Commvault

Cloud Rewind™
Formerly Appranix

eBOOK

Erreichen Sie Cloud Application Resilience mit Wiederherstellungen in Höchstgeschwindigkeit.

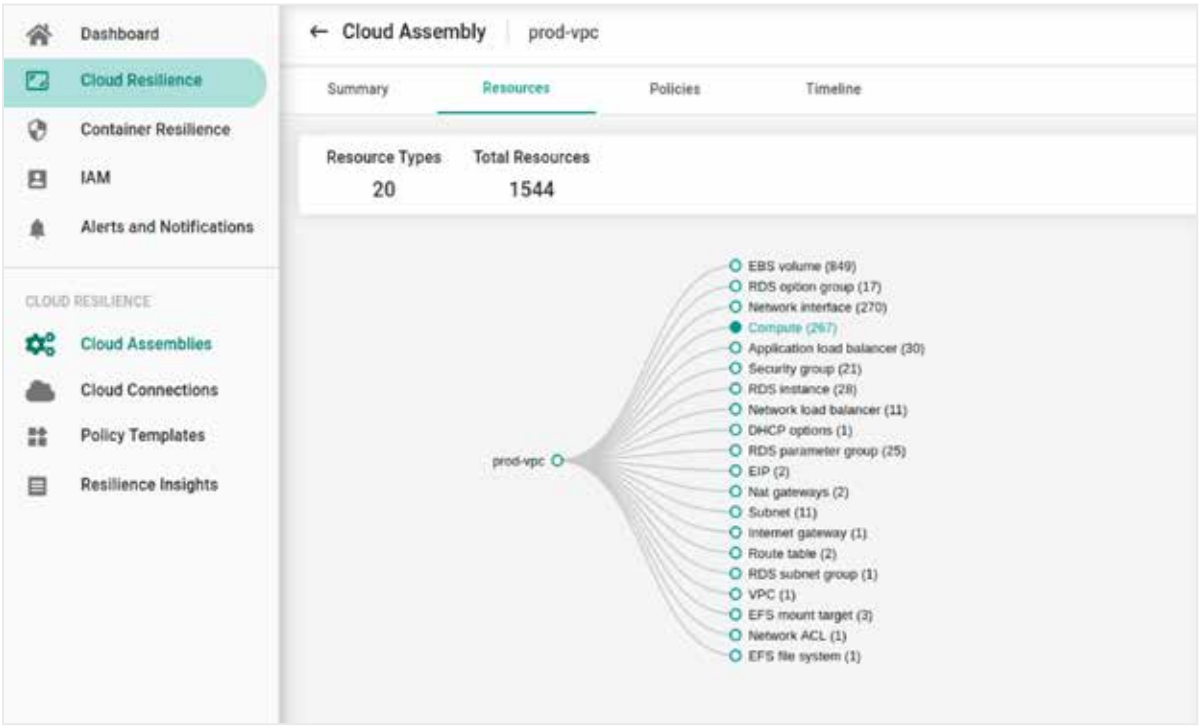
Table of Contents

BEWUSSTSEIN FÜR DIE SUPER SCHNELLE WIEDERHERSTELLUNG DER CLOUD-ANWENDUNGSUMGEBUNG

Cloud-Organisationen haben schnell ein dezentralisiertes Betriebsmodell für ihre Anwendungen und Dienste angenommen. Die Softwarearchitekturen sind ebenfalls verteilter geworden, wobei leicht zugängliche Cloud-Ressourcen in verschiedenen Cloud-Zonen verwendet werden. Site-Reliability-Engineer (SREs) haben durch DevOps-Praktiken dynamischere und schnellere Veröffentlichungszyklen eingeführt, um den steigenden Anforderungen der Kunden gerecht zu werden. Zudem ermöglichen programmierbare Cloud-Ressourcen, dass Umgebungen sich automatisch anpassen, um den Leistungsanforderungen kritischer Geschäftsanwendungen gerecht zu werden.

Allerdings haben all diese Veränderungen auch enorme Herausforderungen für die Teams der gemeinsamen Betriebsdienste geschaffen, die die Resilienz, Sicherheit und Kosten verwalten. Die dringendste Frage heute, insbesondere angesichts der erhöhten Anfälligkeit von Cloud-Umgebungen für Cyberangriffe, lautet, wie diese dynamischen und selbstentwickelnden Anwendungsumgebungen im Falle von Ausfällen schnell wiederhergestellt werden können, indem sie auf die native Cloud-Infrastruktur zurückgreifen, um die SLAs zu erfüllen, die den Unternehmen zugesagt wurden.

WARUM EIN TRADITIONELLES BCDR-DATENZENTRUMSMODELL NICHT FÜR CLOUD-ANWENDUNGEN GEEIGNET IST



Anwendungen hängen nicht mehr von wenigen Servern oder einer einzigen kritischen Datenbank ab. Betrachten wir das folgende Beispiel einer einfachen, dreistufigen Cloud-Anwendung mit automatischer Skalierung, die aus zwei virtuellen Maschinen und einer Datenbank besteht. Sie besteht aus mindestens zwanzig (20) verschiedenen Arten und Instanzen von Cloud-Ressourcen. Traditionelle Backup- und Wiederherstellungssysteme waren darauf ausgelegt, nur die Festplatten von virtuellen Maschinen, Datenbanken und Dateisysteme zu schützen. Um die Resilienz der gesamten Cloud-Anwendung sicherzustellen, müssen alle Cloud-Ressourcen geschützt sein, um jederzeit und in jeder Cloud-Region wiederhergestellt werden zu können. Die herkömmlichen Backup- und Wiederherstellungssysteme wurden nicht dafür entwickelt, alle diese von dynamischen, verteilten und selbstentwickelnden Anwendungen genutzten Cloud-Ressourcen zu schützen, die auf einer softwaredefinierten Cloud-Infrastruktur basieren.

DIE VERBREITUNG VON RANSOMWARE VERÄNDERT DIE ANWENDUNGSWIEDERHERSTELLUNG

Da Ransomware-Angriffe zunehmen und zunehmend raffinierter werden, werden Wiederherstellungen von Cloud-Umgebungen immer schwieriger. Noch wichtiger ist, dass moderne Ransomware-Angriffe speziell auf Backup-Produkte und deren Verwaltungskonsolen abzielen. Da die meisten BCDR-Produkte im gleichen Cloud-Konto wie die Produktionsysteme installiert sind, kann es im Falle eines Ransomware-Angriffs, der das gesamte Cloud-Konto kontrolliert, nicht einmal möglich sein, auf die Konsolen der Backup- und Wiederherstellungssysteme zuzugreifen, um die Anwendungsumgebungen wiederherzustellen. Dies ist möglicherweise eines der kritischen Modelle, die Organisationen überdenken müssen, wenn sie die Resilienzarchitektur der Anwendungen neu gestalten, und nicht nur die Datensicherung und -wiederherstellung.

Da Cloud-Anwendungssysteme aus mehreren Cloud-Infrastruktur-Diensten bestehen, benötigen Benutzer, die nach Ransomware-Angriffen Wiederherstellungen durchführen, ein tiefes Verständnis, um virtuelle Maschinen, Datenbanken, Netzwerke, zahlreiche Cloud-Dienste und die zugehörigen Konfigurationen wiederherzustellen. Oft müssen Schlüsselkomponenten der Anwendungsumgebungen, wie virtuelle private Netzwerke (VPCs), Lastenausgleicher, Gateways, Sicherheitsgruppen, Datenbankparametergruppen usw., von den Cloud-Operations-Teams manuell im Voraus zusammengestellt werden, bevor die BCDR-Systeme für die Datenwiederherstellung eingesetzt werden.

DIE KONTINUIERLICHE ENTDECKUNG VON CLOUD-RESSOURCEN IST DER SCHLÜSSEL ZU BESSERER RESILIENZ

Dynamische und selbstentwickelnde Cloud-Umgebungen stellen enorme Herausforderungen für die Operations-Teams, um sie sicher und resilient zu halten. Da viele Entwicklungsteams die meisten Cloud-Infrastrukturressourcen autonom verwalten, erweitern sich Cloud-Anwendungsumgebungen schneller als im traditionellen Datenzentrum-Modell. Diese programmierbaren und ständig sich verändernden Umgebungen erfordern ein System, das in der Lage ist, alle Ressourcen, die zu einer Anwendung gehören, kontinuierlich zu entdecken. Organisationen verfügen auch über viele Cloud-Konten, um ihre Entwicklungs-, Produktions- und Testumgebungen nach ihren Geschäftsanforderungen zu isolieren. Heutzutage ist es nicht ungewöhnlich, dass Organisationen Hunderte von Cloud-Konten haben.

Die Komplexität vieler Cloud-Konten, verbunden mit ständig sich verändernden Umgebungen, erschwert es zentralisierten Teams, auf traditionelle, nicht anwendungsorientierte Schutz- und Wiederherstellungssysteme zu verlassen. Tatsächlich begnügen sich diese Systeme damit, von den Benutzern die richtigen Ressourcen auszuwählen und den Schutz manuell anzuwenden. Auf der anderen Seite folgen Anwendungsentwickler nicht all den Cloud-Infrastrukturressourcen, die für ihre Anwendungen verwendet werden, was sie daran hindert, den SREs (Site Reliability Engineers) im entscheidenden Moment der Wiederherstellung zu helfen. Oft ändern mehrere DevOps-Pipelines die zentralen Cloud-Umgebungen, was es für die SREs noch schwieriger macht, die Anwendungen zu dem Zeitpunkt wiederherzustellen, wenn es am dringendsten ist. Es ist daher notwendig, ein System zu haben, das die Cloud-Ressourcen kontinuierlich entdeckt und anwendungsorientiert ist, mit der Fähigkeit, durch automatisierte Abhängigkeitskarten das Verständnis der Systemressourcen zu gewährleisten, um alle relevanten Cloud-Ressourcen ordnungsgemäß zu schützen. Dies ermöglicht es dann, Anwendungen, Daten, Konfigurationen, Zustände und Abhängigkeiten schnell wiederherzustellen oder zu failovern, um die Verfügbarkeitsanforderungen der Anwendungen zu erfüllen.

SCHÜTZEN SIE DEN ZUSTAND IHRER CLOUD-UMGEBUNG MIT EINEM LERNENDEN SYSTEM

Gartner schätzt, dass ein typisches Cloud-Umfeld mehr als 50 Konfigurationsänderungen pro Tag durchläuft. Es ist entscheidend, ein unveränderliches Repository für Cloud-Konfigurationsmetadaten für alle kritischen Cloud-Anwendungsumgebungen zu erstellen. Es ist auch sehr wichtig, diese Konfigurationsmetadaten in einem auf einem anderen Cloud-Dienst basierenden Anwendungsresilienzsystem zu hosten, um zusätzliche

Resilienzebenen zu erzielen. Diese Konfigurationsmetadatenschatullen sollten nach Anwendungs-Diensten segmentierbar und für eine Wiederherstellung zu einem bestimmten Zeitpunkt in jeder Cloud-Region protokolliert sein. Sie sollten ausreichend detailliert sein, um den Operations-Teams die Anforderung einer einzelnen Ressource zu einem bestimmten Zeitpunkt zu ermöglichen, um im Falle eines Ausfalls eine bestimmte Instanz eines Cloud-Dienstes schnell wiederherstellen zu können. Ein lernendes System zur kontinuierlichen Entdeckung und Metadatenanalyse eliminiert vollständig die Notwendigkeit einer manuellen Bewertung und die damit verbundenen Risiken durch getrennte Metadaten während des Wiederherstellungsvorgangs.

HYPER-SCHNELLE WIEDERHERSTELLUNG VON VOLLSTÄNDIGEN UMGEBUNGEN MIT DISASTER RECOVERY AS CODE (DR-AS-CODE)

Der komplexeste Teil der Wiederherstellung besteht darin, die passenden Ressourcen für Berechnung, Speicher, PaaS und Netzwerk-Infrastruktur zu identifizieren, die zu einem Satz von Anwendungen gehören, und sie dann zu sequenzieren, um eine orchestrierte Wiederherstellung durchzuführen. Dies wird als “Technischer Wiederherstellungsplan” oder kurz TDP bezeichnet. Es gibt auch einen nicht-technischen Aspekt des Wiederherstellungsplans (DR), der die Bereitstellung menschlicher und organisatorischer Ressourcen für die Validierung der Anwendungen nach der Wiederherstellung betrifft.

TDPs bestehen in der Regel aus mehreren Seiten und erfordern die Zusammenarbeit mehrerer betrieblicher Personen, um zu identifizieren, was in der Produktion funktioniert, hinsichtlich Konfigurationen, Abhängigkeiten, Sequenzierung und Skripten. Organisationen, die traditionelle BCDR-Produkte verwendet haben, können Ihnen sagen, wie komplex TDPs sind und warum sie oft keine Wiederherstellungstests durchführen.

Dank eines automatisierten Infrastruktur-as-Code (IaC)-Modells ist es nun möglich, komplexe manuelle TDPs vollständig zu eliminieren. Insbesondere für garantierte Wiederherstellungen ist es wichtig, ein cloudnaives IaC anstelle eines cloudneutralen IaCs zu verwenden, damit die Verantwortung für die Wiederherstellung großer Systeme an den Cloud-Anbieter übertragen wird, der über dynamisch skalierbare Ressourcen verfügt, um während eines Ausfalls erfolgreich Wiederherstellungen durchzuführen.

VERWALTUNG VON CLOUDBASIERTEN DATENKOPIEN

Cloud-Plattformen verfügen über ausreichende Datenverwaltungsfähigkeiten, um viel schnellere Datenkopien für Backups, Replikationen und Wiederherstellungen durchzuführen. Es ist nicht notwendig, zusätzliche Datenverwaltungsfähigkeiten von Drittanbietern hinzuzufügen. Es ist auch nicht erforderlich, das Speicherformat der nativen Anwendungsdaten in ein allgemeines Datensicherungsformat zu konvertieren oder den langen Prozess des Importierens und Exportierens in ein neutrales Backup-Dateisystem durchzugehen.

Es ist möglich, inkrementelle und konsistente Datenkopien von virtuellen Maschinen und Datenbanken zu erstellen, um die Kosten für Backup und Disaster Recovery (DR) zu reduzieren. Serverlose Dienste verfügen über ausreichende integrierte Datenverwaltungsfähigkeiten, um teure Kopien zu und von hinzugefügten Datenverwaltungsplattformen in einer Cloud-Umgebung zu vermeiden.

Hyperskalierbare Cloud-Plattformen haben den Weg zu einer viel besseren Resilienz im Vergleich zum Datenzentrum-Infrastrukturmodell geebnet. Globale Organisationen können wörtlich inkrementelle Datenreplikationen von einer Cloud-Region in eine andere innerhalb von Minuten durchführen. Dies erhöht nicht nur die Datenresilienz, sondern ermöglicht auch die Erstellung weniger kostenintensiver, mehrfacher Kopien weltweit, was im Falle eines Ausfalls zu viel besseren Anwendungsresilienzniveaus führt.

ZEITMASCHINE FÜR DIE CLOUD-ANWENDUNGSUMGEBUNG

Die Zeitmaschine für die Cloud-Anwendungsumgebung ist ein einfacher Konzept, bei dem ein automatisiertes System alle anwendungsorientierten Cloud-Metadaten aus einem Tresor, die Anwendung aus einem unveränderlichen Repository und die Anwendungsdaten aus dem Speicher und den Datenbanken sammeln kann, um eine synchronisierte Wiederherstellung zu einem bestimmten Zeitpunkt durchzuführen. Man kann sich diese Zeitmaschinen als protokollierte CMDBs vorstellen, die automatisch aus einer anwendungsorientierten Perspektive unter Verwendung aller nativen Cloud-Fähigkeiten aktualisiert werden.

Jedoch ist der wichtigste Unterschied zwischen einer Cloud-Zeitmaschine und den alten CMDBs (Configuration Management Databases), dass sie die Datenkopien zu einem bestimmten Zeitpunkt für die Anwendungen kennt. Im Laufe der Zeit wird eine Cloud-Zeitmaschine für Organisationen unersetzlich, da verschiedene Gruppen innerhalb einer Organisation leicht darauf zugreifen können, um verschiedene Rückgängigmachungs-, Wiederherstellungs- und Failover-Operationen durchzuführen. Traditionelle BCDR-Systeme (Business Continuity and Disaster Recovery) haben nie die Systemmetadaten so gesammelt, dass sie über die einfachen Anforderungen der Datensicherung hinaus nützlich waren.

ZUSAMMENFASSUNG

Die dynamische Natur, die Komplexität und die Geschwindigkeit der Änderungen an Cloud-Anwendungen erfordern wirklich ein neues, anwendungsorientiertes Resilienzmodell, anstelle der aus der Datenzentrumsera stammenden traditionellen Schutz- und Wiederherstellungs- oder Disaster-Recovery-Modelle. Ob Anwendungen in die Cloud migriert wurden oder auf Cloud-Plattformen nativ erstellt wurden, dieses neue Modell ermöglicht nicht nur eine schnelle Wiederherstellung der gesamten Anwendungsumgebungen bei mehreren Ausfällen, sondern reduziert auch erheblich die operativen Albträume, insbesondere wenn kleinere Operations-Teams eine viel größere Anzahl von Ressourcen im Vergleich zur letzten Dekade verwalten.

ÜBER CLOUD REWIND™

Cloud Rewind bietet Anwendungsresilienz in der Cloud mit einem Backup und einer Wiederherstellung der gesamten Cloud-Umgebung, einschließlich aller Ressourcen, Dienste und Abhängigkeiten, zu jedem beliebigen Zeitpunkt und in jeder Cloud-Region.