Cloud-Tiering und Objektspeicher zur Datensicherung – Der Spagat zwischen Kosten und Geschwindigkeit

So erhalten Sie das Beste beider Welten: Einen günstigen Cloudspeicher mit kurzen Datenabrufzeiten. Gewährleisten Sie zunächst die Bereitstellung der richtigen Architektur.

Von Mike Wilson, Director of Technology, Quest®

Es gibt zwei Arten von Organisationen: Organisationen, die die Cloud zur Datensicherung nutzen, und Organisationen, die die Cloud zur Datensicherung nutzen werden.

Und warum sollte man nicht von den Vorteilen der Cloud zur Datensicherung/-wiederherstellung, Notfall-Wiederherstellung und langfristigen Speicherung profitieren? Die Cloud ist mittlerweile omnipräsent und bietet flexible Zugänglichkeit und Kostenstrukturen. Da Unternehmen für die stetig wachsende Menge an Daten, die sich möglicherweise nie ändern oder auf die nur unregelmäßig zugegriffen wird, auf Objektspeicher zurückgreifen, ist Cloud-Tiering zu einem beliebten Tool geworden.

Aber Organisationen nutzen diese Vorteile nicht einfach durch ein Übertragen ihrer Daten in Amazon S3 oder Azure Blockblobs. Sie holen das meiste aus dem Cloudspeicher heraus, wenn sie Änderungen der Architektur in Betracht ziehen und auch implementieren. Nur so können die Vorteile vollumfänglich unterstützt werden. Eine sorgfältige Abwägung in Bezug auf Technologie und Bereitstellung wird sie davor bewahren, teure Fehler zu begehen, wie beispielsweise das Senden von deduplizierten Daten an die Cloud und das Speichern von Daten mit niedriger Priorität in teuren Ebenen (den sogenannten "Tiers").

Bei dieser Abhandlung geht es um die Datensicherung durch Speicherung von Daten in unterschiedlichen Ebenen in der Cloud – dem sogenannten Cloud-Tiering. Untersucht werden Kosten, Nutzen und Risiken im Zusammenhang mit dem Cloud-Tiering von Sicherungsdaten. Mit der richtigen Architektur können sich Organisationen darauf verlassen, dass das Cloud-Tiering die Kosten der Datensicherung senkt und das Leben für Backup-Administratoren vereinfacht.

OBJEKTSPEICHER, CLOUD-TIER, INVESTITIONSAUSGABEN UND BETRIEBSKOSTEN

Mit dem explosionsartigen Wachstum von Daten sowie neuen Arten von Daten, die es zu schützen gilt, ist eine Objektspeicherung von Sicherungsdaten für Unternehmen immer reizvoller geworden. Der Objektspeicher eignet sich ideal für Sicherungsdaten, da er grenzenlos skalierbar und unheimlich kosteneffizient ist, fast überall funktioniert und nicht an eine bestimmte Größe oder ein bestimmtes Format gebunden ist.

Das Cloud-Tiering profitiert vom Objektspeicher in der Cloud. Amazon Simple Storage Service (Amazon S3) und Azure Blockblobs sind Beispiele für Cloudspeicherziele, für die Cloud-Tiering-Lösungen entwickelt wurden, denn sie bieten eine unglaublich

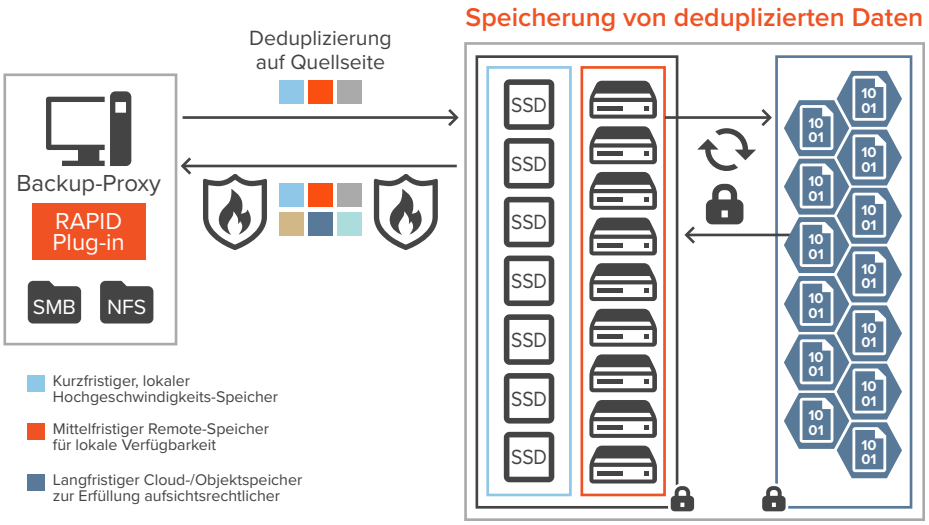

Abbildung 1: Typische Hierarchie für Cloud-Tier-Speicher

Der Objektspeicher eignet sich ideal für Sicherungsdaten, da er grenzenlos skalierbar und unheimlich kosteneffizient ist, fast überall funktioniert und nicht an eine bestimmte Größe oder ein bestimmtes Format gebunden ist. Das Cloud-Tiering nutzt Objektspeicher in der Cloud.

große Skalierbarkeit und unterstützen große Mengen unstrukturierter Daten.

Da Cloudanbieter Speicher zu sehr geringen Kosten anbieten, haben sich schlaue Organisationen für die Cloud als Teil ihrer Speicherstrategie entschieden. Abbildung 1 zeigt das Beispiel einer Backup-Speicher-Hierarchie eines Unternehmens.

Tabelle 1 beinhaltet Details zu den unterschiedlichen Ebenen (Tiers) in der Speicher-Hierarchie. Ein überzeugendes Merkmal bei der Nutzung von Cloud-Tier-Speicher zur Datensicherung (in den letzten beiden Zeilen von Tabelle 1) ist dessen Kostenmodell.

Selbst bei der Datenspeicherung auf Magnetband ist die Infrastruktur für die lokale oder externe Datenspeicherung mit Investitionsausgaben und langfristigen Kauf- und Besitzverpflichtungen verbunden. Neben Hardware, Software und Räumlichkeiten umfasst der Wartungszyklus alle paar Jahre auch die Aktualisierung der Daten. Dieses beinhaltet das erneute Einlesen aller Daten, das Ersetzen der Medien, das Umschreiben der Daten auf neue Medien, das Ersetzen von Laufwerken und das Bezahlen von Personen, die diese Aufgaben letztendlich durchführen.

Das Speichern und Pflegen von Daten in der Cloud geht hingegen mit einer monatlichen Betriebsausgabe einher, die viel einfacher zu kontrollieren ist. Ein Unternehmen, das 100.000 $ Investitionsausgaben zum Aufbau seines Rechenzentrums für langfristigen

Speicher-ebene	Art der zu speichernden Daten	On-/Offline	Wahrscheinlichkeit des Zugriffs/der Wiederherstellung	Speicher-zeitraum	Time to First Byte (TtFB)	Optimale Speicherart	Kosten-modell
Lokal (On-Premises)	Benutzerdateien (Dokumente, allgemeine Produktivität, E-Mails und Anhänge)	Online	Hoch	Bis zu 30 Tage	< 1 Sek.	Datei/Block	Investitions-ausgaben
Remote-Standort	Benutzerdateien	Online	Mittel	Bis zu 90 Tage	< 10 Sekunden	Datei/Block	Investitions-ausgaben
Cloud – Hot und Cold Tiers	Allgemeine Sicherungsdaten	Online	Gering – selten innerhalb eines Monats	3 Monate bis 3 Jahre	< 10 Sekunden	Objekt	Betriebs-ausgaben
Cloud – Archiv und Deep Archive	Daten, die zur langfristigen Einhaltung von Vorschriften erforderlich sind (Finanzwesen, Gesundheitsweisen, öffentlicher Dienst)	Offline	Sehr niedrig – selten innerhalb eines Jahres	Mehrere Jahre	Von Bruchteilen eines Tages bis zu Tagen	Objekt	Betriebs-ausgaben

Tabelle1: Beispiel einer Speicherhierarchie

Sicherungsdaten-Speicher aufwenden muss, könnte es ganz einfach bevorzugen, 1.000 $ pro Monat an Betriebsausgaben für eine ähnliche Kapazität ohne Besitzen der Infrastruktur aufzubringen.

Die Betriebsausgaben und Cloud-Preisgestaltung ermöglichen es Organisationen, ihre Ausgaben entsprechend an ein erforderliches Vergrößern oder Verkleinern des Speichers anzupassen.

DER KOSTENVORTEIL VON CLOUD-TIERS

Warum sollte man also nicht alle Sicherungsdaten in der Cloud speichern, wenn das Kostenmodell dies so sehr begünstigt?

Zunächst einmal sind hier die Übertragungskosten zu nennen. Auch wenn es weniger pro Gigabyte kostet, Daten in der Cloud zu speichern, kostet es mehr pro Gigabyte, Daten anzufordern (d. h. zu lesen, überarbeiten, verzeichnen, kopieren usw.). Daher ergibt es wenig Sinn, die letzte Sicherung als Objekt in der Cloud zu speichern – es ist nämlich wahrscheinlich, dass jemand genau diese Daten abrufen möchte. Die Kosten für das erneute Anrühren des Objekts wird alle möglichen Ersparnisse wieder zunichte machen.

Dann ist auch die Abrufzeit zu bedenken.

Ein wichtiger Faktor bei der Nutzung von Cloudspeicher für Sicherungsdaten ist die Erwartung an die Wiederanlaufzeit (Recovery Time Objective, RTO). Wie in Tabelle 1 dargestellt, können die Abrufzeiten von der Ebene abhängen. Die Speicherebene "Cloud – Archiv und Deep Archive" in der letzten Zeile der Tabelle bezieht sich auf Daten, die faktisch offline mit erheblicher Verzögerung – Time to First Byte oder TtFB – gespeichert werden, um die Daten wieder zugänglich zu machen. Während die Gebühren je nach Ebene variieren, bleiben die Daten über Stunden oder sogar Tage nach der ursprünglichen Abrufanforderung offline. Dies kann mit den Erwartungen an die RTO in Widerspruch stehen.

Ein weiterer wichtiger Faktor, der von Organisationen häufig übersehen wird, ist der Anstieg der Netzwerkkosten bei Verschieben der Sicherungsdaten in die Cloud und zurück. Zum Aufrechterhalten einer WAN-Verbindung zur Cloud und zur häufigen Nutzung für das Cloud-Tiering ist generell eine zusätzliche Bandbreite erforderlich. Diese höheren Kosten sind nicht in den Datentransfergebühren der Cloudanbieter enthalten.

Ziel hierbei ist also, da Beste beider Welten zu erhalten: den geringen Aufwand und die Erschwinglichkeit des Betriebskostenmodells mit der kurzen TtFB des Invenstitionsausgabenmodells.

Die richtige Art von Cloudspeicherkonto macht beide Dinge möglich.

Hot und Cold Storage? Oder Archiv und Deep Archive?

Wie können Administratoren den Balanceakt zwischen niedrigen Speicherkosten und kurzer TtFB bewältigen? Sehen Sie sich dieses typische Speicherschema im Vergleich zu den Ebenen in Tabelle 1 an:

1. Zunächst speichert eine Organisation ihre neuesten Sicherungsdaten der letzten 30 Tage **lokal**, da die "heißesten", dringlichsten und wahrscheinlichsten Datenwiederherstellungen in diesem Zeitraum liegen werden. Die Organisation muss in der Lage sein, die jüngsten Daten schnell wiederherzustellen, um Beeinträchtigungen auf die Geschäftstätigkeit zu vermeiden.

2. Als Nächstes werden die Daten, die für 90 Tage gespeichert werden, in einen **Remote-**Speicher kopiert. Die Daten sind so immer noch schnell abrufbar, aber die Wiederherstellung insgesamt erfolgt etwas langsamer als von der lokalen Ebene aus. Dieses Vorgehen entspricht auch der Best Practice, die eine sekundäre Offsite-Kopie von Sicherungsdaten zur Notfall-Wiederherstellung vorsieht.

3. Dann muss die Organisation manche Daten für einige Jahre für mögliche Audits speichern. Die Wahrscheinlichkeit, dass sie die Daten abrufen muss, ist geringer. Daher ist eine langsamere Wiederherstellung vertretbar. So speichert sie die Daten in der Cloud als **„heiße“ (hot) und „kalte“ (cold)** Objekte.

4. Schließlich speichert sie Daten, die langfristig üblicherweise für die Einhaltung von staatlichen oder aufsichtsrechtlichen Vorschriften erforderlich sind, im **Archiv und Deep Archive**. Die Wiederherstellung findet viel seltener statt und ist viel weniger dringend. Aus diesem Grund werden die Daten am kostengünstigsten, langsamsten Ort gespeichert.

Neben Hardware, Software und Räumlichkeiten umfasst der Wartungszyklus alle paar Jahre auch die Aktualisierung der Daten.

Es ergibt wenig Sinn, die letzte Sicherung als Objekt in der Cloud zu speichern – es ist nämlich wahrscheinlich, dass jemand genau diese Daten abrufen möchte.

Wie viel kostet Cloud-Tiering?

Tabelle 2 fasst die entsprechenden Kosten unterschiedlicher Cloud-Tiers und Speicherdienste zusammen. Bitte beachten Sie, dass die Cloud-Tier "Archivspeicher" (Azure) und "Deep Archive" (Amazon) zwar weniger pro Gigabyte pro Speicher kosten, aber mehr pro Übertragung mit längerer TtFB.

Bei günstigeren, langsameren Angeboten müssen Administratoren die Wiederherstellung des gesamten Objekts anfragen und dann lange auf den Zugriff warten. Dies macht wiederum eine Schnittstelle in der Sicherungs-/Wiederherstellungsanwendung, über die sich die gewünschten Daten anfordern lassen, sowie auch Callbacks, die die Anwendung bei Verfügbarkeit der Daten benachrichtigen, erforderlich.

Je besser sich die Technologie für das Cloud-Tiering eignet, desto mehr Optionen gibt es, um das Beste beider Welten zu erhalten: geringere monatliche Kosten und schnellerer Speicher. Doch diese Vorteile lassen sich nicht einfach nur durch eine Entscheidung für den Objektspeicherweg und das Verschieben aller Sicherungsaufgaben in die Cloud erzielen. Wie so häufig, wenn es um die Cloud geht, ist es erforderlich, sich erneut mit der IT-Architektur auseinanderzusetzen und diese zu optimieren.

Das beginnt schon bei der Sicherheit.

ARCHITEKTUR — SICHERHEIT UND CLOUD-TIERING

Der Objektspeicher verzichtet auf den Mehraufwand von Richtlinien, Benutzerkonten und Zugangsprivilegien. Dies bedeutet jedoch, dass sich Unternehmen nicht auf die üblichen Sicherheitsstrukturen beim Sperren eines Objekts verlassen können. Beim Cloud-Tiering sind eine andere Firewall und andere Zugriffsmuster sowie eine damit verbundene Lernkurve erforderlich.

Service	Ebene (Tier)	Time to First Byte (TtFB)	Speicherkosten/GB/Monat	Kosten für den Datenabruf/GB	Kosten/1.000 Schreibanfragen (PUT)	Netzwerkkosten/GB – eingehend	Netzwerkkosten/GB – ausgehend
Amazon S3 Standard	"Heiß" (Hot)	Von Minuten bis Stunden	0,024–0,026 $	0,00 $	0,0055 $	0,00 $	0,00–0,09 $
Azure Blockblob "Heiß" (Hot)	"Heiß" (Hot)	Von Minuten bis Stunden	0,017–0,184 $	0,00 $	0,005 $	0,00 $	0,00–0,087 $
Amazon S3 Standard – Unregelmäßiger Zugriff	"Kalt" (Cold)	Von Minuten bis Stunden	0,0152–0,019 $	0,01 $	0,01 $	0,00 $	0,00–0,09 $
Azure Blockblob "Kalt" (Cold)	"Kalt" (Cold)	Von Minuten bis Stunden	0,01 $	0,01 $	0,01 $	0,00 $	0,00–0,087 $
Amazon S3 Glacier	Archiv	Von Bruchteilen eines Tages bis zu Tagen	0,005 $	0,011–0,033 $	0,055 $	0,00 $	0,00–0,09 $
Azure Blockblob "Archivspeicher"	Archiv	Von Bruchteilen eines Tages bis zu Tagen	0,00099 $	0,02–0,05 $	0,01 $	0,00 $	0,00–0,087 $
Amazon S3 Glacier Deep Archive	Deep Archive	Von Bruchteilen eines Tages bis zu Tagen	0,002 $	0,022–0,0035 $	0,06 $	0,00 $	0,00–0,09 $

Tabelle 2: Typische Kosten für Cloud-Tiering[1]

1 Auf Grundlage von "*Amazon S3 Preisgestaltung*" (USA, Westen), Microsoft Azure "*Blockblob Preisgestaltung*" und "*Details zur Bandbreitenpreisgestaltung*". Stand: November 2019.

Nehmen Sie einfach an, dass Objektspeicher weniger sicher sind

Eine fehlende Vertrautheit mit der Sicherheit objektbasierter Speicher kann zu Datenschutzverletzungen führen. Viele Datenschutzverletzungen mit großen Auswirkungen sind das Ergebnis des Übertragens eines Objekts in die Cloud (wie z. B. ein Amazon S3 Bucket oder Azure Blob Storage), ohne das Objekt zunächst ordnungsgemäß zu sichern. Benutzer und Administratoren, die nicht mit den Vorgehensweisen bei Infrastructure as a Service (IaaS) vertraut sind, können sehr einfach Fehler machen, indem sie davon ausgehen, dass die Cloud-Sicherheit genauso funktioniert wie die herkömmliche On-Premises-Sicherheit.

So lassen sich Daten sicher an einen Objektspeicher senden

Wenn ein Cloudanbieter die Infrastruktur besitzt, ist es unmöglich, nachzuvollziehen, wer alles auf das Netzwerk zugreifen kann, wer im Rechenzentrum über Berechtigungen verfügt und ob die Sicherheitsvorschriften umgesetzt werden. Für einen sicheren Objektspeicher verschlüsseln intelligente Organisationen daher ihre Daten vor der Übertragung und nutzen ihre eigenen Verschlüsselungscodes statt der Schlüssel des IaaS-Anbieters.

Anwendungen, die Daten sicher in die Cloud übertragen, weisen in einigen Punkten dieselben Verschlüsselungsmerkmale auf. Sie bieten den dem Branchenstandard entsprechenden, FIPS 140-2-konformen 256-Bit-AES-Algorithmus für die Ver- und Entschlüsselung von Benutzerdaten. Sie nutzen Zero-Knowledge-Verschlüsselung, um eine lokale Kontrolle der Verschlüsselungscodes anstelle der Schlüssel des Cloudanbieters zu ermöglichen. Sie beinhalten sich stets ändernde, rotierende Verschlüsselungscodes, die das Risiko einer umfassenden Datenschutzverletzung noch weiter reduziert.

Diese Merkmale entsprechend mindestens der Sicherheit und dem Prozess der meisten lokalen Infrastrukturen – in manchen Fällen ist das Niveau sogar höher.

TECHNOLOGIE-ARCHITEKTUR – DEDUPLIZIERUNG VERRINGERT DIE MENGE AN DATEN, DIE IN DIE CLOUD ÜBERTRAGEN WERDEN

Neben dem Vornehmen von Änderungen an der Architektur für die Sicherheit können IT-Teams den Kompromiss zwischen niedrigen Preisen und einer kürzeren TtFB eingehen, indem sie die Architektur hinter dem Speicher selbst überdenken. Aus Tabelle 1 und Tabelle 2 lässt sich Folgendes schließen: Je weniger Daten in die Cloud verschoben werden, desto geringer sind die Gesamtkosten für das Speichern und Übertragen.

Zur Verringerung der Menge an Sicherungsdaten, die die lokale Infrastruktur verlassen, stehen Unternehmen primär die Technologien der Deduplizierung ("deduplizieren") und Komprimierung zur Verfügung.[1] Bei der Deduplizierung werden Algorithmen genutzt, um die Daten zu scannen und alle Elemente zu entfernen, die bereits gespeichert wurden. Dabei werden diese durch eine Verknüpfung ("Pointer") zu ähnlichen, gesicherten Daten ersetzt.

Genauer gesagt, handelt es sich bei einer quellseitigen Deduplizierung in Kombination mit einer Komprimierung um die effektivste Art und Weise, die Größe der zu speichernden Daten zu reduzieren, bevor diese in den Speicher übertragen werden. So kann das Verschieben von Daten deutlich beschleunigt und die Verarbeitungsmenge erhöht werden.

Tatsächlich ermöglicht es eine Kombination von Komprimierung und Deduplizierung mit einer "heißen“ (hot) oder "kalten" (cold) Cloud-Tier das Beste beider Welten zu erhalten: niedrigere Preise und kürzere TtFB.

> Die Vorteile geringerer monatlicher Kosten und eines schnelleren Speichers lassen sich nicht einfach durch das Verschieben aller Sicherungsaufgaben in die Cloud erzielen. Es ist erforderlich, sich erneut mit der IT-Architektur auseinanderzusetzen und diese zu optimieren.

ARCHITEKTUR – DIE RICHTIGE CLOUD-TIER-TECHNOLOGIE FINDEN

Welche Faktoren spielen bei der Verringerung der zu speichernden Datenmenge eine Rolle, bevor die Daten die lokale Infrastruktur verlassen?

Bandbreite

Wie schon zuvor erwähnt, rechnen einige Unternehmen mit der Erfordernis einer WAN-Verbindung mit größerer Kapazität und einem Anstieg der Netzwerkkosten. Da die quellseitige Deduplizierung jedoch nur deltabasiert speichert und Cloud-Tiering durchführt, können diese Unternehmen bei der benötigten Bandbreite und dem erforderlichen Speicherplatz eine Reduktion um bis zu 80 Prozent feststellen. Dadurch erübrigt sich ein langfristiges Upgrade der WAN-Verbindungskapazität. (Hinweis: Eine Deduplizierung, die nicht auf der Quellseite stattfindet, beinhaltet das

1 Eine ausführliche Abhandlung zu Deduplizierungstechniken finden Sie in “*Deduplizierung: Die versteckte Wahrheit und was Sie diese kostet*”, eine technische Kurzbeschreibung von Quest.

Für einen sicheren Objektspeicher verschlüsseln intelligente Organisationen ihre Daten lokal und nutzen ihre eigenen Verschlüsselungscodes statt der Schlüssel des IaaS-Anbieters.

Übertragen einer vollständigen Kopie der zu speichernden Daten. Dies verbraucht Netzwerkbandbreite und Speicherplatz auf der Zielseite.)

Sliding-Window-Deduplizierung variabler Länge

Die Sliding-Window-Deduplizierung variabler Länge stellt den Goldstandard bei der Datenreduktion dar. Anwendungen, die über diese Methode verfügen, können Daten in die Cloud übertragen, diese dort speichern und effizient wieder an einen lokalen Ort zurückholen – und dabei senken sie die monatlichen Speicherkosten auch noch um bis zu 95 Prozent.

Lokaler Speicher

Anwendungen, die quellseitig deduplizieren, können sich die lokale Kapazität zunutze machen, um denselben Wiederanlaufzeitpunkt (Recovery Point Objective, RPO) ohne Steigerung der WAN-Verbindungskapazität zu erreichen. Sie können das Abrufen von Daten aus der Cloud beschleunigen und gleichzeitig einen Echtzeit-Zugriff auf die Daten sowie in vielen Fällen eine Wiederherstellung von Daten innerhalb von Minuten statt Tagen bereitstellen.

Transparenter Betrieb

Im transparenten Betrieb verringert die Anwendung, welche die Daten liest und schreibt, die Komplexität, indem sie immer gleich vorgeht – unabhängig davon, ob die Daten auf einem lokalen Gerät oder in der Cloud gespeichert sind. Dies bedeutet, dass sie den lokalen Speicher durch transparente Sicherung und Wiederherstellung der Daten auf die Cloud erweitert, ohne dass weitere Maßnahmen erforderlich wären. Bei der Wiederherstellung von Daten befreit sie die Administratoren von der Aufgabe, den Speicherort eines Objekts ausfindig zu machen und darauf zu warten, dass die Daten wieder zugänglich sind.

CLOUD-TIER- SICHERUNG – EIN BEISPIEL

Stellen Sie sich eine Organisation vor, die sich dazu entscheidet, Daten für 30 Tage lokal zu speichern und diese danach in einer Online-Cloud-Tier zu sichern. Eine transparente Anwendung, die für Cloud-Tier-Daten entwickelt wurde, sollte keine spezielle Konfiguration erfordern. Dafür sollte sie ältere und möglicherweise kostspielige Methoden wie Magnetband-Sicherungen und Offsite-Speicher und -Verarbeitung ersetzen. Administratoren können einfach eine Richtlinie in der Sicherungsanwendung festlegen, welche die Daten automatisch dedupliziert, komprimiert, verschlüsselt und dann nach 30 Tagen an eine verfügbare Cloud-Tier sendet.

Da die Daten vor der Übertragung in die Cloud komprimiert und dedupliziert wurden, sind die Kosten geringer als bei günstigeren, langsameren Cloudspeichern, wie Amazon Glacier und Azure-Archivspeicher. Diese wärmere Online-Cloud-Tier ermöglicht hingegen eine ständige und einfache Verfügbarkeit aller Sicherungsdaten.

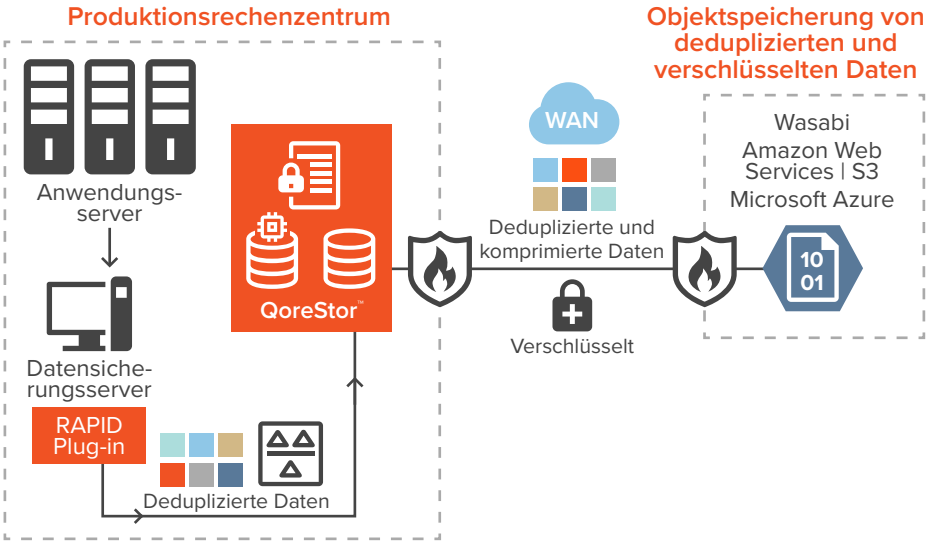

Abbildung 2: Cloud-Tier-Sicherung vom Rechenzentrum zu Cloudspeicheranbietern (Azure, AWS, Wasabi)

Bei der Wiederherstellung ist dann bei einer transparenten Anwendung kein manuelles Eingreifen erforderlich. Und noch wichtiger: Administratoren müssen Daten oder Sicherungsbilder nicht ausfindig machen oder überhaupt wissen, wo die Daten derzeit gespeichert sind. Sie starten den Wiederherstellungsprozess bei den gewünschten Daten und die Anwendung übernimmt die Aufgabe des Findens und Wiederherstellens der Daten. Das Abrufen erfolgt schneller, da die Deduplizierung lokale Datenobjekte abgleicht, bevor sie Daten aus dem Cloudspeicher abruft. Zudem ist dies weniger kostenaufwendig, da die Übertragungskosten zum Lesen der Clouddaten geringer sind. Die Anwendung setzt die Daten wieder zusammen und stellt sie wieder her.

Abbildung 2 zeigt eine typische Konfiguration für eine Cloud-Tier-Sicherung mithilfe von Quest QoreStor™ – mit Deduplizierung und Komprimierung zur Reduzierung der Datenmenge, die über die WAN-Verbindung übertragen wird.

FAZIT – FRAGEN, DIE GESTELLT WERDEN SOLLTEN

Für einige Unternehmen und Administratoren stellt das Cloud-Tiering eine verlockende Alternative zur Magnetband-Sicherung dar: neuere Technologie, weniger Aufwand, geringere Speicherkosten und weniger Fehlerstellen. Doch bevor sie alle ihre Sicherungen und Archive vom Band in die Cloud übertragen, sollten Administratoren ihre Architektur vor dem Hintergrund einer strategischer Fragen betrachten:

- Wie viele Daten muss ich monatlich speichern?
- Wie häufig muss ich die Daten abrufen und verarbeiten?
- Wie lange sollte ich die Daten lokal speichern, bevor ich sie in die Cloud verschiebe?
- Sollte ich zwei Kopien der Daten für Notfälle speichern?
- Welche RPO und RTO erwarten Benutzer bei Wiederherstellungen? Wie schnell muss ich in der Lage sein, Daten abzurufen und wiederherzustellen?
- Wie kann ich die Zeit produktiv nutzen, wenn sich mehrere Wiederherstellungsjobs angesammelt haben? Oder muss ich jeden Job einzeln überwachen und warten, bis dieser abgeschlossen ist?
- Wie viel effizienter könnte ich arbeiten, wenn alle Datenbewegungen durch Richtlinien automatisiert wären?
- Wie viel einfacherer wäre meine Tätigkeit, wenn alle Sicherungsdaten (unabhängig von ihrem Alter) direkt zugänglich wären?

Die Online-Cloud-Tier-Technologie – in Kombination mit der richtigen Sicherungsanwendung, Komprimierung und quellseitiger Deduplizierung und Verschlüsselung – bietet die besten Möglichkeiten für eine transparente, kosteneffektive Datensicherungsstrategie. Sie nutzt kostengünstigen Cloud-Objektspeicher für eine hocheffiziente Wiederherstellung von Daten der letzten Sicherungen und aus Langzeitarchiven.

Durch Änderungen an der Architektur zur Nutzung von Objektspeicher wird die Übertragung von Daten an einen Offsite-Speicherort vollständig automatisiert und das Abrufen ist transparent. Unternehmen können die Kosten für die Datensicherung senken und Zeit und Ressourcen von Backup-Administratoren auf wichtigere Aufgaben lenken. Eine transparente Cloud-Tier-Lösung verringert Arbeitsaufwand, Kosten, Zeit und Risiko.

INFORMATIONEN ZUM AUTOR

Mike Wilson verfügt über mehr als 20 Jahre Erfahrung mit Anwendungen und End-to-End-Lösungen. Zuletzt arbeitete er an der Deduplizierungs-, Komprimierungs- und Replikations-Engine, die in Quest QoreStor zum Einsatz kommt. Er war bereits als IT-Administrator, Netzwerkarchitekt und QoreStor Architect tätig und hat nun die Position des Director of Technology in der Abteilung "Data Protection" von Quest inne.

Die Kombination von Komprimierung und Deduplizierung mit einer "heißen“ (hot) oder "kalten" (cold) Cloud-Tier ermöglicht es, das Beste beider Welten zu erhalten: niedrigere Preise und kürzere TtFB.

ÜBER QUEST

Quest liefert Softwarelösungen für die ständig im Wandel befindliche Welt der Unternehmens-IT. Wir helfen, die durch Datenexplosion, Cloud-Erweiterung, Hybrid-Rechenzentren, Sicherheitsbedrohungen und gesetzliche Bestimmungen hervorgerufenen Schwierigkeiten zu verringern. Wir sind der globale Anbieter für 130.000 Unternehmen in 100 Ländern, einschließlich 95 % der Fortune 500 und 90 % der Global 1000. Seit 1987 entwickeln wir eine Palette von Lösungen, die aktuell Datenbankverwaltung, Datensicherung, Identitäts- und Zugriffsverwaltung, Microsoft-Plattformverwaltung sowie die Verwaltung vereinheitlichter Endgeräte umfasst. Mit Quest investieren Unternehmen weniger Zeit in die IT-Administration und haben mehr Zeit für geschäftliche Innovationen. Weitere Informationen finden Sie auf www.quest.com.

Sollten Sie Fragen hinsichtlich der potenziellen Nutzung des Materials haben, wenden Sie sich bitte an:
www.quest.com/de-de/company/contact-us.aspx