung vorzuziehen. Das kann fast so schnell erfolgen wie eine lokale Wiederherstellung, da der warme Standort die gleichen oder ähnliche Replikate zur Wiederherstellung verwenden kann, die am primären Standort vorhanden waren, aber zum warmen Standort repliziert wurden. Das Umleiten der Benutzer über das Netzwerk zum warmen Standort für Zugriff auf die Anwendungen und Daten kann jedoch die RTO-Werte verringern, sodass diese Option möglicherweise langsamer ist als die erste.

Wenn Daten zu einem zweiten Standort repliziert werden, es aber keine orchestrierten und automatisierten Failover-Mechanismen gibt, um die Daten und Anwendungen schnell wieder online zu bringen, wird das RTO-Ziel ernsthaft beeinträchtigt und die vollständige Wiederherstellung der Systeme in Stunden oder sogar Tagen gemessen.

Die besten RPO-Werte liegen im Sekundenbereich. Sie beruhen auf Replikationstechnologien, die manchmal als echtzeitbasiert, synchron oder nahezu synchron bezeichnet werden und deren Intervalle in Sekunden gemessen werden. Ein weiterer Schlüsselfaktor bei der Replikation für RPO ist der applikationsorientierte Schutz. Unternehmensanwendungen bestehen aus verschiedenen VMs und Abhängigkeiten und müssen als einzelne, konsistente Einheiten mit akzeptablen RTOs und RPOs wiederhergestellt werden. Nicht alle Replikationstechnologien sind allein in der Lage, die Wiederherstellungskonsistenz zu sichern. Stattdessen müssen sie regelmäßige Prüfpunkte nutzen, wodurch die RPO-Werte von Anwendungen nicht Sekunden, sondern Minuten oder Stunden betragen.

Das Erreichen der bestmöglichen RTOs und RPOs minimiert auf einfache Weise die Kosten einer Katastrophe, indem die Störung auf ein Minimum reduziert wird. Je schneller Systeme mit den aktuellsten Daten wieder online sind, desto schneller kann das betroffene Unternehmen den Betrieb wieder aufnehmen.

DIE GRÖSSTEN HERAUSFORDERUNGEN BEIM SICHERN UND WIEDERHERSTELLEN

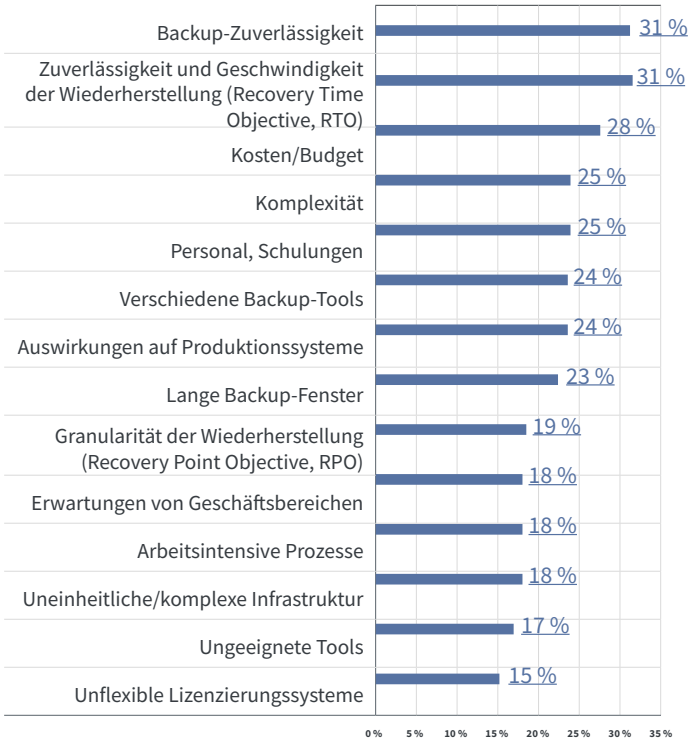


Abbildung 3. Abgesehen von den Kosten nannten Umfrageteilnehmer als größte Herausforderungen die Zuverlässigkeit und Komplexität ihrer Backup- und Recovery-Lösungen. Es wurden sowohl die Backup-Zuverlässigkeit als auch die Zuverlässigkeit bei der Wiederherstellung genannt, die sich sowohl auf RPO als auch auf RTO auswirken.

Quelle: IDC The State of Ransomware and Disaster Preparedness:↑ 2022

Ransomware-Resilienz

Früher wurden bei Cyberangriffen nur Daten gestohlen und es lag in der alleinigen Verantwortung von Cybersicherheitsexperten, sie zu stoppen. Ransomware hat aber Ausmaß und Folgen von Cyberangriffen verändert, sodass jetzt DR-Experten an der vordersten Front der Cybersicherheit stehen. Historische Trends zeigen, dass es für Unternehmen und andere Einrichtungen wie Schulen, Krankenhäuser und kommunale Behörden oft billiger ist, Lösegeld zu zahlen, wenn sie von Unterbrechungen betroffen sind und keine effektiven DR-Maßnahmen aufweisen. Dadurch setzt sich der Kreislauf von Ransomware fort. Ransomware ist inzwischen so weit verbreitet, dass es nicht mehr eine Frage des „ob“, sondern des „wann“ eines Angriffs auf Ihr Unternehmen ist.

Ransomware kann mit verschiedenen Verschlüsselungsmethoden angreifen, die einzelne Dateien bis hin zu ganzen Systemen betreffen. Anstelle einer Backup-Lösung brauchen Sie eine DR-Lösung, die Folgendes kann:

- Ihre Systeme bis zum letzten Zeitpunkt vor der Infektion zurücksetzen – bis auf wenige Sekunden.
- Die Wiederherstellung aller kritischen Systeme innerhalb weniger Minuten automatisieren – mit nur wenigen Mausklicks.
- Für den Fall, dass ein ganzer Standort kompromittiert wird, mehrere Kopien von Daten über mehrere Standorte hinweg erstellen.
- Ganze Anwendungen, Datenbanken und einzelne Dateien konsistent wiederherstellen.
- Jederzeit unterbrechungsfreie Failover-Tests durchführen, um sicherzustellen, dass Ihr Unternehmen sofort wieder online gehen kann.

- Durch Bereitstellung von On-Demand-Sandboxes für Sicherheitsscans bei der Erkennung von Ransomware helfen.
- Unter Verwendung von On-Demand-Sandboxes für Patch-Tests beim Sicherheitspatching helfen.
- Offsite-Datenkopien für unveränderbare Datenkopien und eine längerfristige Datenaufbewahrung erstellen.

Workload-Priorisierung

Je digitalisierter die Welt wird , desto wichtiger werden einige Ihrer IT-Systeme für die Bereitstellung von 24/7-Diensten, die Nutzer und Kunden erwarten. Beim Entwickeln einer DR-Strategie sollten Sie ermitteln, welche Systeme, Anwendungen und Daten den höchsten Grad an Datensicherheit und -verfügbarkeit benötigen und welche ggf. weniger. Das kann von Ihren SLAs abhängen; alternativ müssen Sie untersuchen, wie sich verschiedene Systeme auf Umsatzströme und Produktivität auswirken.

Für Kernanwendungen ist eine funktionierende DR-Strategie mit einem entfernten DR-Standort, niedrigen RTO- und RPO-Werten (geringer Datenverlust und kurze Wiederherstellungszeit) sowie einem getesteten Wiederherstellungsplan unerlässlich. Für andere Anwendungen und Datentypen können höhere RPO- und RTO-Werte akzeptabel sein.

Das Priorisieren ist ein Schlüsselelement für die Notfallplanung. Besprechen Sie mit Geschäftsinhabern, welche Ausfallzeiten für einzelne Anwendungen tolerabel sind. Es wird sich zeigen, welche Anwendungen schnell und mit minimalem Datenverlust verfügbar sein müssen.

Gesamtbetriebskosten

Beim Entwickeln einer DR-Strategie können Sie aus einer Vielzahl von Lösungen wählen. Die Kosten für die Lösungen sind unterschiedlich hoch. Das Gleiche gilt aber auch für ihre Effizienz. Darum sollten Sie nicht nur auf die Kosten für den Kauf oder die Lizenzierung der Lösung achten. Die Gesamtkosten umfassen zusätzliche Ausgaben für Implementierung, Verwaltung, Schulung und vor allem für die Wiederherstellung im Katastrophenfall, einschließlich der Kosten für Ausfallzeiten und Datenverluste. Nicht alle Lösungen bieten dieselben RTO- oder RPO-Werte. Außerdem müssen die Ausgaben für Wiederherstellungszeit und Datenverluste in die Gesamtkosten einkalkuliert werden. Manchmal kann eine Lösung, die im Vorfeld günstiger zu sein scheint, am Ende deutlich mehr kosten, wenn eine Katastrophe eintritt und Sie es mit einer schwierigen Wiederherstellung zu tun haben.

Außerdem sollten Sie die Anzahl der Tools berücksichtigen, die in einem Disaster-Recovery-Plan enthalten sein werden. So bringt beispielsweise ein Disaster-Recovery-Plan, der sich auf viele verschiedene und komplexe Technologien stützt, einen komplexen und schwierigen Wiederherstellungsprozess mit sich. Unter hohem Druck kann die Verwendung mehrerer Tools zu Fehlern führen – und das in einer Zeit, in der Fehler besonders teuer sind. Sie sollten eine zentrale Lösung in Betracht ziehen, die alle Komponenten Ihres Disaster-Recovery-Plans abdeckt.

Doch selbst innerhalb einer zentralen Lösung verursachen zusätzliche Tools manchmal zusätzliche Kosten. Der Preis einer Lösung kann drastisch steigen, wenn der Softwareanbieter z.B. eine Premium-Lizenzgebühr für zusätzliche Enterprise-Funktionen wie Orchestrierung oder Automatisierung verlangt.

Replikationstechnologien

Im Laufe der Jahre wurden zahlreiche Replikationstechnologien entwickelt. Viele davon wurden erarbeitet, bevor es Virtualisierung gab, und müssen daher noch virtualisierungs- oder cloudfähig gemacht werden. Der Schlüssel zu einer effektiven DR-Strategie besteht darin, diese Technologien zu verstehen und zu wissen, welche davon für die moderne digitale Welt der Virtualisierung und Cloud-Plattformen geeignet sind.

Array-basierte Replikation

Speicherhersteller bieten Array-basierte Replikationsprodukte an, die als Module innerhalb des Speicherarrays bereitgestellt werden. Es handelt sich dabei um Lösungen eines Anbieters, die nur mit der spezifischen, bereits verwendeten Speicherlösung kompatibel sind. Die Beziehung zwischen der VM und dem Speicher ist fest, und die gesamte LUN wird repliziert, unabhängig davon, ob sie ganz oder teilweise genutzt wird. Array-basierte Replikation wird zum Teil durch folgende Eigenschaften eingeschränkt:

- **Hardware-definiert.** Array-basierte Replikation ist für die Replikation physischer Einheiten konzipiert. Sie „sieht“ VMs nicht und bemerkt keine Konfigurationsänderungen.
- **Nicht unabhängig.** Obwohl sie für die Zusammenarbeit mit dem vorhandenen Speicher-Array optimiert ist, bindet Array-basierte Replikation Unternehmen an einen einzigen Anbieter.
- **Weitere Verwaltungspunkte.** Zusätzlich zur Verwaltungskonsole des physischen Speicherarrays muss die IT-Abteilung über eine Virtualisierungsverwaltungskonsole auch virtuelle Ressourcen verwalten.
- **Wachstum und Veränderungen.** Die Beziehung zwischen der VM und dem Speicher ist fest, wodurch die Flexibilität von Virtualisierung und die Möglichkeit, auf sich ändernde Geschäftsanforderungen zu reagieren, verloren gehen.
- **Granularität.** Da die gesamte LUN repliziert werden muss, fehlt der Array-basierten Replikation die in virtuellen Umgebungen erforderliche Granularität.
- **Kosten.** Die Replikation der gesamten LUN erhöht die Ausgaben für Strom, Kühlung, Netzwerk und Speicher, selbst wenn nur 40 % der LUN genutzt werden.
- **Ein einziger Wiederherstellungspunkt.** Viele Array-basierte Lösungen können keine Historie der LUN-Leistung speichern. Wenn der letzte Datenpunkt beschädigt wurde, müssen Unternehmen diesen für die Wiederherstellung verwenden, was die DR-Lösung unbrauchbar macht.
- **Zeitbedarf.** Ohne Automatisierung ist eine Wiederherstellung sehr zeitaufwändig und kompliziert; VMs und Anwendungen müssen von Grund auf neu eingerichtet werden.

Appliance-basierte Replikation

Appliance-basierte Replikationslösungen sind Hardware-basiert und spezifisch für eine einzige Plattform. Der Hauptunterschied zwischen Appliance-basierter und Array-basierter Replikation besteht darin, dass Appliance-basierte Replikation auf einer externen, physischen Appliance und nicht im Speicherarray selbst ausgeführt wird. Dadurch ist die Lösung flexibler und weniger ressourcenintensiv als Array-basierte Replikation. Die Nachteile sind jedoch mehr oder weniger die gleichen wie bei Array-

basierter Replikation. Appliance-basierte Replikation wird zum Teil durch folgende Eigenschaften eingeschränkt:

- **Hardware-definiert.** Konzipiert für die Replikation physischer Entitäten (und nicht für virtuelle Entitäten).
- **Nicht unabhängig.** Obwohl sie flexibler ist als Array-basierte Replikation, ist Appliance-basierte Replikation immer noch spezifisch für eine einzige Plattform.
- **Weitere Verwaltungspunkte.** Appliance-basierte Replikation erfordert zwei Verwaltungspunkte: die physische Verwaltungskonsole und die Virtualisierungsverwaltungskonsole.
- **Wachstum und Veränderungen.** Bei Appliance-basierter Replikation werden Konfigurationsänderungen nicht „gesehen". Das hat zur Folge, dass BC/DR-Pläne bald nicht mehr mit der aktuellen Produktionsumgebung übereinstimmen, was die Flexibilität von Virtualisierung zunichtemacht und Unternehmen die Möglichkeit nimmt, auf sich ändernde Geschäftsanforderungen zu reagieren.
- **Granularität.** Appliance-basierte Replikation konzentriert sich auf die logische Einheit und nicht auf die VM. Dieser Mangel an Granularität steht im Widerspruch zu den Anforderungen und Versprechen von Virtualisierung.
- **Kosten.** Bei Appliance-basierter Replikation wird außerdem die gesamte LUN repliziert, was die Ausgaben für Strom, Kühlung, Speicher und Netzwerk erhöht.

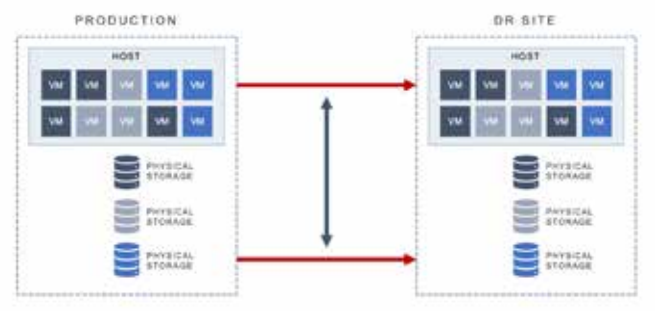


Abbildung 4. Array- und Appliance-basierte Replikationsmethoden erfordern die Koordination zweier Replikationsprodukte: eines für die physische Umgebung und eines für die virtualisierte Umgebung. Das erhöht die Komplexität der Verwaltung und untergräbt die in Virtualisierung getätigten Investitionen.

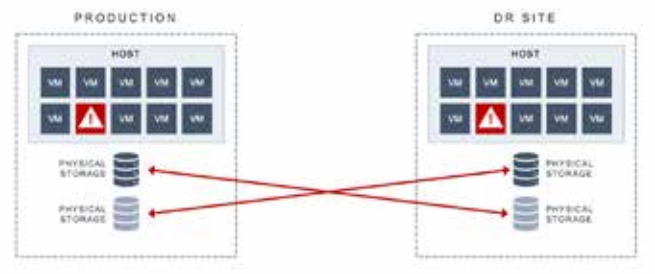


Abbildung 5. Das Spiegeln von Systemen über ein schnelles Netzwerk ermöglicht eine sehr hohe Verfügbarkeit; es werden aber auch beschädigte Softwarekomponenten repliziert.

Synchrone Replikation

Bei synchroner Replikation wird eine vollständige Kopie einer Infrastruktur an einem sekundären Standort erstellt und jeder Schreibvorgang dorthin kopiert oder entfernt. Bei einer Katastrophe wird ein automatischer Failover eingeleitet, und die Remote-Infrastruktur übernimmt den Betrieb. Diese synchrone Replikationsoption, die z. B. in MetroCluster von NetApp zu finden ist, klingt wie eine perfekte, wenn auch teure, Lösung. Sie basiert jedoch vollständig auf Hardware und ist mehr Hochverfügbarkeitslösung als Disaster-Recovery-Lösung. Das Failover funktioniert im Fall eines Hardwarefehlers, eines Stromausfalls oder einer Naturkatastrophe. Wenn die Störung jedoch softwarebasiert ist (z. B. beschädigte Datenbank oder ein Virus), wird sie auch auf den entfernten Standort repliziert. Dadurch wird die Replikation unbrauchbar, und das Team muss für die Wiederherstellung auf das nächtliche Backup zurückgreifen. Synchrone Replikation wird zum Teil durch folgende Eigenschaften eingeschränkt:

- **Festlegung auf Anbieter.** Der sekundäre Standort erfordert eine exakte Kopie der Hardware des primären Standorts, die vom selben Hersteller stammen muss.
- **Kosten.** Synchrone Replikation ist eine teure Lösung, die die Hardwarekosten buchstäblich verdoppelt und eine Netzwerklösung mit viel Bandbreite erfordert.
- **Unvollständig.** Komplett hardwarebasiert; im Falle einer softwarebasierten Katastrophe müssen Snapshots verwendet werden.

Gast-/OS-basierte Replikation

Bei einer Gast-/OS-basierten Replikationslösung müssen auf jedem einzelnen physischen und virtuellen Server Softwarekomponenten installiert werden. Das ist zwar deutlich portabler als bei Array-basierten Lösungen, doch sind Gast-/OS-basierte Replikationslösungen für Unternehmen ungeeignet.

Abbildung 6. Host-basierte Replikation erfordert einen Agenten auf jeder VM, was die Komplexität erheblich erhöht.

Gast-/OS-basierte Replikation wird zum Teil durch folgende Eigenschaften eingeschränkt:

- **Wachstum und Veränderungen.** Die Anforderung, auf jedem Server ein Modul zu installieren, schränkt die Skalierbarkeit ein und macht eine Implementierung und Verwaltung in großen Unternehmensumgebungen unmöglich. Außerdem kann der Overhead der einzelnen Agenten auf den VMs zu Leistungsproblemen bei Anwendungen führen, auf die Unternehmen angewiesen sind.
- **Komplexität.** Schatten-VMs sind oft Teil einer Gast-/OS-basierten Replikation, was Komplexität und Verwaltungsaufwand erhöht.
- **Keine Anwendungskonsistenz.** Jede VM ist einzeln geschützt, was es unmöglich macht, Gruppen von VMs für eine Anwendung zu verwalten und konsistent zu replizieren.
- **Hoher Verwaltungsaufwand.** Alle Agenten müssen verwaltet und gepflegt werden. Während das in kleineren Umgebungen kein allzu großes Problem darstellt, werden Verwaltung und Wartung bei Umgebungen, die mehr als 20 VMs aufweisen, zu einer viel größeren Herausforderung. Das Pflegen und Aktualisieren der Disaster-Recovery-Strategie wird jetzt zu einer Wochenendaufgabe, die oft Ausfallzeiten erfordert.

Snapshots

Viele Lösungen nutzen Snapshots, um eine schnelle Wiederherstellung zu erlauben. Ein Snapshot ist eine Möglichkeit, ein Live-Speichersystem oder eine VM zu einem bestimmten Zeitpunkt „einzufrieren“, während nach der Snapshot-Erfassung weiter Änderungen vorgenommen werden können. Wenn nach der Snapshot-Erfassung Änderungen vorgenommen werden und bei der VM oder dem Speichersystem ein Problem auftritt, ist es möglich, die Veränderungen zu verwerfen, indem die VM oder das Speichersystem auf den Snapshot-Zustand zurückgesetzt wird. Ein Snapshot ist besonders nützlich, wenn Änderungen an einer einzelnen VM, bei denen ein Rollback erforderlich sein könnte, vorgenommen wurden.
Bei Snapshot-basierter Replikation werden Snapshots vom Produktionsstandort an einen Zielstandort kopiert, wo sie verwendet werden können, um die VM zum nächstmöglichen Zeitpunkt neu zu erstellen. Wie ein inkrementelles Backup enthält ein Snapshot nur die Daten, die sich seit dem letzten Snapshot geändert haben, sodass sich Snapshots durch eine hohe Speicher- und Bandbreiteneffizienz auszeichnen. Im Vergleich zu kontinuierlicher Echtzeitreplikation werden sie jedoch häufig nur selten durchgeführt und dienen eher als Backup denn als Disaster Recovery.

Vor- und Nachteile von Snapshot-basierter Replikation

Disaster Recovery mit Hypervisoren

Vorteile	Nachteile
Effizient	**Unregelmäßig**
Da Snapshots nur Daten enthalten, die sich seit dem letzten Snapshot geändert haben, benötigen sie relativ wenig Speicherplatz und sind bei der Replikation bandbreiteneffizient. Die Größe des Snapshots hängt vom Tempo der Datenänderungen und der Häufigkeit des Snapshot-Zeitplans ab. In manchen Umgebungen, z. B. in Public Clouds, kann Snapshot-basierte Replikation eine effiziente Möglichkeit sein, die Kosten für ausgehende Daten zu senken.	Die Häufigkeit von Snapshots ist wegen der Leistungsbeeinträchtigungen oft auf Inkremente von nicht weniger als 15 Minuten beschränkt. Erstellung von Snapshots von vielen VMs gleichzeitig oder Zeitaufwand für die Erstellung von Snapshot-Stapeln und Replikation zwischen Intervallen. Im Vergleich zu kontinuierlichen Datensicherungs- oder Echtzeit-Replikationstechnologien schaffen diese Intervalle eine größere Lücke zwischen Wiederherstellungspunkten. Das könnte man jedoch auch als Kompromiss für Effizienz in großem Maßstab betrachten.
Agentenlos	**Auswirkungen auf die Leistung**
VM-Snapshots erfordern keine Installation eines Agenten auf der VM, sondern werden direkt von der zugrunde liegenden Virtualisierungs- oder Speicherplattform ausgeführt. Agentenlose Replikation ist ein wichtiger Verwaltungsvorteil bei der Skalierung von Schutz und der Verringerung der Leistungsbeeinträchtigungen bei VMs.	Je nach Virtualisierungsplattform oder Speichersystem haben Snapshot-Technologien unterschiedliche Auswirkungen auf die Systemleistung, während ein Snapshot oder ein Stapel von Snapshots erstellt wird. Snapshots können den VM-Betrieb durch ein kurzes, sekundenschnelles Einfrieren direkt beeinträchtigen bzw. die Leistung des Speichersubsystems oder die CPU-Leistung des Hostsystems beeinflussen.

Hypervisor-Anbieter wie VMware bieten oft eigene softwarebasierte Replikationslösungen an, die jedoch auf den eigenen Hypervisor beschränkt sind. Eine Lösung wie VMware vSphere Replication (VR) bietet begrenzte Replikationsfunktionen und umfasst nicht alle Orchestrierungs-, Test-, Berichts- und DR-Funktionen der Enterprise-Klasse, die eine vollständige DR-Lösung ausmachen. Selbst in Kombination mit VMware Site Recovery Manager (SRM) reichen die Wiederherstellungszeit und Skalierbarkeit von VR möglicherweise nicht aus, um die Anforderungen Ihres Unternehmens zu erfüllen. SRM bietet zwar zusätzliche Funktionen für das Planen, Testen und Ausführen eines DR-Plans, kann aber die Replikationsbeschränkungen von VR nicht überwinden, da VMware vSphere Replication Snapshot-Technologie für virtuelle Maschinen verwendet.

Software-definierte Replikation

Alle zuvor genannten Kategorien von Replikationstechnologien weisen in Bezug auf moderne virtualisierte und cloudbasierte Architekturen entscheidende Einschränkungen auf. Sie untergraben die Versprechen von Virtualisierung und Cloud und schränken die Möglichkeiten einer plattformübergreifenden, hybriden IT-Infrastruktur ein. Um DR in Ihrer modernen IT-Infrastruktur richtig zu realisieren, ohne Kompromisse bei Einfachheit und Kosten eingehen zu müssen, benötigen Sie einen neuen Ansatz: Software-definierte Replikation. Zerto hat Replikation von der Speicherebene über die Ressourcenabstraktionsebene in die Virtualisierungs-/Hypervisor-/Cloud-Ebene verlagert.

Disaster Recovery: Lokal oder in der Cloud

Eine häufig gestellte Frage im Zusammenhang mit DR ist, ob ein lokaler DR-Standort, ein gehosteter Standort oder die Public Cloud am besten geeignet ist. Jede dieser Optionen kann in Abhängigkeit von verschiedenen Faktoren eine gute Wahl darstellen.

- **Verfügbarkeit eines geeigneten lokalen Standorts.** Ein DR-Standort sollte geografisch weit genug von Ihrem Produktionsstandort entfernt sein, um Sie auch bei regionalen Katastrophen zu schützen. Außerdem muss der Standort über eine ausreichende Stromversorgung, Kühlung und Konnektivität (Bandbreite) verfügen, um als DR-Standort geeignet zu sein. Durch Nutzung der Cloud lassen sich diese Herausforderungen schnell bewältigen.
- **CAPEX vs. OPEX.** Aufgrund der beträchtlichen IT-Ressourcen, die für den Aufbau und die Wartung der Infrastruktur erforderlich sind, kann das Einrichten eines lokalen DR-Standorts mit hohen Investitionskosten verbunden sein. Ein gehosteter Standort oder eine Public Cloud bieten hingegen mehr Flexibilität beim Cashflow und stellen eine Betriebsausgabe dar, bei der die Kosten eventuell gleich hoch, aber auch besser vorhersehbar sind. Es gibt einige wichtige Unterschiede zwischen den beiden Modellen, die Sie berücksichtigen sollten, bevor Sie sich für eine Option entscheiden.
- **Expertise und Personalausstattung.** Der Aufbau und die Wartung eines lokalen DR-Standorts erfordert wahrscheinlich mehr Personal und in einigen Fällen auch mehr Expertise. Bei einer gehosteten oder Public-Cloud-Option sind die Wartungskosten für den Standort in den wiederkehrenden Gebühren enthalten, was zusätzliches Personal überflüssig machen (oder zumindest minimieren) kann.

Mit dem richtigen Standort und den richtigen Mitarbeitern sowie den entsprechenden Investitionen kann eine On-Premise-Lösung eine

gute und kostengünstige Wahl sein. Andererseits bieten gehostete Websites und die Public Cloud einen sofort einsatzbereiten Standort zu wiederkehrenden Kosten.

Disaster-Recovery-as-a-Service-Lösungen

Nicht jedes Unternehmen verfügt über einen geeigneten Standort für DR oder das Fachwissen, um eine Lösung selbst zu implementieren, sei es vor Ort oder in der Cloud. Für solche Unternehmen kann Disaster-Recovery-as-a-Service (DRaaS) eine perfekte Lösung sein. DRaaS bietet einen resilienten, entfernten, cloudbasierten Standort für DR, DR-Spezialisten, die die Lösung verwalten, und vorhersehbare, wiederkehrende Kosten.

Doch sind nicht alle DRaaS-Lösungen gleich. Verschiedene DRaaS-Lösungen haben einen unterschiedlichen Verwaltungsbedarf. Bei manchen Diensten können Sie einen Teil der DR-Lösung selbst verwalten. Je nach Bedarf Ihres Unternehmens können Sie von verschiedenen Verwaltungsebenen mehr oder weniger profitieren.

Wie bei jeder DR-Lösung hängt die Effektivität von DRaaS letztendlich von der zugrunde liegenden Technologie ab. Leider nutzen viele DRaaS-Lösungen immer noch veraltete Sicherungs- und Replikationstechnologien, die schlechte RPOs und RTOs bieten. Die Evaluierung von Wiederherstellungszeiten und -punkten ist nicht nur entscheidend für die Einhaltung von SLAs, sondern auch für die Senkung der Kosten einer Lösung, sollte es zu einer Katastrophe kommen. Ausgaben für Ausfallzeiten und Datenverluste, die durch veraltete Technologien wie Snapshot-basierte Replikation oder langsame manuelle Wiederherstellungen wahrscheinlicher werden, erhöhen die Kosten der Lösung.

Um Sie bei der Bewertung von DR-Lösungen, einschließlich DRaaS, zu unterstützen, haben wir eine Anforderungs-Checkliste erstellt, die Sie auf der folgenden Seite finden.

Checkliste für Disaster-Recovery-Anforderungen –

sowohl für interne als auch für DRaaS-Lösungen

Leistung

1. Bietet die DR-Lösung kontinuierliche Replikation? Welche Auswirkungen hat die jeweilige Technologie (z. B. Snapshots) auf den Produktionsstandort?
2. Welche RTO- und RPO-Werte bietet die Lösung? Werden sie in Sekunden, Minuten oder Stunden gemessen? Lässt sich das nachweisen, und haben Sie kontinuierlich Einblick?
3. Entsprechen die RPO/RTO-Werte realistischerweise Ihren geschäftlichen Anforderungen, und zu welchen Opfern oder Kosten?
4. **DRaaS** – Bietet der Cloud Service Provider eine zuverlässige und schnelle Netzwerklösung an, und sorgt die DRaaS-Lösung für Netzwerkeffizienzen wie Komprimierung?

Unterstützung für Ihre Systeme

5. Ist die DR-Lösung speicher- und hypervisorunabhängig? Mit anderen Worten: Können Sie von jeder Umgebung aus zur DR-Lösung replizieren?
6. Ist die Lösung anwendungsbezogen? Erlaubt sie Wiederherstellungen von einem konsistenten Zeitpunkt, selbst bei Multi-VM-Anwendungen, die auf unterschiedliche Hosts und Datenspeicher angewiesen sind?
7. Wie skalierbar ist die Lösung (in einer DRaaS-Umgebung aufwärts und abwärts)?
8. Wie sieht die Installation aus? Müssen Sie Anwendungen, LUNs und VMs neu konfigurieren?
9. Unterstützt die DR-Lösung Änderungen, z. B. wenn VMs an andere Speicherorte verschoben werden oder wenn Sie eine Migration durchführen möchten?
10. Bietet die Lösung Flexibilität und die Möglichkeit, die als Ziel-DR-Standort zu verwendende Public Cloud zu wechseln?
11. **DRaaS** – Unterstützt die Lösung mehrere Standorte, und ist sie mandantenfähig? Bietet sie sicher isolierte Datenströme für geschäftskritische Anwendungen und Compliance?

Funktionen

12. Handelt es sich um eine vollständige Offsite-Schutzlösung, die Speicherplatz sowohl für DR- als auch für Archivierung (Backups) bietet, mit sehr geringen Beeinträchtigungen des Produktionsstandorts?
13. Ist sie sowohl für Hardware- als auch für logische Ausfälle geeignet?
14. Bietet sie ausreichende Failover- und Failback-Funktionen, einschließlich Automatisierung und Orchestrierung der Wiederherstellung, Skripte vor und nach der Wiederherstellung, automatische IP-Anpassung usw.?
15. Wie würde sich ein Failover oder Failback auf die Produktion auswirken? Und wie sieht der Failback-Prozess aus? Ähnelt er dem Failover-Prozess?

Compliance

16. Kann die Lösung leicht getestet werden, und sind Testberichte verfügbar? Was sind die Auswirkungen der Tests? Kann das während der Geschäftszeiten erfolgen, oder ist dies eine Wochenendaktivität? Muss die Produktion heruntergefahren werden? Wird die Replikation während der Tests angehalten oder unterbrochen, und beeinträchtigt dies die DR-Lösung bei jedem Test?
17. **DRaaS** – Gibt es Lizenzprobleme oder andere Investitionen, die im Voraus zu tätigen sind?
18. **DRaaS** – Wo werden die Daten gespeichert? Hält der Dienstleister die Vorschriften der EU ein?

Benutzerfreundlichkeit

19. Ist die Lösung einfach zu erlernen und zu benutzen? Fügt sie Ihrer Umgebung weitere Verwaltungskontrollpunkte hinzu, oder lässt sie sich nahtlos integrieren?
20. Bietet sie die richtige Wiederherstellungsgranularität? Können Sie eine Datei, eine einzelne VM, eine einzelne Anwendung, einige Anwendungen oder den gesamten Standort wiederherstellen?
21. **DRaaS** – Bietet die DRaaS-Lösung sowohl Self-Service als auch Managed Services?

ABSCHNITT 3

Zerto

Zerto basiert auf einem Fundament aus Continuous Data Protection (CDP). Die Lösung vereint DR, Ransomware-Resilienz und Multi-Cloud-Mobilität. Zerto-Benutzer profitieren von einer einheitlichen und automatisierten Wiederherstellung und Datenverwaltung für virtualisierte und Cloud-Workloads.

Zerto vereinfacht den Schutz, die Wiederherstellung und die Mobilität von Anwendungen und Daten in privaten, öffentlichen und hybriden Clouds und sorgt so für ein optimales Nutzererlebnis.

Vorteile von Zerto Disaster Recovery

Die CDP-Technologie von Zerto bietet die branchenweit besten RPO- und RTO-Werte, um jede Art von Unterbrechung abzufedern, einschließlich Naturkatastrophen, Hardwareausfällen, Ransomware und anderen geplanten oder ungeplanten Ausfällen. So haben Sie die Gewissheit, dass Datenverluste und Ausfallzeiten Ihren laufenden Betrieb nicht unterbrechen. Darüber hinaus arbeitet Zerto CDP cloud- und plattformübergreifend und hilft Ihnen, das Potenzial einer hybriden und Multi-Cloud-Welt voll auszuschöpfen.

Continuous Data Protection

- **RPOs im Sekundenbereich.** Erzielen Sie durch permanente Replikation und kontinuierliche Backups lokal, remote und plattformübergreifend RPOs im Sekundenbereich.
- **RTOs im Minutenbereich.** Failover eines gesamten Standorts oder ausgewählter Workloads auf einen entfernten Standort in nur wenigen Minuten und mit nur wenigen Klicks.
- **Nahezu synchrone Replikation.** Vereint das Beste aus synchroner und asynchroner Replikation. Zerto ist eine reine Softwarelösung, die auf der Hypervisor-Ebene angesiedelt ist und völlig unabhängig von der zugrundeliegenden Hardware und Infrastruktur, einschließlich Speicher, arbeitet.
- **Einzigartige Journaling-Funktionen.** Zerto ermöglicht eine kontinuierliche Replikation auf Blockebene ohne Beeinträchtigung der Anwendungsleistung. Alle Checkpoints werden im Abstand

von Sekunden für bis zu 30 Tage im Journal gespeichert, um für RPOs im Sekundenbereich zu sorgen und Dateien, Ordner und VMs – sogar ganze Anwendungen und Standorte – praktisch ohne Datenverlust wiederherzustellen.

- **Anwendungsbezogener Schutz.** Unternehmensanwendungen umfassen verschiedene VMs und Abhängigkeiten. Herkömmliche Methoden wie inkrementelle Backup-Jobs stellen eine große Herausforderung dar, wenn Anwendungen konsistent und mit einem akzeptablen RTO-Wert wiederhergestellt werden sollen. Zerto löst diese Herausforderung mit der Funktion Virtual Protection Group (VPG). Mit VPGs können Sie eine ganze Anwendung (inklusive aller dazugehörigen VMs) mit einem Klick schützen und wiederherstellen, und zwar zu einem konsistenten Zeitpunkt und mit zuverlässiger Schreibreihenfolge.

- **Ransomware-Wiederherstellung auf die Sekunde genau.** CDP liefert einen kontinuierlichen Strom von Wiederherstellungsprüfpunkten. Im Falle von Ransomware oder anderen bösartigen Angriffen können Daten zu einem Zeitpunkt nur wenige Sekunden vor der Beschädigung wiederhergestellt werden, was die negativen Folgen für das Unternehmen und die Marke minimiert.

- **Echtzeit-Erkennung von Verschlüsselung.** Erkennungs- und Warnfunktionen warnen Benutzer bei verschlüsselungsbezogenen Anomalien, damit sie die frühesten Stadien eines Ransomware-Angriffs erkennen und entschärfen können.

Multiplattform- und Multi-Cloud-Unterstützung

Zerto unterstützt verschiedene Plattformen und Cloud-Konfigurationen. Bei Zerto profitieren Sie von folgenden Vorteilen:

- **Unabhängigkeit von Hardware und Hypervisor.** Beseitigen Sie Innovationsbarrieren mit einer Replikationslösung, die keine Hardware- oder Hypervisor-Abhängigkeiten aufweist und nicht an einen bestimmten Anbieter gebunden ist.

- **Einfache und nahtlose Installation.** Die Installation erfolgt nahtlos innerhalb weniger Minuten in die bestehende Infrastruktur, ohne dass Ausfallzeiten oder Konfigurationsänderungen erforderlich sind.

- **Skalierbar und granular.** Skalierung auf Tausende von VMs möglich. Verwenden Sie Cloud-Instanzen für Granularität, um jeden Workload einzeln zu verwalten.

- **One-to-many-/Multi-Platform.** Einfache, unterbrechungsfreie Replikation in die Public Cloud, zu einem Dienstanbieter oder zu einem sekundären Standort – sogar auch gleichzeitig für zusätzliche Wiederherstellungsoptionen.

- **SaaS-Backup für geschäftskritische Daten.** Zerto Backup for SaaS, powered by Keepit, bietet nicht nur Schutz für virtualisierte Workloads in lokalen und Cloud-Plattformen, sondern auch Backups für Ihre Daten bei Plattformen wie Microsoft 365, Salesforce, Google Workspace, Microsoft Azure AD und Microsoft Dynamics 365. Diese Daten können genauso wertvoll sein wie alle Daten, die Sie lokal schützen. Zerto gibt Ihnen die Gewissheit, dass Daten bei diesen Plattformen im Falle einer Katastrophe oder Störung geschützt sind.

Verwaltung und Orchestrierung

Automatisierung und Orchestrierung machen die Dinge mit Zerto einfach und bieten Ihnen:

- **Automatischen VM-Schutz.** Der automatische VM-Schutz mithilfe von vSphere-Tags gewährleistet vollständigen, flexiblen Datenschutz in Ihrer gesamten Umgebung, selbst wenn Sie neue VMs hinzufügen.

- **Einfache und zentralisierte Verwaltung.** Zentrale Verwaltung von lokalen und cloudbasierten Lösungen. Verwenden Sie vollständige APIs für Integration und Automatisierung.

- **Katastrophenvermeidung.** Proaktives Failover oder Migration zu anderen Standorten, bevor ein Zwischenfall eintritt (z. B. bei einem nahenden Wirbelsturm oder einer anderen vorhersehbaren potenziellen Katastrophe).

- **On-Demand-Sandboxes.** Erstellen Sie Sandbox-Versionen Ihrer Produktionsumgebung für unterbrechungsfreie DR-Tests, Update- und Patch-Tests, Malware-Scans und vieles mehr. Testen Sie den gesamten Wiederherstellungsprozess, ohne Produktionsumgebungen oder laufende Replikation zu beeinträchtigen, und bieten Sie Ihrem Team im Falle einer Katastrophe ein gutes Gefühl.

Compliance

Die Funktionen von Zerto erleichtern die Einhaltung verschiedener regulatorischer Bestimmungen, von SLAs bis hin zu behördlichen Anforderungen. Bleiben Sie konform mit:

- **Berichterstattung und Analytics.** Umfasst automatisierte Disaster-Recovery-Berichte zur Einhaltung von Vorschriften und zur Überprüfung des Systemzustands.

- **Ransomware-Resilienz.** Ganze Anwendungen, Datenbanken oder einzelne Dateien lassen sich konsistent und granular wiederherstellen. Führen Sie jederzeit unterbrechungsfreie Failover-Tests durch, um sicher zu sein, dass Sie Ihr Unternehmen sofort wieder online bringen können.

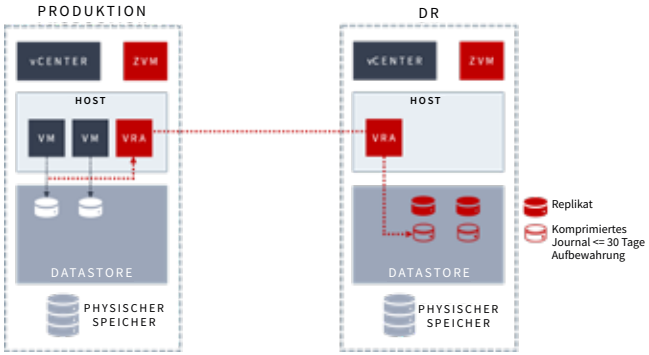
- **Support der Enterprise-Klasse.** Erhalten Sie Support-Leistungen der Enterprise-Klasse, die in alle Zerto-Produkte integriert sind. Zu Support-Leistungen gehören Echtzeitwarnungen, wenn RPO/RTO-Ziele nicht erreicht werden, Alarme bei Netzwerkverschlechterung und Erinnerungen zur Überprüfung von Konfigurationen und VPGs. Lösungen von Zerto werden von globalen Support Service Centern unterstützt, die bei Bedarf Zugang zu einem Expertenteam von Supportingenieuren bieten.

Die Zerto-Architektur

Das Herzstück der CDP- und Replikationstechnologie von Zerto besteht aus zwei Komponenten:

- **Zerto Virtual Manager.** Zerto Virtual Manager (ZVM) ist eine sicherheitsverstärkte virtuelle Appliance, die in die zugrunde liegende Plattform integriert ist, um Replikation, gepaarte Standorte, VM-Schutz und Leistung zu verwalten. Wenn ein Problem auftritt, stellt ZVM es visuell dar und sendet außerdem Warnmeldungen. Außerdem ist ZVM für die Orchestrierung und Automatisierung von Failback- und Wiederherstellungsprozessen wie Bootreihenfolge, Re-IP, Skripte, Test- und Validierungsoptionen zuständig.

- **Zerto Virtual Replication Appliance.** Die Virtual Replication Appliance (VRA) ist eine VM, die auf jedem virtuellen Host oder jeder Cloud-Umgebung läuft. Sie sorgt für ständig aktive Replikation auf Blockebene zu einem oder mehreren entfernten Standorten. Im Gegensatz zu agentenbasierter Replikation übernimmt die VRA die Replikation von den VMs und eliminiert so Leistungsbeeinträchtigungen bei diesen VMs. Und anders als bei Snapshot-basierter Replikation kann die VRA Daten alle fünf Sekunden replizieren und so nahezu unmittelbare RPO-Werte unterstützen.



Anwendungsbezogener Schutz: Virtual Protection Groups

Viele Unternehmensanwendungen umfassen mehr als einen virtuellen Server (z. B. Web-, Anwendungs- und Datenbankserver), die voneinander abhängig sind. Wenn eine Wiederherstellung erforderlich ist, müssen alle Server zu einem einzigen, konsistenten Zeitpunkt wiederhergestellt werden. Zu diesem Zweck hat Zerto VPGs entwickelt, die die Konsistenz der Festplatten in einer Gruppe von VMs sicherstellen. VPGs replizieren und stellen Unternehmensanwendungen konsistent wieder her, unabhängig von der zugrunde liegenden Infrastruktur. Zerto erkennt und bewahrt die Beziehungen und unterstützt gleichzeitig wichtige VMware-Funktionen wie DR, vMotion und Storage vMotion.

Zerto VPGs sind so konzipiert, dass sie Replikation und Wiederherstellung mit folgenden Merkmalen ermöglichen:

- **Konsistent.** Repliziert und stellt komplette Multi-VM-Anwendungen konsistent wieder her.
- **Flexibel.** Ermöglicht es Unternehmen, eine Anwendung auf verschiedenen physischen Geräten bereitzustellen, um die Leistung oder Kapazität zu maximieren bzw. die Komplexität der Infrastruktur zu reduzieren.
- **Granular.** Bietet bei vielen Arten von Katastrophen die richtige Granularität für die Wiederherstellung einzelner VMs sowie von Gruppen von VMs.
- **Priorisiert.** Priorisiert VPGs für Replikation und Wiederherstellung.
- **Unterstützt.** Unterstützt Virtualisierungsfunktionen wie vMotion, svMotion, HA etc.

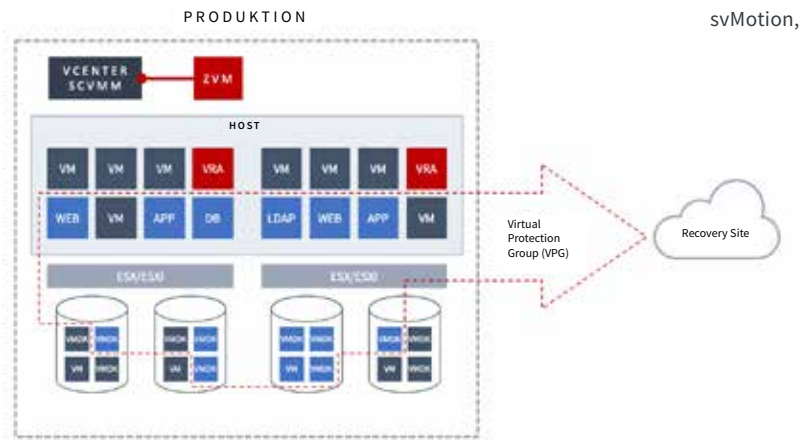


Abbildung 7. Die verschiedenen VMs, aus denen eine Anwendung besteht, befinden sich in einer VPG und werden konsistent repliziert, auch wenn sie auf verschiedene Hosts und Datenspeicher verteilt sind.

Automatischer Schutz virtueller Maschinen

In modernen Rechenzentren werden schnell und häufig neue VM-Workloads eingerichtet und bereitgestellt, insbesondere in virtualisierten Umgebungen. Allerdings kann es sehr mühsam sein, jede neu erstellte VM über eine Verwaltungsoberfläche zu schützen. Durch Verwendung von VM-Tags in vSphere ermöglicht Zerto eine automatische Erstellung von VPGs und schützt VMs, ohne dass Sie ZVM öffnen müssen. Systemadministratoren können sicherstellen, dass VMs bei der Erstellung geschützt und einer aktuellen oder neuen VPG zugewiesen werden, ohne eine weitere Verwaltungsschnittstelle öffnen zu müssen.

Vollständig konfigurierter Failover-Prozess

Ein Schritt der VPG-Konfiguration ist die Einrichtung des Failover-Prozesses. Bei dieser Konfiguration werden Bootreihenfolge, Re-IP bei Failover, Länge des Journals und andere Parameter kalibriert. Wenn diese Vorarbeiten abgeschlossen sind, wird der Wiederherstellungsprozess vereinfacht und benötigt nur noch wenige Klicks.

Vollständig automatisiert und orchestriert

Bei DR ist die Replikation von Daten zum Wiederherstellungsstandort nur die halbe Miete. Die andere Hälfte besteht aus der schnellen und einfachen Nutzung der Informationen zum Schutz der Geschäfte im Katastrophenfall. Zerto hat das Problem erkannt und hat automatisierte und orchestrierte Prozesse entwickelt, die Sie mit nur wenigen Klicks ausführen können, wenn die IT-Abteilung in einer Drucksituation steckt.

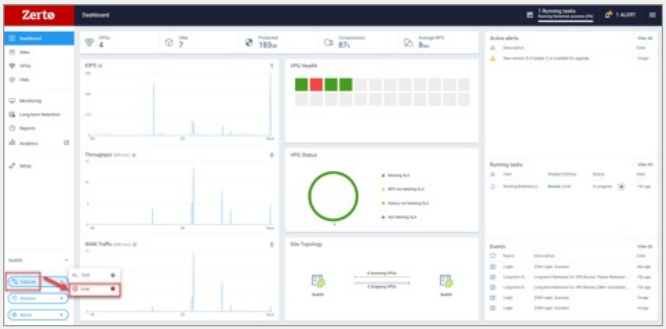
Failover als geschäftliche Entscheidung

Da jede Katastrophe anders ist, ist Zerto der Meinung, dass Failover eine geschäftliche Entscheidung sein sollte und kein automatisierter Prozess. Da Sie einen Zeitpunkt wählen können – den Zeitpunkt, kurz bevor eine Datenbankbeschädigung auftrat –, ist diese Entscheidungsphase für ein korrektes Failover-Verfahren von großer Bedeutung. Nach dem Anklicken der Failover-Schaltfläche wird ein automatisierter und orchestrierter Prozess gestartet, um Dienste wieder online zu bringen.

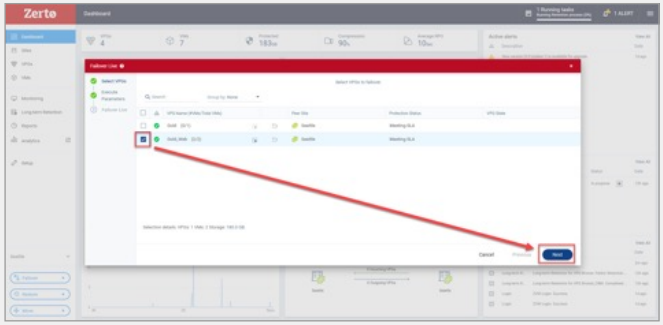
SCHNELLER 4-STUFIGER FAILOVER-PROZESS

Der Failover-Prozess besteht aus vier einfachen Schritten. Nachdem ein Vorfall in der Verwaltungskonsole sichtbar ist:

1. Klicken Sie auf Failover Live. ⟶

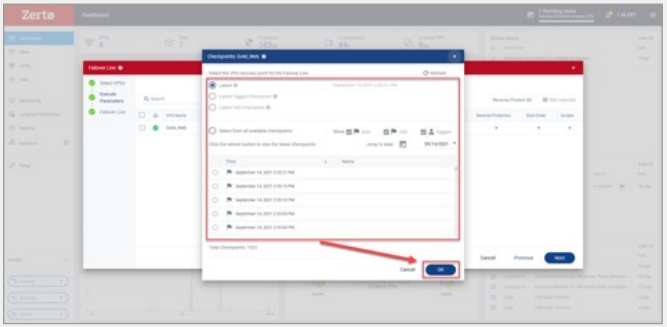


2. Wählen Sie die Anwendungen (VPGs), die wiederhergestellt werden müssen, aus der Liste aus.

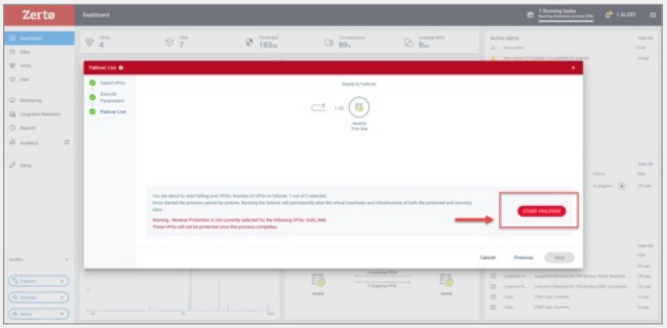


3. Überprüfen Sie den Zeitpunkt, zu dem die Anwendungen wiederhergestellt werden sollen. Möglich ist eine Wiederherstellung auf den:

- Letzten Prüfpunkt (Standardeinstellung)
- Zuletzt getaggten Prüfpunkt
- Letzten VSS-Prüfpunkt
- Bestimmten Zeitpunkt aus der Liste aller verfügbaren Prüfpunkte



4. Starten Sie den Failover-Prozess. Der Wiederherstellungsprozess beginnt und VMs werden in der Wiederherstellungsumgebung gebootet und nach Bedarf neu konfiguriert.



Automatischer Failover und Failback

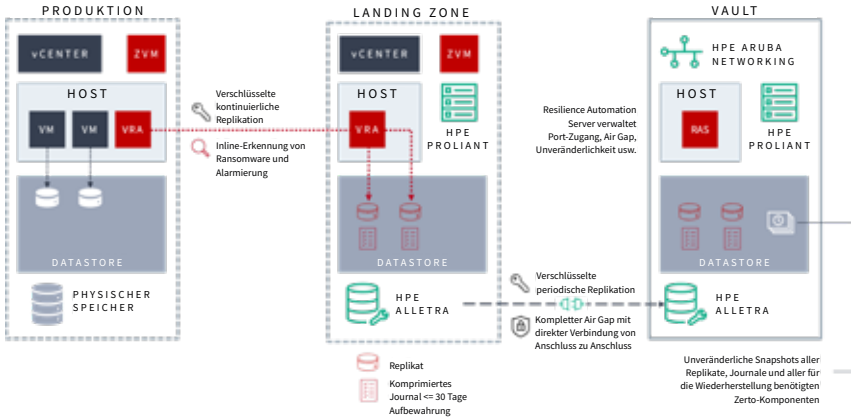
Nach der Konfiguration der VPGs ist der Wiederherstellungsplan nun einsatzbereit. Skripte zur Vor- und Nachbereitung einer Wiederherstellung können auch für jede VPG einzeln konfiguriert werden. Failover und Failback lassen sich jetzt mit wenigen Klicks vornehmen. Selbst wenn der DR-Prozess eingeleitet wird, besteht die Möglichkeit, den Failover zurückzusetzen, falls am Wiederherstellungsstandort Probleme auftreten, die nicht mit Zerto zusammenhängen (z. B. ein Netzwerkausfall).
Nach einem erfolgreichen Failover wird der Failback-Prozess durch den sog. Reverse-Protection Prozess noch einfacher. Sobald der Produktionsstandort einsatzbereit ist, startet die Reverse-Protection mit dem Synchronisieren zwischen der am Wiederherstellungsstandort geleisteten zusätzlichen Arbeit und dem Produktionsstandort. Nachdem die Anwendungen auf den ursprünglichen Produktionsstandort aktualisiert wurden, erfolgt das Failback mit nur wenigen Klicks. Viele Unternehmen verzichten auf Failover, weil Failback so umständlich ist – mit Zerto ist das alles aber ganz einfach.

Wiederherstellung von Dateien und Ordnern

Die häufigsten Katastrophen, die Administratoren bewältigen müssen, sind nicht Naturkatastrophen oder Standortausfälle, sondern verlorene oder versehentlich gelöschte Dateien oder Ordner. Zerto löst dieses gängige Problem durch eine Wiederherstellung von Einzeldateien und -ordnern bis zu 30 Tagen in die Vergangenheit unter Verwendung des Journals. CDP liefert Wiederherstellungspunkte im Abstand von nur wenigen Sekunden, sodass die IT-Abteilung zu dem Punkt zurückkehren kann, bevor die Datei gelöscht oder beschädigt wurde, um sie wiederherzustellen. Dies lässt sich mit nur wenigen Klicks erledigen, und die Arbeitsverluste werden auf ein Minimum reduziert.

Zerto CDP:

- **Minimiert Risiken.** Die Möglichkeit zur Wiederherstellung auf jeder Ebene und zu jedem Zeitpunkt sorgt dafür, Datenverluste bei Dateien, Ordnern, VMs, Anwendungen und Standorten zu minimieren.
- **Erhöht die Einfachheit.** Automatisierte Workflows für die Wiederherstellung von Dateien, Anwendungen und Daten verkürzen die durchschnittliche Zeit bis zur Wiederherstellung.
- **Schützt die Produktivität.** Die Produktivität und Arbeitsmoral von Mitarbeitern bleiben erhalten, da Endbenutzer nicht mehr Stunden oder einen ganzen Tag verlorener Arbeit wiederherstellen müssen, sollte eine Datei oder ein Ordner versehentlich gelöscht werden.



Cyber Resilience Vault-Architektur

Ransomware-Resilienz

Ransomware-Angriffe sind in den letzten Jahren immer häufiger geworden und richten sich gegen Unternehmen aller Größen und Branchen. Die Folgen von Ransomware-Angriffen können verheerend sein: Unternehmen verlieren den Zugriff auf wichtige Daten und Systeme und müssen mit finanziellen Verlusten und Rufschädigung rechnen. Um die ständig wachsende Bedrohung durch Ransomware zu bekämpfen, setzt Zerto eine Kombination aus fortschrittlichen Technologien und Best Practices ein.

- **Echtzeit-Erkennung von Verschlüsselung.** Der Encryption Analyzer von Zerto erkennt sofort verdächtige Schreibaktivitäten in geschützten Workloads und schlägt Alarm. Das neue Inline-Verschlüsselungs- und Warnsystem liefert Ihnen frühzeitig Hinweise auf gefährliche Anomalien. Sie müssen nicht mehr darauf warten, Ransomware erst nach einem Backup zu erkennen: Die Erkennung erfolgt innerhalb von Sekunden gleich beim ersten Auftreten.

- **Verbesserte Erkennung.** Sie können schnell und unterbrechungsfrei eine Zerto On-Demand-Sandbox einrichten, wobei Ihre gesamte Umgebung kopiert wird. So können Sie Malware-Scans durchführen, ohne die Produktion zu beeinträchtigen. Sicherheitsscans können ressourcenintensiv sein und Produktionsmaschinen verlangsamen. In einer isolierten Sandbox, die ein Duplikat der Produktionsumgebung ist, können Malware-Scans jedoch schnell und ohne Auswirkungen auf die Produktion durchgeführt werden.

- **Minimale Datenverluste.** Mit der Journaling-Technologie von Zerto können Daten in der Regel auf einen Zeitpunkt Sekunden vor einem Ransomware-Angriff wiederhergestellt werden, sodass Datenverluste auf ein Minimum reduziert werden.

- **Verschiedene Optionen für eine schnelle Wiederherstellung.** Zerto bietet verschiedene Wiederherstellungsoptionen aus lokalen, Warm-Site- und Cold-Site-Daten. Optionen umfassen schnelles Failover, kontinuierliches Point-in-Time-Journaling, Wiederherstellung von Dateien und Ordnern, vollständige VM-Wiederherstellung und orchestrierte Wiederherstellung.

- **Datenkopien über verschiedene Plattformen hinweg.** Mit Zerto können Workloads über verschiedene Plattformen hinweg geschützt werden (einschließlich lokal und in der Cloud), wodurch die Wahrscheinlichkeit verringert wird, dass ein Ransomware-Angriff Sicherungskopien erreicht.

- **Isolieren und Sperren mit einem Cyber Resilience Vault.** Der Zerto Cyber Resilience Vault sorgt für Wiederherstellbarkeit selbst nach den schlimmsten Angriffen. Die vollständig isolierte Wiederherstellungsumgebung mit Air Gap speichert unveränderliche Kopien auf sicherer, leistungsstarker Hardware. Der Cyber Resilience Vault nutzt eine Zero-Trust-Architektur sowie eine Kombination aus branchenführender Software und Hardware, um einen hochsicheren Reinraum zu schaffen – und erlaubt gleichzeitig eine schnelle Wiederherstellung innerhalb von Minuten oder Stunden anstelle von Tagen oder Wochen.

- **Wiederherstellung in einem isolierten Netzwerk.** Die Wiederherstellung nach einem Ransomware-Angriff kann schwierig sein, da Malware auch in wiederhergestellten Daten sitzen kann. Zerto setzt isolierte Wiederherstellungsumgebungen ein, um wiederhergestellte Daten und Systeme zu überprüfen. So können Sie nach Malware scannen und diese entfernen, bevor Sie die Produktionsumgebung vollständig wiederherstellen.

- **Unveränderliche Replikate.** Zusätzlich zu mehreren Kopien auf verschiedenen Plattformen unterstützt Zerto unveränderliche Replikate in der Cloud als letzten Ausweg gegen Ransomware-Angriffe. So wird sichergestellt, dass die Replikate nicht kompromittiert werden können.

Analysen und Berichterstellung

Die in die Lösung integrierten Zerto SaaS-basierten Analysefunktionen umfassen sofort einsatzbereite Dashboards und Berichte. Diese sorgen für vollständige Transparenz über verschiedene Standorte und Cloud-Umgebungen hinweg, damit Sie Ihre SLAs erfüllen und eine einfache, unkomplizierte Berichterstattung zur Einhaltung von Vorschriften vornehmen können. Mit der Zerto-App können Sie SLAs von überall aus überwachen. Zerto geht jedoch über reine Transparenz hinaus: Die Lösung gibt Ihnen Tools für eine intelligente, vorausschauende Infrastrukturplanung an die Hand, sodass Sie Ihre Datenschutzstrategie optimieren und proaktiv gestalten können.

Zerto In-Cloud für AWS

Zerto In-Cloud für AWS ermöglicht hoch skalierbare, orchestrierte DR von und zu AWS-Regionen und -Verfügbarkeitszonen. Zerto In-Cloud für AWS wurde für hohe Skalierbarkeit entwickelt und schützt Tausende von Instanzen auf verschiedenen Konten mit schneller Wiederherstellung, Einfachheit und ohne zu verwaltende Agenten. API-zentrierte Verwaltung ermöglicht Zerto In-Cloud die einfache Integration mit einem Automatisierungstool Ihrer Wahl (z. B. Ansible, Jenkins oder Terraform), um DR zu einem Teil Ihrer automatisierten Verwaltungsstrategie zu machen.

- **Skalierbarkeit.** Der agentenlose, native Integrationsansatz von Zerto In-Cloud ermöglicht eine einfache Skalierung zum Schutz von mehr als 1.000 Workloads und fördert die Ausfallsicherheit für Unternehmen jeder Größe in Amazon EC2. Unabhängig davon, ob Sie ein AWS-Konto oder Hunderte von Konten besitzen, können Sie den Schutz für Ihr gesamtes Unternehmen problemlos orchestrieren.

- **Orchestrierung.** Zerto In-Cloud automatisiert den Schutz von EC2-Instanzen und eliminiert so die Notwendigkeit für übermäßige, manuelle und fehleranfällige Schritte beim Ausführen von Wiederherstellungsplänen. Failover-Funktionen und Failover-Testfunktionen werden dann im Hinblick auf Skalierbarkeit und Einfachheit automatisiert.

- **Einfachheit.** Mit nativer, agentenloser AWS-Integration statt Einrichtung einer weiteren Softwareebene in AWS nutzt Zerto In-Cloud die Vorteile von Amazon EBS-Snapshots und nativer AWS-Replikation. Analysen bieten Ihnen Einblicke und Berichte zu RTOs und RPOs.

- **Unterbrechungsfreie Failover-Tests.** Die Automatisierung von Zerto In-Cloud und Orchestrierung von Zerto ermöglichen unterbrechungsfreie Failover-Tests aller Instanzen in einer AWS-Region oder -Verfügbarkeitszone, um Wiederherstellungspläne und die Bereitschaft im Falle eines Ausfalls oder einer Katastrophe zu überprüfen.

- **Flexible Verwaltung.** Eine vollständige REST-API steht im Vordergrund des Zerto In-Cloud-Managements, sodass das Produkt leicht mit anderen Verwaltungssystemen integriert sowie mit anderen Automatisierungs- und Integrationslösungen kombiniert werden kann.

- **Anwendungsgruppen.** Orchestrierung mit Zerto In-Cloud ermöglicht anwendungsbezogenen VPGs die Wiederherstellung von Anwendungen als eine Einheit in einer anderen Region oder Verfügbarkeitszone, wodurch Sie große komplexe Anwendungen wie SAP bequem schützen und wiederherstellen können.

- **Stateless-Verwaltung.** Die Zerto In-Cloud Manager Appliance läuft in jeder Amazon EC2-Region und kann bei einem Ausfall schnell in eine andere Region verlagert werden, um Workloads zuverlässig wiederherzustellen und zu verwalten.

Die Zerto In-Cloud-Architektur

Der Zerto In-Cloud Manager ist eine Linux-basierte virtuelle Appliance, die mit Amazon DynamoDB und Amazon EBS zusammenarbeitet, um eine Automatisierung von Snapshots und Replikation für EC2-Instanzen über alle zugehörigen Konten hinweg zu ermöglichen. Der Zerto In-Cloud Manager ist „stateless“, befindet sich in einer beliebigen EC2-Region und kann bei Bedarf schnell in eine andere Zone oder Region verlegt werden. Für die Verwaltung wird nur eine einzige Zerto In-Cloud Manager-Appliance benötigt, unabhängig davon, wie viele EC2-Instanzen geschützt werden.

Abbildung 8 – Mit EBS-Snapshots und nativer AWS-Replikation schützt Zerto In-Cloud Amazon EC2-Instanzen bei lokalen und regionalen Ausfällen und anderen potenziellen Katastrophen.

Zerto In-Cloud koordiniert Amazon EBS-Snapshots und -Replikation zum Schutz von Instanzen über Regionen hinweg. Bei einem Ausfall, einer Katastrophe oder einem Ransomware-Angriff werden Daten und Anwendungen in einer separaten Region oder Zone geschützt, damit sie schnell wieder online gehen können.
Anwendungen sowie die Instanzen, auf denen sie in Amazon EC2 laufen, werden in VPGs geschützt, welche die Replikation und Wiederherstellung über die gesamte Anwendungsgruppe hinweg koordinieren. Dieser anwendungsbezogene Schutzansatz bedeutet, dass ganze Anwendungen mit Konsistenz und zuverlässiger Schreibreihenfolge wiederhergestellt werden. Die im Produkt enthaltenen Analysen bieten Einblicke und Berichte zu RTOs und RPOs Ihrer VPGs.

ABSCHNITT 4

Zusammenfassung

Die Planung der Wiederherstellung im Katastrophenfall ist ein komplexer Prozess, der viele Überlegungen erfordert. Die Wahl der richtigen DR-Lösung für Ihren Bedarf kann herausfordernd sein, da es so viele neue und ältere Lösungen gibt und die Wahl der falschen Lösung durch Ausfallzeiten und Datenverluste zu Verlusten in Millionenhöhe führen kann.

Wenn Sie die wichtigsten Aspekte in diesem Leitfaden verstehen und sich für eine DR-Lösung wie Zerto entscheiden, können Sie nicht nur alle Ihre SLAs für RTOs und RPOs zuverlässig einhalten, sondern auch viele weitere Vorteile nutzen, die ältere Lösungen einfach nicht bieten. Bei Zerto profitieren Sie von diesen und weiteren Vorteilen, jetzt und in Zukunft.

Um mehr über Zerto zu erfahren, nutzen Sie unsere interaktive Produkttour oder melden Sie sich für unsere kostenlose Testversion an.

Über Zerto

Zerto, ein Unternehmen von Hewlett Packard Enterprise, ermöglicht es seinen Kunden, einen Always-On-Betrieb zu managen, indem es den Schutz, die Wiederherstellung und die Mobilität von On-Premises- und Cloud-Anwendungen vereinfacht. Zerto beseitigt die Risiken und Komplexitäten, die mit der Modernisierung und Cloud-Einführung in privaten, öffentlichen und hybriden Umgebungen verbunden sind. Die einfache Softwarelösung basiert auf Continuous Data Protection (CDP), um Ransomware-Resilienz, Disaster Recovery und Multi-Cloud-Mobilität sicherzustellen. Zerto genießt das Vertrauen von über 9.500 Kunden weltweit und unterstützt Angebote für Amazon, Google, IBM, Microsoft, Oracle und mehr als 350 Managed Service Provider. **www.zerto.com**

RITM0066172