Zerto
a Hewlett Packard Enterprise company

Leitfaden zur Zerto-Architektur

Disaster Recovery, Ransomware-Resilienz und Multi-Cloud-Mobilität

Inhaltsverzeichnis

Zusammenfassung 2

Zerto im Überblick und Anwendungsfälle 2

- Zerto für Disaster Recovery 2
- Zerto für Ransomware-Resilienz 3
- Zerto für Multi-Cloud-Mobilität 3
- Analytics 4

Kernkomponenten von Zerto 4

- Zerto Virtual Manager 4
- Virtual Replication Appliance 4
- Zerto Cloud Appliance für Microsoft Azure 5
- Zerto Cloud Appliance für AWS 5
- Virtual Protection Groups 5
- Journal 5
- Unveränderbare Repositorys 6

Referenzarchitekturen 6

- Anwendungsfälle 7
- Architektur 1: Disaster Recovery 7
- Architektur 2: Lokale Replikation und Erkennung mit lokaler Disaster Recovery 8
- Weitere Anwendungsfälle 9
- Architektur 3: Lokale, kontinuierliche Datensicherung und Disaster Recovery in der öffentlichen Cloud 9
- Weitere Anwendungsfälle 10

Schlussfolgerung 10

Zusätzliche Ressourcen 11

Zusammenfassung

Dieses Dokument bietet einen Architekturleitfaden für alle, die eine Datenschutzlösung mit Zerto entwerfen oder implementieren– insbesondere für Unternehmen, die eine lokale Produktionsumgebung mit einem lokalen oder Public-Cloud-basierten Disaster-Recovery-Ziel (DR) kombinieren möchten.

Dieses Dokument beinhaltet einen vollständigen Überblick über alle Designprinzipien, Architekturüberlegungen und Größenbestimmungen sowie eine Übersicht über die Installation für alle, die Zerto einsetzen möchten oder bereits verwenden. Außerdem werden wir uns gängige Herausforderungen und Anwendungsfälle ansehen, die sich mit Zerto lösen lassen.

Die in diesem Leitfaden vorgestellten Architekturen zeigen nur einen kleinen Ausschnitt dessen, was Zerto unterstützen kann. Die rein Software-basierte, horizontal skalierbare Architektur mit einem technologieunabhängigen Ansatz erlaubt es Ihnen, Ihre Anwendungen nach Belieben zu schützen, zu verschieben und wiederherzustellen.

Zerto im Überblick und Anwendungsfälle

Zerto sorgt in lokalen und Cloud-basierten Umgebungen für Disaster Recovery (DR), Ransomware-Resilienz und Multi-Cloud-Mobilität. Die Lösung beruht auf kontinuierlichem Datenschutz (CDP) mit integrierter Orchestrierung und Automatisierung, um IT-Teams einfachen, unternehmensweiten und flexiblen Datenschutz zu ermöglichen, der Zeit, Kosten und Ressourcen spart. Intelligente Analysen – einschließlich Dashboards, Live-Berichten und Funktionen für vorausschauende Ressourcenplanung – sorgen in Multi-Site- und Multi-Cloud-Umgebungen für vollständige Transparenz und geben Unternehmen die Gewissheit, dass sie geschäftliche Service-Level- und Compliance-Anforderungen jetzt und auch in Zukunft zuverlässig erfüllen können.

Zerto für Disaster Recovery

Unternehmen jeder Größe, die über virtualisierte Umgebungen verfügen, nutzen Replikation für DR-Zwecke, da die Folgen von fehlgeschlagenen oder langsamen Wiederherstellungen katastrophal sein können und ein systemisches Risiko darstellen. Seit der umfangreichen Einführung von Virtualisierung gibt es verschiedene DR-Technologien für Unternehmen, die jedoch in der Regel für den Schutz physischer Server mit speicherbasierter Replikation und nicht für virtuelle Maschinen (VMs) konzipiert wurden.

Speicherbasierte Replikation erhöht die Komplexität, da sie auf Basis von Festplatten und LUNs konfiguriert wird und daher passende Speicher- und LUN-Konfigurationen erfordert. Dabei gibt es keine Granularität auf VM-Ebene oder Integration in die Virtualisierungsplattform. Darüber hinaus erfordert speicherbasierte Replikation separate, komplexe Software für die Orchestrierung und Automatisierung von VMs. Das erfordert verschiedene Fähigkeiten und Ressourcen und passt nicht zu den Vorteilen von Virtualisierung.

Eine weitere gängige Replikationsmethode basiert auf Snapshots. Produkte, die Snapshot-basierte Replikation nutzen, wurden in der Regel primär zur Datensicherung und erst in zweiter Linie für die Notfallwiederherstellung entwickelt. Den meisten dieser Produkte fehlt es an Skalierbarkeit, Orchestrierung und Automatisierung auf dem für Unternehmensarchitekturen erforderlichen Niveau. Außerdem wirken sich Snapshots auf Produktions-Workloads aus, sodass sie sich oft nicht so nutzen lassen, wie es Unternehmen benötigen. Da Snapshots in der Regel nur einmal am Tag erstellt werden, kann es zwischen den Sicherungsfenstern zu großen Datenverlusten kommen.

Zerto wurde von Grund auf als besonders einfache und leistungsfähige DR-Lösung für virtualisierte Infrastrukturen entwickelt. Durch die Integration aller Replikations-, Wiederherstellungs- und Automatisierungsprozesse in einer einfachen Softwarelösung ermöglicht Zerto den Anwendenden die Wiederherstellung einer, aller oder einer Teilmenge von virtualisierten Anwendungen in jede Richtung und maximiert so die Vorteile der Virtualisierung und der Cloud.

Durch die native Integration in alle unterstützten Plattformen ermöglicht Zerto nicht nur die Replikation und Wiederherstellung zwischen beliebigen Speichermedien, sondern schützt auch über mehrere Hypervisoren und öffentlichen Cloud-Plattformen hinweg. Diese marktführende Technologie ist eine erstklassige Lösung für Business Continuity (BC) und Disaster Recovery (DR), die unabhängig vom zugrunde liegenden Hypervisor, der öffentlichen Cloud oder dem Speicher ist.

Zerto verwendet CDP anstelle von Storage- oder Snapshot-basiertem Schutz. So kann Zerto die besten Recovery Point Objectives (RPOs) und Recovery Time Objectives (RTOs) der Branche erreichen, ohne Produktionsworkloads zu beeinträchtigen. Die für Zerto typischen RPOs im Sekundenbereich und RTOs im Minutenbereich ermöglichen es Unternehmen, Datenverluste und Ausfallzeiten drastisch zu begrenzen, unabhängig von der Art der Katastrophe oder Störung.

Zerto für Ransomware-Resilienz

Cyberkriminalität, einschließlich Ransomware, ist eine der größten Herausforderungen, denen sich IT-Verantwortliche heute stellen müssen. Die Cybersicherheit konzentriert sich auf präventive Maßnahmen wie Netzwerksicherheit oder Endpunktschutz, z. B. durch Antivirenlösungen. Auch wenn diese Bestandteile für sich genommen extrem wichtig sind, sind sie nur Teile eines viel größeren Puzzles.

Ransomware-Schutz allein reicht also nicht aus. Angreifende müssen nur einmal erfolgreich sein, um einem Unternehmen Schaden zuzufügen. Die Lösung von Zerto verlagert den Schwerpunkt von Prävention auf Resilienz – unter Einbeziehung einer Vielzahl von Technologien und Methoden, um echte Ransomware-Resilienz zu erreichen. Im Großen und Ganzen können wir diese Technologien und Methoden in vier Hauptelemente aufteilen:

1. Schulung
2. Prävention
3. Erkennung
4. Wiederherstellung

Investitionen sind in allen Bereichen erforderlich, damit sich Unternehmen optimal gegen Ransomware wappnen können.

Zerto konzentriert sich auf Ransomware-Resilienz, indem es eine erstklassige Lösung für Ransomware-Wiederherstellung anbietet. Sobald Ransomware beginnt, Daten in Ihrer Umgebung zu verschlüsseln, gibt Zerto die frühestmögliche Warnung, dass ein Angriff im Gange ist. Die Erkennung erfolgt in Echtzeit, noch während Daten einströmen und von Zerto geschützt werden, und nicht als Scan im Anschluss an die Verarbeitung, nachdem die Daten in ein Replikat geschrieben wurden. Dank der Echtzeit-Verschlüsselungserkennung mit sofortigen Warnmeldungen können Unternehmen schneller als je zuvor reagieren.

Unternehmen können mit Zerto dann genau feststellen, welche Anwendungen betroffen waren, und alle Daten bis auf wenige Sekunden vor dem Auftreten des Problems wiederherstellen. Die Wiederherstellung ist unglaublich granular, da es Tausende von Wiederherstellungspunkten gibt, die jeweils nur 5–15 Sekunden voneinander entfernt sind. Außerdem erstreckt sich die Wiederherstellung auf einzelne Dateien oder Ordner, einzelne VMs, ganze Multi-VM-Anwendungen und auch ganze virtualisierte Standorte. Dank Automatisierung und Orchestrierung bleiben die RTOs so niedrig wie möglich.

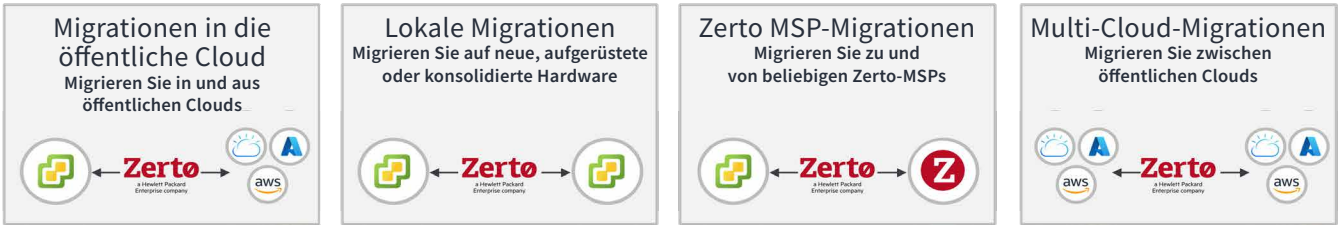
Zerto für Multi-Cloud-Mobilität

Datenmobilität ist im heutigen Computing-Umfeld eine entscheidende Fähigkeit. Sie ermöglicht es Unternehmen, Anwendungen und Daten über verschiedene Plattformen hinweg zu verschieben – mit minimalen Auswirkungen auf den Geschäftsbetrieb und ohne Einschränkungen bei der Infrastruktur. Angesichts der zunehmenden Beliebtheit von Cloud Computing gibt es heute zahlreiche Cloud-Plattformen, von denen jede über einzigartige Eigenschaften verfügt, die sie für bestimmte Workloads geeignet macht. Allerdings sind nicht alle Workloads für die Cloud geeignet, sodass manche Unternehmen weiterhin auf herkömmliche lokale Bereitstellungen setzen. Infolgedessen werden Multi-Cloud- und Hybrid-Cloud-Strategien immer beliebter, da Unternehmen versuchen, sich nicht an eine bestimmte Plattform oder einen bestimmten Anbieter zu binden und die Flexibilität zu wahren, Anwendungen und Daten dorthin zu verschieben, wo sie am besten funktionieren.

Echte Datenmobilität ermöglicht es Unternehmen, Anwendungen und Daten nahtlos zwischen verschiedenen Plattformen zu verschieben, unabhängig davon, ob sie sich lokal oder in der Cloud befinden. Die Produktionsumgebung wird dabei nicht beeinträchtigt. So können Unternehmen Migrationen vor dem jeweiligen Live-Ereignis validieren und dafür sorgen, dass Anwendungen und Daten nicht an eine bestimmte Plattform oder einen bestimmten Anbieter gebunden sind.

Sobald sich Daten in der Cloud befinden, bietet Zerto die Freiheit, sie bei Bedarf wieder zurück zu verschieben oder über verschiedene Regionen und Zonen hinweg innerhalb der Cloud zu schützen und zu migrieren. Diese Flexibilität ist entscheidend, um mit einer sich ständig verändernden Cloud-Landschaft und einer sich entwickelnden Cloud-Strategien Schritt halten können. Dank der Freiheit, Anwendungen und Daten über verschiedene Plattformen hinweg zu verschieben,

können Unternehmen die individuellen Eigenschaften einzelner Plattformen nutzen und ihre Datenverarbeitungsumgebung optimieren, um alle ihre Ziele zu erreichen.



Analytics

Zerto Analytics bietet zusätzliche Transparenz für geschützte IT-Umgebungen in privaten, öffentlichen und hybriden Clouds und ist somit ein wertvolles Tool für IT-Verantwortliche. Mit Zerto Analytics erhalten Anwendende einen umfassenden Überblick über ihre gesamte Multi-Site- und Multi-Cloud-Umgebung, da sie Metriken wie durchschnittlicher RPO-Wert, Netzwerkleistung und Speicherverbrauch anzeigen können. Dies ermöglicht Echtzeit- und Verlaufsanalysen des Zustands und Schutzstatus von Anwendungen und Daten.

Ein weiteres Leistungsmerkmal von Zerto Analytics ist das Kapazitätsplanungs-Tool, das Anwendenden auf Grundlage ihrer realen Daten bei der Planung und Vorhersage des Ressourcenbedarfs für zukünftige Datenschutzanforderungen hilft. So wird sichergestellt, dass Benutzende die Anforderungen genau kennen, die sie zur Erweiterung ihrer Datenschutzkapazitäten und zum Schutz zusätzlicher Workloads berücksichtigen müssen.

Darüber hinaus bietet Zerto Analytics intelligente Dashboards, die es Anwendenden ermöglichen, Trends zu erkennen, Anomalien zu identifizieren und Probleme zu beheben – mit einer zentralen Übersicht über die gesamte IT-Umgebung. Das umfasst sowohl lokale Daten als auch Daten in der Cloud, sodass Benutzende den Zustand und Schutzstatus von Anwendungen und Daten in Echtzeit überwachen können.

Insgesamt hilft Zerto Analytics IT-Führungskräften dabei, bessere Entscheidungen zu treffen und eine effizientere, belastbarere Arbeitsweise zu erreichen, da die Lösung ihnen die Einblicke liefert, die sie benötigen, um komplexe, vielfältige und disparate Rechenzentrums- und Cloud-Workloads zu verwalten.

Kernkomponenten von Zerto

Zerto Virtual Manager

Der Zerto Virtual Manager (ZVM) spielt eine entscheidende Rolle bei der Verwaltung des Replikationsverfahrens zwischen den geschützten und den Wiederherstellungsstandorten. Er fungiert als zentrale Steuerungsebene, die mit der Hypervisor-Verwaltungsschnittstelle und anderen Komponenten der Zerto-Infrastruktur kommuniziert, um Replikation zu orchestrieren und zu gewährleisten, dass geschützte Daten konsistent und korrekt sind.

Darüber hinaus bietet der ZVM eine benutzerfreundliche Oberfläche für die Verwaltung von Replikation, die Konfiguration von Recovery-Workflows und die Überwachung des Zustands der Replikationsumgebung. Er wird als sicherheitsgehärtete virtuelle Appliance bereitgestellt und schützt vor unbefugtem Zugriff oder Manipulation. So stellt der ZVM die Integrität und Vertraulichkeit Ihrer wichtigsten Daten sicher. Mit dem ZVM können Sie sich darauf verlassen, dass Ihre Replikationsumgebung reibungslos funktioniert und Ihre Daten vor Verlust oder Manipulation geschützt bleiben.

Virtual Replication Appliance

Die Virtual Replication Appliance (VRA) ist eine schlanke virtuelle Appliance, die auf jedem Hypervisor-Host installiert wird, um die Replikation von Daten zwischen geschützten VMs und ihren lokalen oder entfernten Zielen zu verwalten. Sie bietet eine echte horizontal skalierbare Architektur, die mit Ihrer Umgebung wachsen bzw. schrumpfen kann und die Verwaltung und Skalierung Ihres Replikationsbedarfs spürbar erleichtert. Außerdem verwaltet die VRA in Echtzeit die Erkennung von

Inline-Verschlüsselung, um Unternehmen dabei zu helfen, Folgen von Ransomware zu erkennen, noch während sie auftreten. Die Appliance setzt ein Minimum von nur 3 GB RAM und 1 vCPU voraus, was sie zu einer extrem effizienten und schlanken Lösung macht.

Zerto Cloud Appliance für Microsoft Azure

Beim Einsatz innerhalb von Microsoft Azure dient die Zerto Cloud Appliance (ZCA) als vollständig skalierbare Verwaltungsebene für alle Replikationen in, aus und zwischen Microsoft Azure-Regionen. Sie ist vergleichbar mit dem ZVM für lokale Umgebungen. Die Einzel-Appliance wird innerhalb von Azure IaaS ausgeführt und nutzt Block- und Seiten-Blob-Speicher, um Daten kostengünstig zu speichern. Die Replikation wird dann mit dedizierten In-Cloud-VRA-Instanzen ausgeführt, um eine echte horizontal skalierbare Architektur mit Cloud-nativen Technologien wie Azure Scale Set Workers und Azure Queues zu bieten. Die VRAs werden zur Replikation des aktuellen Datensatzes automatisch und dynamisch angepasst.

Zerto Cloud Appliance für AWS

Im Gegensatz zu lokalen und Azure-Managern fasst die AWS ZCA die Verwaltungs- und Replikationskomponenten in einer einzigen Cloud-Appliance zusammen. Die AWS ZCA ist eine dedizierte VM, die aus den folgenden Services besteht:

- **ZVM:** Dabei handelt es sich um einen Linux-Dienst, der die Benutzeroberfläche hostet und für die Verwaltung und Orchestrierung mit den nativen APIs von Azure/AWS integriert ist.
- **VRA:** Hierbei handelt es sich um einen Linux-Dienst, der die Replikation von Daten von oder nach Azure/AWS selbst übernimmt.

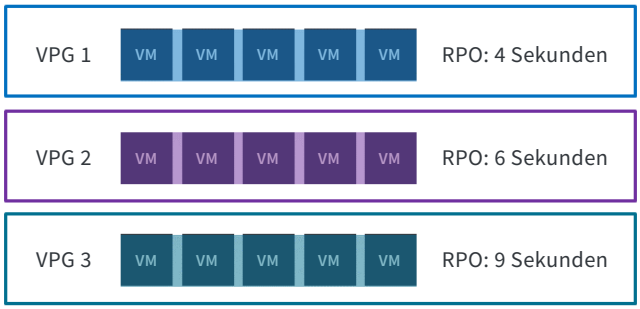
Die ZCA ist nativ in die AWS-Plattform integriert, sodass Sie die Appliance für das Speichern von Journalen in AWS Amazon-S3-Buckets verwenden können. Das erlaubt eine möglichst kosteneffiziente Bereitstellung.

Virtual Protection Groups

Virtual Protection Groups (VPGs) stellen das Herzstück der Schutz- und Wiederherstellungsfunktionen von Zerto dar. Sie dienen als konsistenter und kohärenter Ansatz für den Schutz mehrerer VMs, aus denen eine Anwendung zusammengesetzt ist. Anstatt jede VM einzeln zu schützen, können Sie mit VPGs eine oder mehrere VMs zusammen auf konsistente Weise schützen. So wird sichergestellt, dass jeder in das Zerto-Journal eingefügte Zeitpunkt für alle VMs innerhalb der VPG gleich ist, auch wenn sich die entsprechenden VMs auf unterschiedlichen Hosts oder Datenspeichern befinden. Das bedeutet, dass sich im Falle einer Wiederherstellung alle VMs innerhalb der VPG zum gleichen Zeitpunkt wiederherstellen lassen, was eine kohärente und konsistente Wiederherstellung der gesamten Anwendung ermöglicht.

VPGs fördern durch die Erkennung von Ransomware-Angriffen dank Zerto und die automatische Wiederherstellung nach solchen Angriffen die Resilienz gegenüber Ransomware. Durch eine Überwachung des Journals auf unerwartete Änderungen kann Zerto böswillige oder anomale Verschlüsselungsvorgänge erkennen, noch während sie erfolgen, und eine Wiederherstellung zu einem Zeitpunkt kurz vor Beginn des Angriffs ermöglichen. Außerdem erlauben VPGs Multi-Cloud-Mobilität, indem sie es ermöglichen, Anwendungen zu, aus und zwischen verschiedenen Plattformen/Clouds zu verschieben – mit minimalen geschäftlichen Auswirkungen und ohne herkömmliche Infrastrukturbeschränkungen.

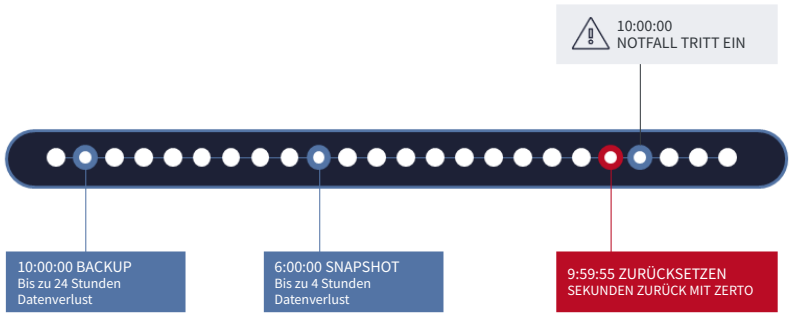
Journal



Zusätzlich zu VPGs speichert Zerto CDP alle replizierten Daten im Journal. Das Journal speichert alle Änderungen für einen benutzerdefinierten Zeitraum (1 Stunde bis 30 Tage) und erlaubt Ihnen Wiederherstellungen zu einem beliebigen Zeitpunkt innerhalb des Journals, sodass Ihr RPO stets extrem niedrig ist (meist nur wenige Sekunden). Jeder Schreibvorgang auf eine geschützte VM wird von Zerto kopiert. Solche Schreibvorgänge werden lokal und/oder remote mit One-to-Many-Funktionen von Zerto repliziert und in ein von einer VRA verwaltetes Journal geschrieben. Jede geschützte VM hat ihr eigenes Journal. Zusätzlich zu den Schreibvorgängen werden alle Journale innerhalb der VPG alle paar Sekunden mit einem Checkpoint-Zeitstempel aktualisiert. Checkpoints dienen dazu, die Einhaltung der Schreibreihenfolge und Konsistenz bei Abstürzen in der gesamten VPG zu gewährleisten.

Mit Zerto können Wiederherstellungen zum letzten Checkpoint oder zu einem vom Benutzer gewählten Checkpoint erfolgen. Dies ermöglicht die Wiederherstellung von Dateien, Ordnern, VMs, Anwendungen oder ganzen Standorten. Der Wiederherstellungspunkt kann entweder auf den letzten mit dem Absturz konsistenten Zeitpunkt oder auf einen Zeitpunkt vor dem Angriff gesetzt werden (z. B. wenn die VM von einem Virus oder Ransomware befallen wurde). In Kombination mit den Erkennungsfunktionen von Zerto erlaubt es eine solche Wiederherstellung, anomale Checkpoints zu markieren und so bequem einen Checkpoint kurz vor dem Auftreten verdächtiger Aktivitäten zu identifizieren. Danach ist es mit Zerto ganz einfach, Daten zu testen und wiederherzustellen, und zwar auf einen Zeitpunkt Sekunden vor dem Auftreten der Störung.

Unveränderbare Repositorys



Zusätzlich zu flexiblen Optionen für kurzfristige Wiederherstellungsszenarien bei Ransomware unter Einsatz des Journals brauchen die meisten Unternehmen, die Compliance-Anforderungen erfüllen müssen, eine unveränderbare Kopie als integralen Bestandteil ihrer Datenschutzstrategie. Herkömmliche Methoden zur Bereitstellung eines unveränderlichen Schutzes werden stets in der Produktionsumgebung selbst durchgeführt, was sich auf die Leistung auswirkt und oft das Benutzererlebnis beeinträchtigt.

Zerto Extended Journal Copy (EJC) hingegen nutzt Ihr bestehendes Journal, um Daten von einem beliebigen Zeitpunkt über Tage, Wochen, Monate oder sogar ein Jahr hinweg zu speichern. Die Lösung verwendet die bereits durch CDP geschützten Daten, kombiniert sie miteinander und speichert sie auf der Zielseite in einem Journal. So können Sie Point-in-Time-Kopien auf sekundäre Speicherziele auslagern und diese Kopien als unveränderlich kennzeichnen, ohne Produktions-Workloads zu beeinträchtigen. Bei Einsatz von öffentlichen Cloud-Speicherzielen (wie AWS und Azure) bietet Zerto native Daten-Tiering-Funktionen, um dafür zu sorgen, dass Daten im kosteneffizientesten Produkt gespeichert werden.

Zerto unterstützt die Verwendung von Festplatten-, Objekt- und Cloud-Speicher; eine vollständige Liste der unterstützten Repositorys und ihrer Versionen finden Sie in unserer Interoperabilitätsmatrix.

Referenzarchitekturen

In diesem Abschnitt werden anhand von drei Beispielkonfigurationen die verschiedenen Möglichkeiten von Zerto verständlich dargestellt. Die aufgeführten Beispielkonfigurationen sind nur als Leitfaden gedacht, um die Vorteile, die Zerto Ihrem Unternehmen bieten kann, zu veranschaulichen und gleichzeitig die Einfachheit der Lösung zu demonstrieren.

Anwendungsfälle

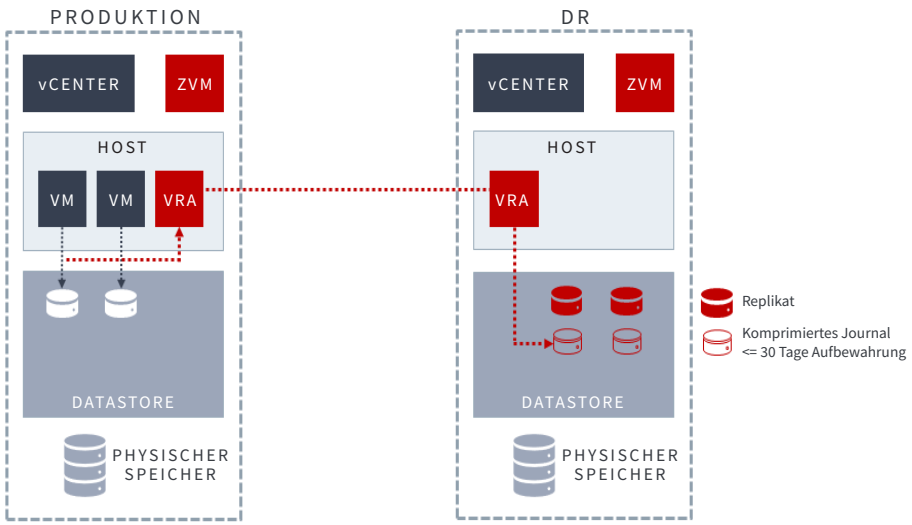
Alle drei Beispielkonfigurationen unterstützen folgende Anwendungsfälle. Wo es eindeutige Unterschiede gibt, werden diese in der jeweiligen Architektur hervorgehoben.

Ausfälle und Störungen	Jede Unterbrechung des Produktionsstandorts (sei es aus Stromversorgungs-, Netzwerk- oder anderen Gründen) wird durch die Wiederherstellung Ihrer Dateien und Ordner, VMs, Anwendungen oder des gesamten Standorts innerhalb weniger Minuten auf einen Zeitpunkt, der nur Sekunden vor dem Auftreten des Problems liegt, geschützt. *Beispiel: Wiederherstellung Ihres gesamten Standorts innerhalb von Minuten nach einem Stromausfall.*
Ransomware-Angriffe	Die Wiederherstellung nach Ransomware-Angriffen kann auf einen Zeitpunkt erfolgen, der nur wenige Sekunden vor dem Erfolgen der Verschlüsselung liegt, was Datenverluste und die Auswirkungen auf den Geschäftsbetrieb minimiert. Sie können Ihre Dateien und Ordner, VMs, Anwendungen oder ganze Standorte wiederherstellen. *Beispiel: Wiederherstellung verschlüsselter Dateien auf einen Zeitpunkt, der nur wenige Sekunden vor dem Erfolgen der Verschlüsselung liegt.*
Modernisierung der Infrastruktur	Dieselbe Architektur kann dazu dienen, Ihre Workloads innerhalb weniger Minuten von einer alten Plattform auf Ihre neue Infrastruktur zu verlagern, was Projekte zur Modernisierung der Infrastruktur erheblich beschleunigt. Solche Migrationen können auch im Vorfeld getestet werden, um Migrationszeiten und -risiken zu minimieren. *Beispiel: Verschiebung Ihrer Workloads in nur wenigen Minuten auf eine neue Plattform – ohne Datenverluste.*
Konsolidierungen und Migrationen	Wenn mehrere Standorte konsolidiert oder zum gleichen Ziel migriert werden sollen, kann diese Architektur zur Vereinfachung des Verfahrens dienen. So werden Tests vor der Migration und Live-Migrationszeiten von nur wenigen Minuten möglich. *Beispiel: Konsolidierung der Workloads von verschiedenen Hardware-, Hypervisor- und Cloud-Plattformen, um Geschäftsstandards in wenigen Minuten zu erfüllen.*
Tests und DevOps	Ermöglicht die Erstellung von Replikaten Ihrer Produktionsumgebung an einem entfernten Standort zu einem beliebigen Zeitpunkt – und zwar innerhalb von Minuten. Das bietet Ihren Entwicklungsteams mehr Flexibilität, reduziert den Aufwand für DevOps-Teams und ermöglicht DR-Tests sowie -Validierung. *Beispiel: Erstellung exakter Replikate von Produktionsanwendungen von vor wenigen Sekunden für UAT-Zwecke in wenigen Minuten.*
Cloud-übergreifende Analysen	Eine zentrale SaaS-basierte Analyseplattform, die vollständige Datenanalysen für alle Ihre Standorte erlaubt, sowohl lokal als auch in der Cloud. So erhalten Sie eine einheitliche Übersicht, die Verwaltung und Überwachung ohne Zusatzkosten vereinfacht. *Beispiel: Ermittlung von Bandbreitenengpässen in Ihrer gesamten IT-Infrastruktur über ein einziges Portal.*

Architektur 1: Disaster Recovery

Abbildung 1 zeigt eine DR-Architektur, bei der ein einzelnes Remote-Ziel als Wiederherstellungsstandort verwendet wird.

Abbildung 1

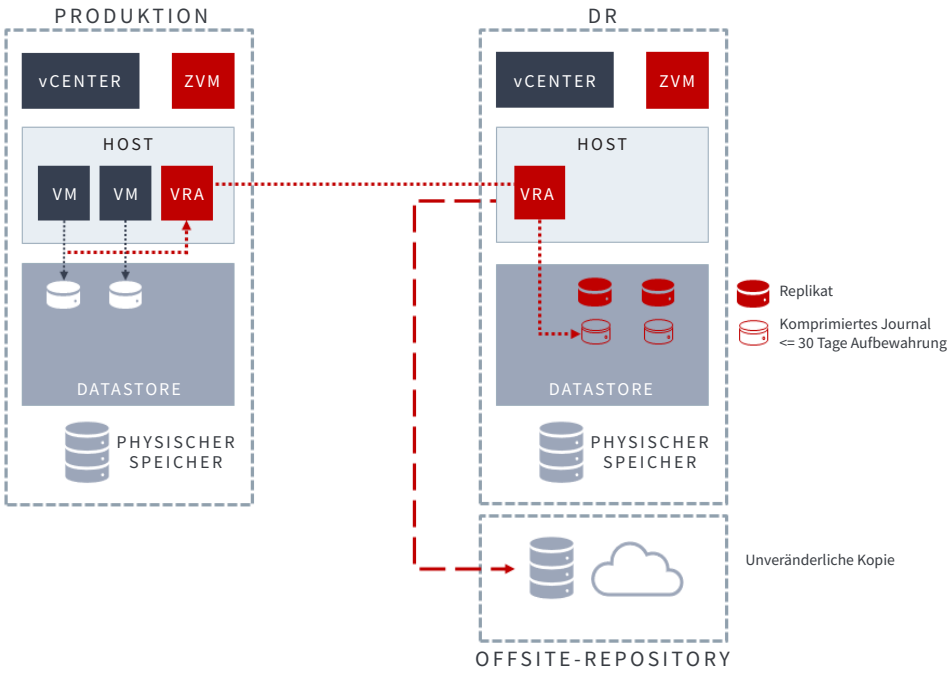


Geschützte VMs werden in VPGs angeordnet, wobei Konsistenz zwischen allen VMs in jeder VPG gewährleistet ist. Ein Remote-Journal wird auf der Remote-Zielseite konfiguriert und für kurzfristige Wiederherstellungsszenarien genutzt, bei denen sich eine Wiederherstellungsgranularität von nur wenigen Sekunden erreichen lässt. Der empfohlene Zeitraum für das Journal beträgt acht Tage, da damit die meisten Wiederherstellungsszenarien abgedeckt werden. Alle Änderungen an den geschützten VMs werden dann acht Tage lang aufbewahrt, bevor sie auf die Remote-Replikationsfestplatten übertragen werden.

Architektur 2: Lokale Replikation und Erkennung mit lokaler Disaster Recovery

Abbildung 2 zeigt eine Referenzarchitektur, die der oben beschriebenen DR-Referenzarchitektur ähnelt, aber zusätzlich ein lokales Journal sowie eine unveränderliche Offsite-Kopie des Journals umfasst. Das lokale Journal bietet kontinuierliche Replikations- und Erkennungsfunktionen, sodass Benutzer von einer Echtzeit-Erkennung von Inline-Verschlüsselung profitieren. Außerdem können Anwendende Dateien, VMs oder Anwendungen lokal mit einer Granularität von wenigen Sekunden wiederherstellen, was im Falle einer Störung minimale Datenverluste sowie eine schnelle Wiederherstellung auf produktionsfähigen Speicher- und Rechenkomponenten erlaubt.

Abbildung 2



In dieser Konfiguration existieren dieselben VMs in zwei separaten VPGs. Die erste VPG dient der Erstellung des Journals in der Quelle, während die zweite VPG die Aufgabe hat, die Journalfunktion auf dem Remote-Ziel zu gewährleisten. Das lokale Journal wird am Quellstandort konfiguriert und für die lokale Replikation und Erkennung von Verschlüsselung im Falle eines logischen Ausfalls verwendet, was für eine Wiederherstellungsgranularität von nur wenigen Sekunden sorgt. Der empfohlene Zeitraum für das Journal beträgt 14 Tage, da damit die meisten logischen Wiederherstellungsszenarien abgedeckt werden. Dank der Deduplizierungsfunktionen moderner Speicher-Arrays wird nur minimaler Speicherplatz verbraucht. Ein täglicher Prozess sendet Zeitpunkte aus dem lokalen Journal an das EJC-Repository, um die Einhaltung von Vorschriften und Unveränderlichkeit zu gewährleisten.

Zusätzlich zur vorher beschriebenen Referenzarchitektur bietet Ihnen diese Architektur die Möglichkeit, Daten direkt am Quellstandort und nicht nur am Remote-Standort wiederherzustellen. Bei dieser Architektur beträgt die empfohlene Mindesthistorie des Remote-Journals drei Tage; damit werden die meisten Wiederherstellungsszenarien abgedeckt, wenn es zu einem physischen Ausfall kommt. Alle Änderungen an den geschützten VMs werden dann drei Tage lang aufbewahrt, bevor sie auf die Remote-Replikationsfestplatten übertragen werden.

Weitere Anwendungsfälle

Zusätzlich zu den standardmäßigen Anwendungsfällen der Plattform gelten die folgenden Nutzungsfälle speziell für diese Architektur.

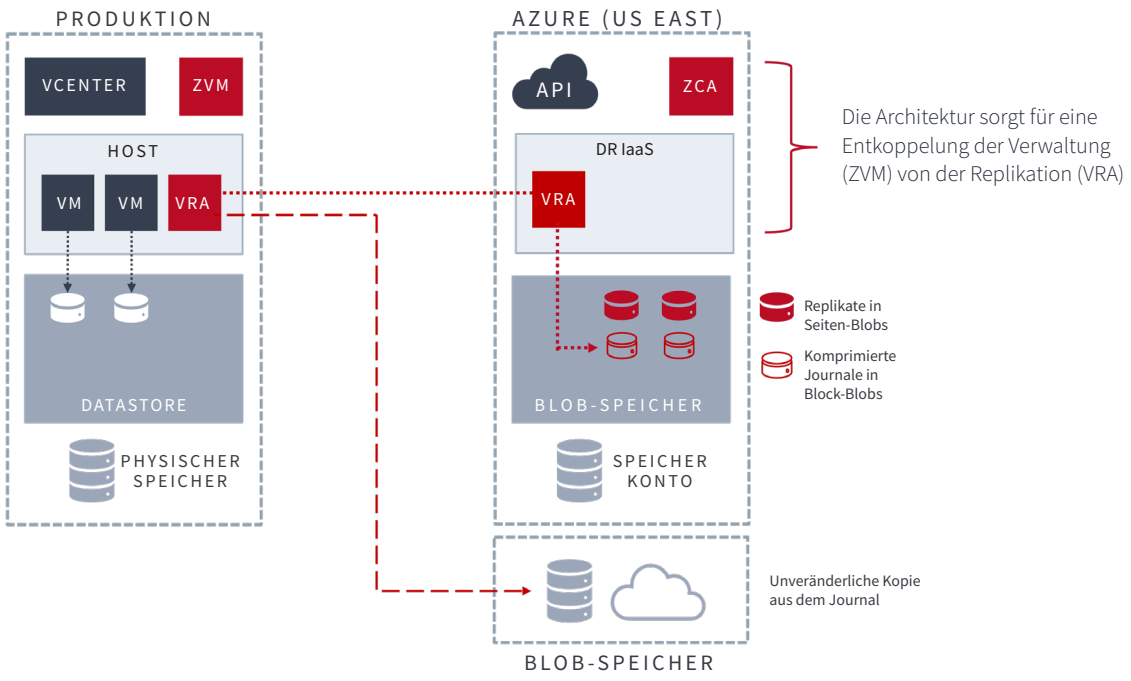
Ausfälle und Störungen	In dieser Konfiguration ist die Fähigkeit enthalten, Dateien und Ordner, VMs, Anwendungen oder Standorte im Falle eines logischen Ausfalls lokal wiederherzustellen. Beispiel: Wenn nur eine Anwendung ein Problem hat, stellen Sie lokal nur diese Anwendung wieder her (und nicht remote) – auf einen Zeitpunkt Sekunden vor dem Auftreten des Problems.
Ransomware-Angriffe	In dieser Konfiguration ist die Fähigkeit enthalten, Dateien und Ordner, VMs, Anwendungen oder Standorte im Falle eines Ransomware-Angriffs lokal wiederherzustellen. Beispiel: Sie stellen nur betroffene Dateien, VMs oder Anwendungen lokal wieder her (und nicht remote) – und zwar auf einen Zeitpunkt Sekunden vor dem Auftreten des Angriffs.
Tests und DevOpS	In dieser Konfiguration ist die Fähigkeit enthalten, die Wiederherstellungsfunktion zu testen oder lokal Replikate für DevOps-Zwecke zu erstellen. Beispiel: Sie erstellen zu Entwicklungszwecken lokal ein Replikat einer Produktions-Workload.

Vereinbaren Sie noch heute einen Termin für eine Demo oder nutzen Sie unsere Hands-on-Labs, um zu sehen, wie Zerto Ihr Unternehmen schützen und jede (geplante und ungeplante) Unterbrechung bewältigen kann. Mit Zerto haben Sie mehr Zeit, sich auf IT-Innovationen zu konzentrieren und den geschäftlichen Nutzen zu steigern, während Sie Risiken minimieren und die Transformation und Innovationen beschleunigen können.

Architektur 3: Lokale, kontinuierliche Datensicherung und Disaster Recovery in der öffentlichen Cloud

Abbildung 3 zeigt eine Referenzarchitektur mit lokaler Replikation und einem Remote-DR-Ziel in der öffentlichen Cloud.

Abbildung 3



In dieser Konfiguration existieren dieselben VMs in zwei separaten VPGs. Die erste VPG dient der Erstellung des Journals in der Quelle, während die zweite VPG eingerichtet wird, um die Journalfunktion auf dem Remote-Ziel in der öffentlichen Cloud bereitzustellen. Das Cloud-Journal wird in Azure in einem Blob-Speicher oder in AWS in einem S3-Bucket abgelegt und auf der Cloud-Seite konfiguriert. Das reduziert Kosten, da lediglich Speicherkosten anfallen und die Rechenressourcen nur in einem Wiederherstellungsszenario hochgefahren werden.

Das lokale Journal wird am Quellstandort konfiguriert und für die lokale Replikation und Erkennung von Verschlüsselung im Falle eines logischen Ausfalls oder von Ransomware verwendet, was für eine Wiederherstellungsgranularität von wenigen Sekunden sorgt. Der empfohlene Zeitraum für die Journalhistorie beträgt 14 Tage, da damit die meisten logischen Wiederherstellungsszenarien abgedeckt werden. Dank der Deduplizierungsfunktionen moderner Speicher-Arrays wird nur minimaler Speicherplatz verbraucht. Ein täglicher Archivierungsprozess archiviert Zeitpunkte aus dem lokalen Journal in einem externen Repository, um für zusätzliche Sicherheit Unveränderlichkeit zu nutzen.

Bei dieser Architektur beträgt die empfohlene Mindesthistorie des Remote-Journals drei Tage; damit werden die meisten Wiederherstellungsszenarien abgedeckt, wenn es zu einem physischen Ausfall kommt. Alle Änderungen an den geschützten VMs werden dann drei Tage lang aufbewahrt, bevor sie auf das Remote-Replikat im Cloud-Speicher übertragen werden.

Weitere Anwendungsfälle

Zusätzlich zu den standardmäßigen Anwendungsfällen für die Plattform gelten die folgenden Nutzungsfälle speziell für diese Architektur oder weisen besondere Fähigkeiten auf, die zum spezifischen Anwendungsfall hinzukommen.

Cloud-Integration und Migration	Cloud-Nutzung und die damit verbundenen Herausforderungen können mit dieser Architektur vereinfacht werden, da sich Workloads innerhalb weniger Minuten und ohne Datenverluste auf die von Ihnen gewählte Cloud-Plattform verlagern lassen. In diesem Anwendungsfall ist eine langfristige Speicherung während der Migration wahrscheinlich nicht erforderlich. Beispiel: Sie verschieben komplexe Anwendungen in nur drei Schritten in die Cloud.
Multi-Cloud bzw. hybride Cloud	Angesichts der zunehmenden Nutzung von Hybrid- und Multi-Cloud-Strategien bietet Ihnen diese Architektur die Freiheit, Workloads bei Bedarf zu verschieben, wenn sich Anforderungen ändern. Beispiel: Sie verschieben Workloads zu, aus und zwischen Cloud-Plattformen, um maximale Effizienz zu erreichen.

Schlussfolgerung

Zerto bietet Ransomware-Resilienz, Multi-Cloud-Mobilität und DR mit zahlreichen Vorteilen, von Freiheit bei der Auswahl von Herstellern und Clouds bis hin zur schnellen Erkennung und Wiederherstellung. Die verschiedenen möglichen Architekturen zeichnen sich durch Komfort und Agilität aus, wobei Anwendungsfälle das gesamte Spektrum an IT-Infrastrukturen und Teamanforderungen abdecken. Um zu sehen, wie Zerto Ihre IT-Umgebung unterstützen kann, fordern Sie noch heute eine Demo an.

DEMO ANFORDERN

Zusätzliche Ressourcen

Folgende Ressourcen enthalten detailliertere Voraussetzungen, Richtlinien und Informationen zur Dimensionierung.

Zerto-Voraussetzungen und -Anforderungen

Zerto-Richtlinien für Skalierung, Dimensionierung und Benchmarking

Zerto-Interoperabilitätsmatrix

Zerto Analytics

Bitte besuchen Sie https://help.zerto.com, um Zugriff auf die gesamte technische Dokumentation von Zerto zu erhalten.

RITM0090538