Reduzierung der Cloud-Sicherungskosten mit Quest® QoreStor®

Nutzung von kostengünstigem Objektspeicher und Cloud-basierter Deduplizierung

EINFÜHRUNG

Objektspeicher, der oft als objektbasierter Speicher bezeichnet wird, ist eine Datenspeicherarchitektur zur Bewältigung großer Mengen an unstrukturierten Daten. Unstrukturierte Daten sind Daten, die nicht zu einer klassischen relationalen Datenbank mit Zeilen und Spalten passen bzw. nicht einfach bequem in eine solche Datenbank eingeordnet werden können. Die heutigen Internetkommunikationsdaten – wie E-Mails, Videos, Fotos, Webseiten, Audiodateien, Sensordaten und andere Arten von Medien und Webinhalten (in Textform oder nicht) – sind größtenteils unstrukturiert.

Aufgrund der skalierbaren und flexiblen Kostenstruktur steigen immer mehr Unternehmen von Bändern auf kostengünstigen Cloud-Objektspeicher zum Sichern ihrer exponentiell wachsenden Volumen an strukturierten und unstrukturierten Daten um. Dies gilt insbesondere für Daten, die sich womöglich nie ändern oder auf die möglicherweise nur selten zugegriffen wird. Cloud-basierte Objektspeicherlösungen bieten hohe Skalierbarkeit, angemessene Leistung, niedrige Kosten und einfache Verwaltung. Statista hat 2020 festgestellt, dass 94 % der weltweit befragten Kleinunternehmen und 81 % der mittleren und großen Unternehmen eigenen Angaben zufolge die Cloud für die Datenspeicherung oder Sicherung verwendet haben.[1]

Aber Organisationen nutzen diese Vorteile nicht einfach durch ein Übertragen ihrer Daten in Amazon S3, Azure Blockblobs oder Google Cloud. Sie ziehen den größten Nutzen aus Cloud-Speicher, wenn sie architekturbezogene Änderungen 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 Datenduplikaten an die Cloud und das Speichern von Daten mit niedriger Priorität in teuren Cloud-Speicherebenen („Tiers“).

In diesem Whitepaper wird erläutert, wie Sie die Cloud-Objektspeicheranforderungen und die Kosten für die Datensicherung deutlich reduzieren können. Mit den richtigen Verfahren und der richtigen Technologie können Sie Objektspeicher in der Cloud nutzen, um die Gesamtkosten für die Datensicherung zu senken.

Mehr als 80 % der befragten Unternehmen aus aller Welt haben die Cloud zum Speichern von Daten oder für Sicherungen genutzt.

DIE BELIEBTHEIT VON OBJEKTSPEICHER

Angesichts des explosionsartigen Datenwachstums und der neuen Arten von Daten, die es zu schützen gilt, ist die Nutzung von Objektspeicher für 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 Marktforschungsunternehmen IDC geht davon aus, dass unstrukturierte Daten bis 2025 ganze 80 % aller Daten weltweit ausmachen werden.

Amazon Simple Storage Service (Amazon S3), Azure Blockblobs und Google Cloud sind Beispiele für Cloud-Objektspeicherziele, die eine unglaublich hohe Skalierbarkeit bieten und große Mengen unstrukturierter Daten unterstützen. Objektspeicher ist in der Regel nicht nur weniger komplex – die Komponenten sind auch kostengünstiger und die Leistungserwartungen niedriger als bei Blockspeicher. Das ermöglicht es Cloud-Anbietern, Objektspeicher zu relativ günstigen Preisen anzubieten. Für intelligente Organisationen eröffnet sich dadurch die Chance, die Cloud in ihre Datensicherungsstrategie einzubinden.

SICHERHEITSÜBERLEGUNGEN BEI OBJEKTSPEICHER

Für die klassische Datensicherheit vor Ort sind sowohl physische als auch netzwerkbasierte Schutzmaßnahmen und entsprechende Investitionen in Hardware und Sicherheits-Know-how erforderlich. Unter Umständen werden für jede Ebene der Unternehmensinfrastruktur separate Sicherheitstools benötigt. Lokale Sicherheitsteams können den Zugang zu ihren Rechenzentren steuern und Datensicherheitsrichtlinien entwickeln und erzwingen. Cloud-Objektspeicher ist anders und kann Benutzern und Administratoren fremd sein, die keine Erfahrung mit Infrastructure as a Service (IaaS) haben.

Beim Speichern von Daten bei einem Cloud-Anbieter teilen Sie sich die Verantwortung für den Schutz dieser Daten mit dem Anbieter. Doch wenn ein Cloud-Anbieter die Infrastruktur besitzt, ist es unmöglich, nachzuvollziehen, wer auf das Netzwerk zugreifen kann, wer Zugang zum Rechenzentrum hat und ob Sicherheitsrichtlinien erzwungen werden. Wenn sie keine Kontrolle über die physische Sicherheit haben, müssen Organisationen sich auf ihre Daten konzentrieren, um den unbefugten Zugriff auf Cloud-Sicherungen zu verhindern. Das bedeutet, dass die Datenverschlüsselung als Teil des Sicherungsprozesses stärker in den Fokus rücken muss und Sie sich vergewissern müssen, dass Ihre Sicherungstools zuverlässige Verschlüsselungsfunktionen bieten. Für einen sicheren Objektspeicher verschlüsseln intelligente Organisationen ihre Daten vor der Übertragung. Außerdem nutzen sie nicht die vom IaaS-Anbieter bereitgestellten Verschlüsselungsschlüssel, sondern ihre eigenen.

Sicherungsanwendungen, 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 Verschlüsselungsschlüssel zu ermöglichen, statt die Schlüssel des Cloud-Anbieters zu verwenden. Sie setzen auf sich stets ändernde Verschlüsselungsschlüssel, die das Risiko einer umfassenden Datensicherheitsverletzung noch weiter reduzieren. Diese Merkmale entsprechen mindestens der Sicherheit und dem Prozess der meisten lokalen Infrastrukturen – in manchen Fällen ist das Niveau sogar höher.

REDUZIERUNG DER IN DER CLOUD GESPEICHERTEN DATENMENGE DURCH DEDUPLIZIERUNG

Die Datendeduplizierung und Komprimierung sind die primären Technologien, die Unternehmen zum Reduzieren der Menge an gespeicherten Sicherungsdaten und der zugehörigen Kosten zur Verfügung stehen. Bei der Deduplizierung kommen Algorithmen

zum Einsatz, um die Daten bei Aufnahme zu scannen und alle Elemente zu entfernen, die bereits gespeichert wurden. Dabei werden diese durch eine Verknüpfung („Pointer“) zu gleichen Sicherungsdaten ersetzt, die bereits gespeichert sind.

Speziell die quellseitige Deduplizierung ist in Kombination mit der Komprimierung die effektivste Art und Weise, das zu speichernde Datenvolumen zu reduzieren, bevor die Daten auf den lokalen Speicher oder in die Cloud übertragen werden. Durch die Deduplizierung kann das Verschieben von Daten deutlich beschleunigt und der Durchsatz erhöht werden. In Anbetracht des wachsenden Trends der Nutzung von Cloud-Speicher für Sicherungsdaten ist es sinnvoll, die Sicherungsdaten selbst zu deduplizieren, bevor sie gespeichert werden. Es stehen verschiedene Cloud-Speicheroptionen zur Wahl, darunter verwaltete Datenträger, Objektspeicher und Speicher für kalte Daten. Da die Speicherkosten angesichts immer größerer Datensätze ein Problem darstellen, müssen IT-Organisationen Kosten und Leistung abwägen, um den richtigen Cloud-Speicher zu ermitteln. Oftmals fällt die Wahl dann auf Objektspeicher.

QORESTOR

QoreStor ist eine softwaredefinierte Sekundärspeicherlösung, die die Sicherungsleistung steigert, die Speicherkosten senkt und Ihre Datensicherungslösung sicher mit der Cloud verbindet. Bei Bereitstellung in der Cloud ermöglicht sie die Nutzung von Cloud-basiertem Objektspeicher anstelle von dediziertem Speicher oder verwaltetem Speicher.

QoreStor kann mit praktisch jeder Sicherungslösung verwendet werden und bietet die Möglichkeit, Daten in Cloud- und lokalem Objektspeicher zu speichern. Dadurch trägt QoreStor zum Schutz der Investitionen von Kunden in vorhandene Datensicherungslösungen und Speicherressourcen bei. Durch das Ausführen von QoreStor in der Cloud unter Verwendung von Objektspeicher können die Kosten für die Speicherung von Objektdaten in der Cloud im Vergleich zu nativem Cloud-basiertem Objektspeicher um das bis zu 15-Fache reduziert werden.

QoreStor arbeitet nahtlos im Rahmen des Speichermechanismus der Sicherungsanwendung. Die Lösung bietet zahlreiche Verbindungsmethoden (z. B. S3, OST, RDA, SMB (CIFS) und NFS),

QoreStor kann die Kosten für Cloud-Objektspeicher um das 15-Fache reduzieren.

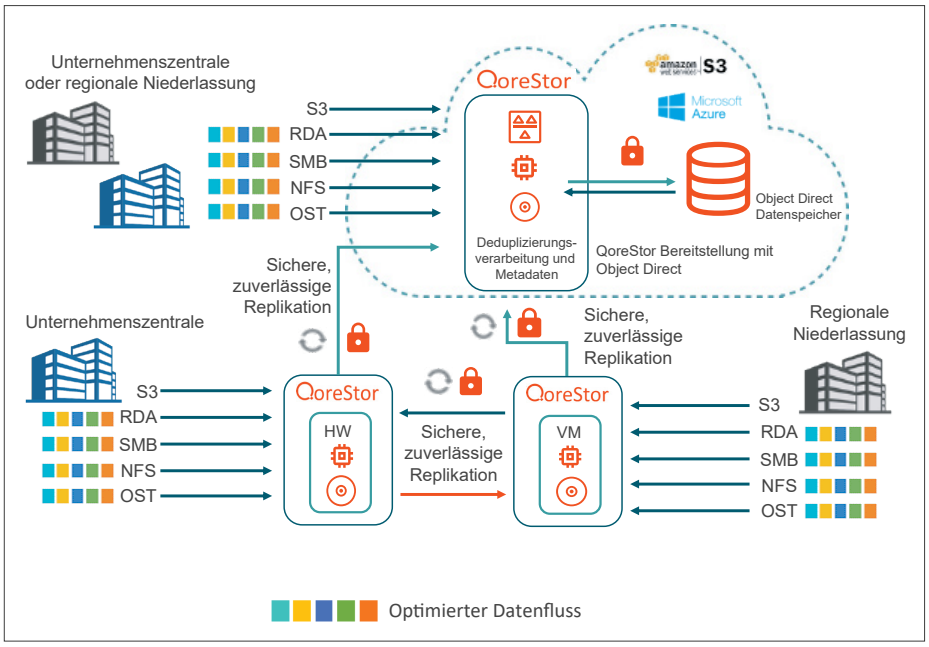

Abb. 1. Verwendung von QoreStor mit einer Sicherungslösung und Cloud-Objektspeicher

Quest

sodass Sie sie mit den beliebtesten Sicherungsanwendungen und Speichermedien verwenden können. Alle diese Verbindungen können zum Senden von Daten an QoreStor verwendet werden – ganz gleich, ob die Lösung lokal oder in der Cloud ausgeführt wird. So können Benutzer Objektspeicher ortsunabhängig nutzen.

QoreStor bietet leistungsstarke quellseitige Datendeduplizierung mit variabler Blocklänge, um den Netzwerkverkehr im LAN oder über das WAN zur Cloud zu minimieren, und kann die Anforderungen und Kosten für die lokale und Cloud-basierte Speicherung um bis zu 95 % reduzieren.

Für Notfallwiederherstellungszwecke müssen IT-Organisationen mehr als eine Kopie der Sicherungsdaten speichern. Viele setzen auf die beliebte 3-2-1-Regel, die vorschreibt, dass drei Kopien der Daten (Produktionsdaten und zwei Sicherungskopien) auf zwei unterschiedlichen Medien (wie Festplatte und Band oder Festplatte und Cloud) und eine Kopie extern oder in der Cloud gespeichert werden. QoreStor ermöglicht die schnelle, sichere Replikation, sodass Sicherungsdaten an mehreren Orten gespeichert werden können (auch in der Cloud). Mit der Lösung kann die Replikationszeit um das bis zu 15-Fache verkürzt und sichergestellt werden, dass die Replikation abgeschlossen wird – sogar bei unzuverlässigen WAN-Verbindungen.

Sicherheit, Integrität und Verfügbarkeit sind wichtige Elemente in jedem Cloud-Sicherungsprozess. QoreStor erstellt einen Kanal mit TLS 2.0 Sicherheit, der auch bei WAN-Ausfällen stabil bleibt. Sie können die Datensicherheit auch mit integrierter Verschlüsselung am Speicherort und FIPS 140-2-Compliance stärken. Dabei kann eine statische oder eine rotierende Zero-Knowledge-Verschlüsselungstechnologie zum Einsatz kommen.

ZUSAMMENFASSUNG

Das exponentielle Datenwachstum veranlasst IT-Organisationen dazu, wertvolle Budgetmittel für Sicherungsspeicher auszugeben, was sich auf das Geschäftsergebnis von Unternehmen auswirkt. Eine öffentliche Cloud kann eine kosteneffizientere Speicherlösung bereitstellen, insbesondere wenn es um Objektspeicher oder Speicher für „kalte“ Daten geht. QoreStor trägt zur beträchtlichen Reduzierung sämtlicher Anforderungen und Kosten für Cloud-Speicher bei und bietet eine schnelle, sichere Möglichkeit zum Replizieren von Sicherungen in die Cloud. Mit QoreStor können Organisationen mehr Daten öfter sichern oder einen Teil des Speicherbudgets für Initiativen verwenden, die dem Unternehmenswachstum zugutekommen.

Die Vorteile von QoreStor

- Reduziert im Vergleich zu nativem Cloud-basiertem Objektspeicher die Kosten für das Speichern von Sicherungsdaten auf Cloud-Objektspeicher um das 15-Fache.
- Reduziert die langfristigen Speicherkosten um das bis zu 10-Fache, indem AWS Glacier und Deep Glacier verwendet wird.
- Optimiert Ihre Technologieinvestition durch Integration in die meisten Sicherungsanwendungen der nächsten Generation, die S3 Objektspeicher nutzen, und Optimierung ihrer Daten.

Weitere Informationen zu QoreStor finden Sie unter www.quest.com/qorestor.

[1] https://www.statista.com/statistics/1114063/worldwide-share-cloud-usage-for-data-storage-and-backup-by-size/

ÜBER QUEST

Quest stellt Softwarelösungen bereit, die die Vorteile neuer Technologien in einer immer komplexeren IT- Landschaft real werden lassen. Von der Datenbank- und Systemverwaltung über die Verwaltung von Active Directory und Office 365 bis zur Cyber-Resilienz: Quest hilft Kunden, bereits jetzt ihre nächste IT-Herausforderung zu bewältigen. Weltweit vertrauen mehr als 130.000 Unternehmen und 95 % der Fortune 500 Quest die proaktive Verwaltung und Überwachung für die nächste Unternehmensinitiative sowie die Bestimmung der nächsten Lösung für komplexe Microsoft Herausforderungen an, um für die nächste Bedrohung gewappnet zu sein. Quest Software Der Zukunft einen Schritt voraus

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