Präsentiert von

rubrik

Cloud Data Management

für dummies

Sichere Daten an jedem Speicherort

Moderne Cloud-Data-Management-Lösungen

Verschlüsselung und Schutz von Backups

Rubrik Sonderausgabe

Lawrence Miller

Über Rubrik

Rubrik (https://www.rubrik.com/en) hilft Unternehmen dabei, die nötige Datenkontrolle für mehr Unternehmensresilienz, Cloud-Mobilität und Compliance zu erzielen. Rubrik schließt die Lücke zwischen unternehmenseigener On-Premises-Infrastruktur und der Cloud. Daten werden durch eine softwaredefinierte Fabric vom Rechenzentrum entkoppelt und über eine einzige Managementebene für alle Daten verwaltet, ganz gleich, ob sie sich vor Ort oder in der Cloud befinden. Umfassendes Datenmanagement wird durch sofortigen Zugriff, automatische Orchestrierung sowie Datenschutz und Ausfallsicherheit der Enterprise-Klasse ermöglicht.

Cloud Data Management

Rubrik Sonderausgabe

Lawrence Miller

für dummies®

Cloud Data Management Für Dummies®, Rubrik Sonderausgabe

Veröffentlicht von
John Wiley & Sons, Inc.
111 River St., Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-84959-9 (pbk); ISBN 978-1-119-84903-2 (ebk)

Hergestellt in den Vereinigten Staaten von Amerika

10 9 8 7 6 5 4 3 2 1

Allgemeine Informationen zu unseren sonstigen Produkten und Dienstleistungen oder zur Erstellung eines individuellen *Für Dummies*-Buches für Ihr Unternehmen oder Ihre Organisation erhalten Sie von unserer Abteilung Business Development in den USA unter Tel. 877-409-4177, E-Mail: info@dummies.biz, oder besuchen Sie www.wiley.com/go/custompub. Für Informationen zur Lizenzierung der *Für-Dummies*-Marke für Produkte oder Dienstleistungen kontaktieren Sie bitte: BrandedRights&Licenses@Wiley.com.

Danksagung des Verlags

Die folgenden Personen haben bei der Erstellung dieses Buches mitgewirkt:

Development Editor: Rebecca Senninger

Acquisitions Editor: Ashley Coffey

Editorial Manager: Rev Mengle

Business Development Representative: William Hull

Production Editor: Mohammed Zafar Ali

Inhaltsverzeichnis

Einführung

Daten sind das wertvollste Gut eines Unternehmens. Nun, wahrscheinlich stimmt das nicht ganz. Ihre Mitarbeiter sind sicherlich Ihr wertvollstes Gut – doch Daten kommen direkt danach! Im Gegensatz zu Gold, Diamanten, Öl und anderen wertvollen Gütern sind Daten jedoch nichts Seltenes. Man findet sie überall – in Ihren On-Premises-Rechenzentren, in SaaS-Anwendungen (Software-as-a-Service) und in der Public Cloud. Und wie jedes andere wertvolle Gut müssen Daten richtig verwaltet, geschützt und gesichert werden, damit sie jederzeit zur Verfügung stehen – aber nur für die richtigen Personen und niemals für die falschen.

Über dieses Buch

Cloud Data Management für Dummies behandelt die folgenden Themen in sechs Kapiteln:

- Warum Unternehmen eine moderne Cloud-Data-Management-Lösung benötigen (Kapitel 1)
- Wie ein deklaratives Modell des Datenlebenszyklus-Managements das Datenmanagement vereinfacht (Kapitel 2)
- Wie Sie Ihre Daten mit mehrschichtiger Datensicherheit schützen können (Kapitel 3)
- Was benötigt wird, um Daten nach Bedarf verfügbar zu machen (Kapitel 4)
- Wie erweiterbares Datenmanagement neue Anwendungsfälle ermöglicht (Kapitel 5)
- Welche Fähigkeiten eine moderne Cloud-Data-Management-Lösung aufweisen sollte (Kapitel 6)

Jedes Kapitel ist in sich geschlossen. Sie können deshalb einfach zu einem Thema springen, das Ihr Interesse weckt. Lesen Sie das Buch, wie es Ihnen am liebsten ist (verkehrt herum oder rückwärts würden wir allerdings nicht empfehlen).

Leichtfertige Annahmen

Man sagt, dass sich die meisten unserer Annahmen bestätigt haben. Im Folgenden erlaube ich mir, einige Annahmen zu treffen!

Ich nehme an, dass Sie ein Datenbankadministrator, ein Techniker, Infrastruktur-Architekt oder Analyst für die Datensicherung und -wiederherstellung oder eine IT-Führungskraft sind, die für den Schutz der kritischen Geschäftsdaten Ihres Unternehmens verantwortlich ist. Außerdem nehme ich an, dass Sie mit Datenverwaltungsproblemen und den Grundlagen der Datensicherung und -wiederherstellung vertraut sind.

Wenn Sie sich in einer dieser Beschreibungen wiedererkennen, dann ist dieses Buch genau richtig für Sie! Wenn nicht, sollten Sie trotzdem weiterlesen. Dieses Buch ist äußerst hilfreich, und wenn Sie es gelesen haben, werden Sie eine ganze Menge über Cloud-Sicherheit und Cloud-Compliance wissen!

In diesem Buch verwendete Symbole

In diesem Buch verwende ich gelegentlich besondere Symbole, um Ihre Aufmerksamkeit auf wichtige Informationen zu lenken. Sie werden auf die folgenden Hinweise stoßen:

MERKEN

Dieses Symbol macht auf Informationen aufmerksam, die Sie Ihrem Festspeicher bzw. Ihrem Kopf anvertrauen sollten!

TECHNISCHES

Wenn Sie in Zukunft mit Fachbegriffen und -wissen prahlen möchten, sind Sie hier an der richtigen Stelle! Dieses Symbol erläutert den Jargon hinter dem Jargon!

TIPP

Tipps sind immer willkommen – vor allem, wenn man nicht mit ihnen rechnet. Die Tipps in diesem Buch werden bestimmt nützlich für Sie sein.

HINWEIS

Dieses Symbol macht auf Dinge aufmerksam, vor denen Sie Ihre Mutter schon immer gewarnt hat (oder auch nicht). Es lohnt sich, diese praktischen Ratschläge zu beherzigen.

Zusätzliche Informationen

Natürlich kann ich in diesem Buch nur eine Auswahl der wichtigsten Themen behandeln. Wenn Sie am Ende dieses Buches unbedingt noch mehr erfahren wollen, gehen Sie einfach zu `https://rubrik.com/en/products/cloud-data-management`.

IN DIESEM KAPITEL

- Datenwachstum und unkontrollierte Datenausbreitung
- Sicherung und Wiederherstellung
- Datenschutzverletzungen und Ransomware
- Einhaltung gesetzlicher Vorgaben

Kapitel 1
Warum Unternehmen Cloud Data Management benötigen

Unternehmensdaten befinden sich heutzutage an vielen unterschiedlichen Orten. Moderne IT-Abteilungen benötigen innovative Lösungen zur Verwaltung dieser geschäftskritischen Unternehmensressourcen, um den größtmöglichen geschäftlichen Nutzen aus ihnen zu ziehen.

In diesem Kapitel wird beleuchtet, welche Herausforderungen das Datenwachstum und die unkontrollierte Datenausbreitung für Unternehmen mit sich bringen und warum sie robuste Datensicherungs-, Sicherheits- und Compliance-Funktionen benötigen.

Datenwachstum und unkontrollierte Datenausbreitung

Die moderne digitale Wirtschaft ist datengesteuert. Sie ist von Daten abhängig, die aus vielfältigen Quellen stammen und für die unterschiedlichsten Zwecke bearbeitet, gespeichert und analysiert werden. Der Aufstieg des Cloud Computing löste eine wahre Datenexplosion aus. Speicherkapazität war plötzlich eine nahezu unbegrenzte Ressource, die Cloud-Kunden auf Abruf zur Verfügung stand.

Neben dem Datenwachstum ist die unkontrollierte Datenausbreitung zu einer zunehmenden Herausforderung für Unternehmen geworden, denen es an starker Governance und angemessenen technischen Kontrollfunktionen zur Richtliniendurchsetzung mangelt. Viele Unternehmen haben Schwierigkeiten bei der Verwaltung ihrer Daten, die sich oft an unterschiedlichen Orten befinden, darunter:

- On-Premises-Rechenzentren und Private Clouds
- lokaler Speicher auf Desktop- und Laptop-Computern
- firmeneigene und private mobile Geräte
- Public Clouds wie Amazon Web Services (AWS), Google Cloud Platform (GCP) und Microsoft Azure
- SaaS-Geschäftsanwendungen (Software-as-a-Service) wie Asana, Microsoft 365, Salesforce und ServiceNow
- File-Sharing-Services wie Box, Dropbox und OneDrive

TIPP

Aus einer aktuellen IDC-Studie geht hervor, dass über 80 Prozent der IT-Führungskräfte die unkontrollierte Datenausbreitung als ernstes Problem erachten. Bei einer durchschnittlichen jährlichen Wachstumsrate (CAGR) von 46 Prozent wird sich das Datenvolumen alle zwei Jahre mehr als verdoppeln.

Datensicherung

Die Notwendigkeit, Daten zu schützen, wiederherzustellen und zu archivieren, besteht nach wie vor, doch veraltete Backup- und Recovery-Infrastrukturen – denen eine komplexe, mehrstufige Architektur zugrunde liegt – sind einfach nicht mehr in der Lage, zukunftsorientierte Geschäfts- und IT-Initiativen zu unterstützen. Ihre Verwaltung ist zeitaufwändig, sie sind schwer zu skalieren und ihre Wartung ist oft sehr kostspielig. Hinzu kommt, dass es schwierig, wenn nicht gar unmöglich ist, einen neuen Cloud-Anbieter oder eine neue Cloud-Anwendung zu diesem Szenario hinzuzufügen.

IT-Abteilungen brauchen eine Lösung zur Beseitigung dieser Engpässe, die eine benutzerfreundliche Software verwendet und die überall – vor Ort und in der Cloud – eingesetzt werden kann, damit sie ihren strategischen Projekte mehr Zeit widmen können.

Datensicherheit

Da datengesteuerte Geschäftsmodelle in der digitalen Wirtschaft immer größere Verbreitung finden, sind Daten zu einem lukrativen Ziel für Cyberkriminelle geworden. Trotz robuster Sicherheitsmechanismen

nimmt die Zahl erfolgreicher Datenschutzverletzungen und Ransomware-Angriffe weiter zu. Laut dem *Risk-Based Security Data Breach Quick-View Report* (`https://riskbasedsecurity.com`) wurden im Jahr 2020 mehr als 37 Milliarden Datensätze kompromittiert. Dem *McAfee Labs Threats Report* (`https://mcafee.com`) zufolge blieb die Anzahl der Ransomware-Angriffe in der ersten Hälfte desselben Jahres konstant.

Effektive Datensicherheit erfordert die Verschlüsselung von Daten sowohl im Ruhezustand als auch während der Übertragung sowie eine sichere Schlüsselverwaltung. Ebenso wichtig ist die Fähigkeit, sich schnell von Ereignissen wie Systemausfällen, Datenverletzungen oder Ransomware-Angriffen zu erholen.


TIPP

Verschlüsselung ist ein wichtiger Bestandteil einer weitergefassten Defense-in-Depth-Strategie. Sie trägt dazu bei, die Vertraulichkeit und Integrität Ihrer Daten im Falle einer Sicherheitsverletzung aufrechtzuerhalten – solange Ihre Verschlüsselungscodes geschützt sind und nicht ebenfalls von Angreifern kompromittiert werden können. Viele Datensicherheitsvorschriften (auf die ich im nächsten Abschnitt eingehen werde) enthalten Safe-Harbor-Bestimmungen für Unternehmen, die ihre sensiblen Daten zum Schutz vor Datenverletzungen verschlüsseln.

Wenn Ihr Unternehmen einem Ransomware-Angriff zum Opfer fällt, haben Sie in der Regel nur zwei Möglichkeiten, Ihre Daten wiederzuerlangen:

- **Das Lösegeld zahlen** – wobei Sie sich auf das Wort der Erpresser verlassen müssen, dass Ihre Daten tatsächlich wiederhergestellt werden. Das Federal Bureau of Investigation (FBI) rät dringend davon ab.
- **Daten aus Backups wiederherstellen** – wobei Sie sich darauf verlassen müssen, dass Ihre Backups aktuell und zuverlässig sind und nicht ebenfalls durch Ransomware beschädigt oder gelöscht wurden.

Obwohl das FBI davon abrät, auf Lösegeldforderungen einzugehen, zahlen Unternehmen jedes Jahr mehr als 1 Milliarde US-Dollar an Ransomware-Kriminelle. Das Zahlen von Lösegeld ist offensichtlich keine wünschenswerte oder zuverlässige Wiederherstellungsoption. Warum zahlen dann so viele Unternehmen weiterhin Lösegeld? Weil die Wiederherstellung mühsam und zeitaufwändig sein kann – wenn man überhaupt gute Backups hat, um die Daten wiederherzustellen. Außerdem haben Unternehmen in der Regel keinen Überblick über das Ausmaß des Schadens und sind dadurch gezwungen, ihre gesamte Umgebung vollständig wiederherzustellen, anstatt nur die betroffenen Daten zu retten, was letztlich zu noch größeren Datenverlusten führt. Viele Ransomware-Angriffe zielen mittlerweile auch auf Backups ab, um Unternehmen

daran zu hindern, ihre Daten wiederherzustellen und dadurch die Zahlung eines Lösegelds zu vermeiden.

TIPP

Unternehmen sollten nicht gezwungen sein, sich zwischen der Zahlung eines Lösegelds und der zeitaufwändigen Wiederherstellung ihrer gesamten Umgebung aus Backups zu entscheiden – ein Prozess, der oft zu teuren Ausfallzeiten führt. Stattdessen sollten sie sich auf ihre Backups verlassen können, um eine schnelle Wiederherstellung mit einem möglichst geringen Datenverlust und finanziellen Auswirkungen zu erreichen. Die Erstellung und Prüfung eines effektiven Wiederherstellungsplans sollte für IT-Abteilungen höchste Priorität haben, bevor es zu einem Angriff kommt.

Daten-Compliance

Die Compliance Anforderungen werden immer komplexer. Weltweit erlassen Gesetzgeber auf allen Regierungsebenen neue Vorschriften für die Datensicherheit und- sicherung, die sich nicht selten widersprechen. Je nach Ihrer Branche (und den Ländern, in denen Sie tätig sind), unterliegen Sie möglicherweise einer oder mehreren der folgenden Vorschriften:

- Australian Privacy Principles
- California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)
- Datenschutz-Grundverordnung (DSGVO)
- Payment Card Industry Data Security Standard (PCI-DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- US Sarbanes Oxley (SOX) Act

Jede Vorschrift stellt unterschiedliche Anforderungen an Unternehmen, sei es in Bezug auf die Datensicherheit, den Datenschutz, die Aufbewahrung von Daten oder andere Aspekte der Datenverwaltung. Einige Vorschriften verlangen eindeutige Verschlüsselungsstufen, andere schreiben vor, welche Daten aufbewahrt werden dürfen und welche nicht oder wo sie gespeichert werden müssen bzw. nicht gespeichert werden dürfen. Backup- und Wiederherstellungssysteme unterliegen ebenso wie Ihre Produktionssysteme gesetzlichen Compliance-Anforderungen. Ihr Backup- und Wiederherstellungssystem muss daher die von Ihrem Unternehmen benötigten Sicherheits- und Compliance-Prozesse unterstützen können.

IN DIESEM KAPITEL

- **ein deklaratives Modell zur Vereinfachung des Datenmanagements**
- **Automatisierung des Datenlebenszyklus-Managements**
- **Abstimmung von Datenmanagement und Geschäftsprozessen**
- **schnellere Anwendungsentwicklung mit Infrastructure-as-Code**

Kapitel **2**

Das deklarative Modell des Datenlebenszyklus-Managements

In diesem Kapitel wird beleuchtet, wie ein deklaratives Modell und Automatisierung das Datenlebenszyklus-Management vereinfachen und zur Abstimmung des Datenmanagements mit bestehenden Prozessen beitragen kann. Außerdem erfahren Sie, wie Sie die geschäftliche Agilität Ihres Unternehmens durch Konfigurationsmanagement und Infrastructure-as-Code (IaC) erhöhen können.

Deklarative und imperative Modelle im Vergleich

Eine hohe Komplexität in der IT-Umgebung ist auf Dauer nicht tragbar. IT-Abteilungen müssen sich zunehmend auf IT-Generalisten verlassen, die über umfassende Fähigkeiten und Erfahrungen mit den unterschiedlichsten Verwaltungsaufgaben verfügen. Veraltete Strategien und Technologien für die Backup-Verwaltung, die sich auf imperative Skripttechniken stützen, beeinträchtigen nicht nur die geschäftliche Agilität. Ihre Wartung ist auch sehr kostspielig und unzuverlässig, was zu unnötigen Risiken führen kann.

Moderne Backup- und Wiederherstellungssysteme müssen einfach zu betreiben und zu verwalten sein und sollten ein deklaratives Managementmodell verwenden. Bei einem deklarativen Managementmodell gibt ein Administrator den gewünschten Zustand für einen Workload in eine Richtlinien-Engine ein. Nachdem eine Richtlinie festgelegt wurde, führt das System automatisch und auf intelligente Weise die Aufgaben aus, die zum Erreichen dieses Zustands erforderlich sind (siehe Abbildung 2-1).

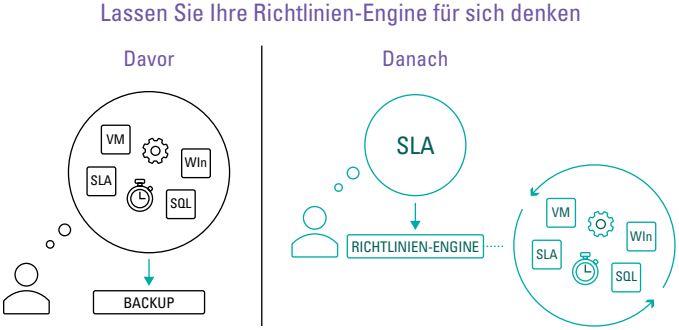

ABBILDUNG 2-1: Mit SLA-Richtlinien können Sie mehrere manuell implementierte Einstellungen zu einer einzigen einfach konfigurierbaren und wartungsfreien Richtlinie zusammenfassen.

Der Unterschied zwischen einem deklarativen und einem imperativen Modelle lässt sich vielleicht am besten durch den folgenden Vergleich erklären: Wenn Sie heute ein Paket versenden wollen, stellen Sie wahrscheinlich einige grundlegende Informationen zur Verfügung, darunter die Zieladresse, Ihre Rücksendeadresse und wie schnell Sie Ihr Paket zugestellt haben möchten. Der Kurier kümmert sich um den Rest. Dies ist ein deklaratives Modell. Bei einem imperativen Modell müssen Sie ebenfalls eine Zieladresse, eine Rücksendeadresse und einen Zeitrahmen für die Zustellung angeben. Sie sind aber auch dafür verantwortlich, das Paket zu verpacken, die Route von Ihrer Adresse zum Zielort festzulegen und die Lastwagen, Züge und Flugzeuge zu bestimmen, die verwendet werden, um Ihr Paket zum Zielort zu bringen – und das sind nur einige der Faktoren. Wie Sie sehen, ist ein imperatives Modell weitaus komplexer als ein deklaratives Modell und erfordert umfassende Kenntnisse, über die die meisten von uns nicht verfügen.

Automatisierung von Lebenszyklus-Aufgaben

Eine starke Richtlinien-Engine in einer Cloud-Data-Management-Lösung kann unterschiedliche Aspekte des Datenlebenszyklus-Managements erleichtern. Durch Service-Automatisierung kann eine

Richtlinien-Engine dazu beitragen, die Anzahl der manuellen Schritte zu reduzieren, die ein IT-Administrator regelmäßig durchführen muss, um eine bestimmte Aufgabe zu erledigen. Hier sind einige Beispiele für häufig anfallende Aufgaben des Datenlebenszyklus-Managements, die automatisiert werden könnten:

- **Replikation:** Möglicherweise müssen mehrere Datenkopien an unterschiedlichen Standorten oder in der Cloud repliziert werden, z. B. für Disaster-Recovery-Zwecke. Durch die Automatisierung der Datenreplikation wird die höchstmögliche Genauigkeit und Konsistenz dieser kritischen Prozesse sichergestellt.
- **Archivierung:** Im Rahmen der internen Governance oder für rechtliche und regulatorische Zwecke kann es erforderlich sein, Daten langfristig zu archivieren. Diese Archive können je nach Art und Alter der Daten automatisiert werden, damit die Daten bei Bedarf verfügbar und leicht durchsuchbar sind.
- **Konsolidierung:** Datendeduplizierung hilft Unternehmen bei der Verwaltung ihres Datenvolumens und ihrer Speicherkapazität, da alle redundanten Daten aus dem digitalen Bestand des Unternehmens eliminiert werden.
- **Verfall von Daten:** Durch die Automatisierung wird sichergestellt, dass Daten, die nicht mehr benötigt oder von Nutzen sind, archiviert oder vernichtet werden. Effiziente Datenablaufprozesse tragen dazu bei, Ihr Datenvolumen zu reduzieren und das Risiko einer Datenschutzverletzung oder eines Verstoßes gegen gesetzliche Vorschriften zu begrenzen.

Durch eine Architektur mit offener API (Application Programming Interface) können Unternehmen Backup- und Recovery-Prozesse in einen IT-Servicekatalog integrieren (z. B. ServiceNow, VMware vRealize Automation oder VMware Cloud Director), die Verwaltung großer verteilter Umgebungen über Konfigurationsmanagement- oder IaC-Tools vereinfachen (z. B. Puppet, Chef, SaltStack und Ansible) und Lebenszyklus-Workflows für das Datenmanagement und die Zentralisierung der Überwachung und Berichterstattung automatisieren (z. B. Splunk oder ein benutzerdefiniertes Monitoring-Dashboard).

Darüber hinaus ermöglicht die Automatisierung eine regelmäßige Backup-Validierung – was notwendig ist, um das Risiko einer „Testlücke“ zu reduzieren (siehe Abbildung 2-2).

MERKEN

Wenn Backups nicht regelmäßig getestet werden, können Sie nicht garantieren, dass sie vollständig und wiederherstellbar sind.

ABBILDUNG 2-2: Ohne regelmäßige Tests kann keine zuverlässige Wiederherstellung gewährleistet werden.

Datenmanagement auf bestehende Geschäftsprozesse abstimmen

Viele Geschäftsprozesse hängen von einem effizienten Datenmanagement ab. Mit einer modernen Cloud-Data-Management-Lösung können Sie sicherstellen, dass Ihre Datenmanagement-Funktionen auf die Unterstützung dieser Geschäftsprozesse abgestimmt sind.

Zur Wiederherstellung verlorener oder gelöschter Dateien und beschädigter Datenbankeinträge können z. B. kundenorientierte Service-Level-Agreements (SLAs) in interne Operational-Level-Agreements (OLAs) integriert werden.

Regulatorische Anforderungen, wie die Datenschutz-Grundverordnung (DSGVO) und der California Consumer Privacy Act (CCPA), schreiben vor, dass Unternehmen Kopien aller ihrer privaten Daten über eine betroffene Person (in einem gängigen übertragbaren Format) zur Verfügung stellen, wenn dies von der betroffenen Person verlangt wird. Diesen Anträgen betroffener Personen muss innerhalb festgelegter Fristen Folge geleistet werden, um die geltenden Compliance-Anforderungen zu erfüllen.

Jedes Unternehmen sollte über Business-Continuity- und Disaster-Recovery-Pläne mit klar definierten Recovery Time Objectives (RTOs) und Recovery Point Objectives (RPOs) verfügen, die auf der Geschäftskritikalität bestimmter Systeme und Daten basieren.

Viele Unternehmen müssen bestimmte Ressourcen auch für Verrechnungs-, Sicherheits- und andere Zwecke mit Tags versehen.

Konfigurationsmanagement und Infrastructure-as-Code (IaC)

Agile DevOps-Teams nutzen IaC, um virtuelle Maschinen, Datenbanken, Speicher und andere Infrastrukturressourcen für ihre Entwicklungs- und Testumgebungen schnell zu instanziieren. Automatisierungstools wie Ansible, Terraform, Puppet und SaltStack sind für das schnelle Einrichten, Konfigurieren und Aktualisieren von Infrastruktur und Daten in Continuous-Integration- (CI) und Continuous-Delivery-Pipelines (CD) unerlässlich.

Mithilfe einer modernen Cloud-Data-Management-Plattform können Sie DevOps-Teams unterstützen und Ihre Infrastruktur und Daten vereinfachen – in nur wenigen Codezeilen. IaC kann auch das Konfigurationsmanagement für mehrere Releases vereinfachen, wobei alle Änderungen im Code dokumentiert werden.

IN DIESEM KAPITEL

- Verschlüsselung von Daten bei der Übertragung und im Ruhezustand
- Implementierung eines Zero-Trust-Sicherheitsmodells
- Erkennung von Ransomware und Wiederherstellung

Kapitel 3
Mehrschichtige Datensicherheit

In diesem Kapitel lernen Sie die wichtigsten Funktionen kennen, auf die Sie bei einer für mehrschichtige Datensicherheit ausgelegten Cloud-Data-Management-Plattform achten sollten.

Flächendeckende Verschlüsselung

Im Jahr 2014 forcierte Google mit der Initiative „HTTPS Everywhere" die Nutzung von Hypertext Transfer Protocol überall im Internet und begann, das Protokoll als Ranking-Signal für Websites in seinen Suchalgorithmen zu verwenden. Da HTTPS den Webverkehr verschlüsselt, forderte Google also im Grunde, dass Daten bei der Übertragung überall verschlüsselt werden sollten. Mit HTTPS ist das Risiko geringer, dass Daten während der Übertragung durch böswillige Akteure ausgespäht oder verändert werden können. Unternehmen müssen diese „flächendeckende Verschlüsselung" auf ihre Produktions- und Backup-Daten im Ruhezustand in ihren On-Premises-Rechenzentren, SaaS-Anwendungen (Software-as-a-Service) und die Cloud ausweiten.

Die sichere Schlüsselverwaltung ist ein wichtiger, doch oft übersehener Aspekt der Verschlüsselung. Ein Verschlüsselungscode ist wie ein Passwort. Es spielt keine Rolle, wie komplex er ist, wenn ein Angreifer ihn entdecken kann (und Ihre Daten beschädigt) oder wenn Sie ihn vergessen (und nicht mehr auf Ihre Daten zugreifen können). Eine

sichere Schlüsselverwaltung ist während des gesamten Lebenszyklus von Schlüsseln unerlässlich und umfasst folgende Prozesse:

- Schlüsselerstellung
- Schlüsselspeicherung
- Schlüsselaktivierung
- Schlüsselverteilung
- Schlüsselrotation
- Schlüsselverfall
- Schlüsselentzug
- Schlüsselvernichtung


TECHNISCHES

Das Kerckhoffs'sche Prinzip besagt im Wesentlichen, dass die Sicherheit jedes Kryptosystems auf der Geheimhaltung der Schlüssel beruht und nicht auf der Geheimhaltung des Verschlüsselungsalgorithmus.


MERKEN

Ein mehrschichtiges Sicherheitssystem sorgt nicht nur für die Verschlüsselung der Daten im Ruhezustand und während der Übertragung, sondern auch für eine flexible interne oder externe Schlüsselverwaltung (über einen TPM-Chip (bzw. Key Management Interoperability Protocol, kurz KMIP).

Zero-Trust-Cluster-Design

Das Zero-Trust-Sicherheitskonzept basiert auf dem Prinzip „Vertrauen ist gut, Kontrolle ist besser". Die Speichercluster einer Cloud-Data-Management-Plattform sollten Zero Trust durch die folgenden Funktionen implementieren:

- **Multi-Faktor-Authentifizierung (MFA)** für ein starkes Identitäts- und Zugriffsmanagement (IAM) durch einen einmaligen Passcode, ein Hardware-Token oder einen biometrischen Identifikator, die neben einem Benutzernamen und einem Passwort erforderlich sind.
- **Rollenbasierte Zugriffskontrolle (RBAC)** zur Definition granularer Berechtigungen für authentifizierte Benutzer nach dem Prinzip der geringsten Rechte.
- **Authentifizierte API-Tokens**, die starke, randomisierte Passwörter verwenden, um verschlüsselte Daten zu und von Protection Clients zu übertragen.

Erkennung von Anomalien/Ransomware und Wiederherstellung

In den letzten Jahren hat die Zahl der Ransomware-Angriffe erheblich zugenommen. Die Attacken werden immer ausgeklügelter und kosten Unternehmen jedes Jahr viele Milliarden Euro. Ransomware-as-a-Service (RaaS) ist ein beunruhigender und wachsender Trend, der es jedem Möchtegern-Kriminellen ermöglicht, gegen eine geringe Lizenzgebühr oder Provision ein komplettes Ransomware-Paket im Dark Web zu erwerben und Personen oder Unternehmen anzugreifen.

HINWEIS

Mit Ransomware wird verhindert, dass autorisierte Benutzer auf ihre Systeme und Daten zugreifen können. Die Schadsoftware verschlüsselt und/oder löscht jedoch nicht nur die Originaldaten, sondern oft auch deren Backups.

Natürlich ist es am besten, Ransomware-Angriffe von vornherein zu verhindern, doch das ist leider nicht immer möglich. Wenn die Prävention fehlschlägt, ist es entscheidend, einen Angriff schnell zu erkennen, die betroffenen Daten zu identifizieren und ein unveränderliches Backup zu haben, das selbst nicht kompromittiert werden kann, um die Daten wiederherzustellen.

Laut dem *Verizon Data Breach Investigations Report* (DBIR) aus dem Jahr 2020 dauerte es bei etwa 20 Prozent der Sicherheitsverletzungen mehrere Monate bis zu ihrer Entdeckung. Der Angriff auf SolarWinds beispielsweise, der im Dezember 2020 bemerkt wurde, soll bereits im März 2020 begonnen haben. Eine verspätete Entdeckung wirkt sich direkt auf die Kosten und die Reichweite eines Angriffs aus und kann auch die Integrität von Backups beeinträchtigen. Die Fähigkeit, die durch Ransomware verschlüsselten Daten auf intelligente Weise zu identifizieren, erleichtert die Wiederherstellung, reduziert die Wiederherstellungszeit und -kosten und minimiert den Datenverlust. Backups enthalten umfangreiche Metadaten, die analysiert werden können, um anomale Aktivitäten zu erkennen und Warnmeldungen zu generieren. Auf diese Weise können Echtzeit-Erkennungs- und Präventions-Tools effektiv ergänzt werden. Modelle für maschinelles Lernen können dabei helfen, Sicherheitsbedrohungen durch tiefgreifende Analysen von Dateisystemen und Inhaltsverhalten zu erkennen.

Bei der Wiederherstellung nach einem Ransomware-Angriff sind Geschwindigkeit und Präzision von entscheidender Bedeutung. Unternehmen müssen in der Lage sein, kompromittierte Daten zu identifizieren und sie schnell und einfach in den zuletzt bekannten Zustand zurückversetzen. Eine moderne Cloud-Data-Management-Plattform

kann kompromittierte Daten auf intelligente Weise identifizieren und dem Incident-Response-Team Möglichkeiten zur Wiederherstellung bieten. Da nur die betroffenen Daten wiederhergestellt werden, bleiben die nicht betroffenen Daten auf demselben System erhalten, wodurch ein zusätzlicher Datenverlust durch eine vollständige Systemwiederherstellung vermieden wird.

TIPP

Um einen wirksamen Schutz vor Ransomware zu gewährleisten, implementieren die besten Anbieter von Backup- und Wiederherstellungslösungen von vornherein starke Sicherheitskontrollen. Die folgenden technische Anforderungen sollten bei der Bewertung der zugrunde liegenden Architektur einer Backup- und Wiederherstellungslösung berücksichtigt werden:

- Der Zugriff auf das Dateisystem zur Durchführung von Lese-/Schreibvorgängen ist jederzeit nur für den Anbieter und niemals für einen externen Client möglich.
- Die Lösung stellt keine Standard-Speicherprotokolle wie Network File System (NFS) oder Server Message Block (SMB) für die Interaktion mit den gesicherten Daten zur Verfügung.
- Der Anbieter speichert die Daten nicht in seinem eigenen Format, wodurch ein einfacher Zugriff auf die Sicherungsdaten bzw. deren Änderung möglich ist.
- Der Anbieter führt Backup-Validierungskontrollen durch, um sicherzustellen, dass die Sicherungsdaten niemals verändert werden. So wird genau das wiederhergestellt, was in der Originalkopie enthalten war.
- Das Dateisystem ist auf Unveränderlichkeit ausgelegt und erfordert keine Konfiguration oder Verwaltung durch den Benutzer.

IN DIESEM KAPITEL

- Katalogisierung, Verwaltung und Wiederherstellung von Backup-Daten
- Beschleunigung der Wiederherstellungszeiten
- Erreichen von Wiederherstellungszielen (RPOs) nahe Null
- Archivierung von Daten in der Cloud

Kapitel 4
Daten auf Abruf verfügbar machen

Ausfallzeiten haben heute viel weitreichendere Auswirkungen als in der Vergangenheit. Sie beeinträchtigen nicht nur die Geschäftsprozesse, sondern auch die Kundenzufriedenheit und den Ruf des Unternehmens. Es gibt mehr Daten als je zuvor, die sich an vielen unterschiedlichen Orten befinden. Alle diese Daten müssen verwaltet und geschützt werden. In diesem Kapitel betrachten wir die wichtigsten Funktionen, die Sie benötigen, um Ihre Daten bei Bedarf sofort verfügbar zu machen.

Indizierte, verwaltete und wiederherstellbare Daten

Unternehmen müssen heute enorme Datenmengen sichern. Dazu benötigen sie eine moderne Backup- und Wiederherstellungslösung, mit der es möglich ist, Daten schnell und genau zu indizieren. Diese Lösung muss über effektive Verwaltungsfunktionen verfügen und in der Lage sein, wichtige Geschäftsdaten über ihren gesamten Lebenszyklus hinweg wiederherzustellen.

Durch eine schnelle und genaue Indizierung wird sichergestellt, dass die richtigen Daten schnell gefunden werden, wenn eine Wiederherstellung

durchgeführt werden muss. Dazu ist eine intelligente Protokollverwaltung und eine umfassende Metadaten-Analyse erforderlich. Zu den effektiven Verwaltungsfunktionen sollte ein richtlinienbasiertes Datenmanagement gehören, damit Administratoren Bare-Metal-Servern, virtuellen Maschinen (VMs), Anwendungen, Datenbanken und Daten mithilfe eines einfachen und intuitiven deklarativen Modells Richtlinien für Service Level Agreements (SLAs) zuweisen können (siehe Kapitel 2).). Die Lösung sollte in der Lage sein, Daten zu suchen, die in der Cloud archiviert sind, und nur die benötigten Daten wiederherzustellen, ohne dass ganze Workloads neu instanziiert werden müssen, um eine einzige Datei zurückzugewinnen. Dadurch kann die Zahlung der von vielen Cloud-Anbietern geforderten Datenrückholkosten vermieden werden.

Sofortige Wiederherstellung ohne Rehydrierung

Die Datenrehydrierung ist ein zeitaufwändiger Prozess, der bei herkömmlichen Backup- und Recovery-Lösungen jedoch nicht zu umgehen ist. Bei der Datenrehydrierung muss ein Backup zunächst dekomprimiert, dedupliziert und dann auf einem Übertragungsmedium entschlüsselt werden, bevor die gewünschten Daten identifiziert und in einem nutzbaren Zustand am richtigen Ort wiederhergestellt werden können. Dieser Prozess macht es für IT-Abteilungen schwierig, Recovery Time Objectives (RTOs) einzuhalten, und erhöht gleichzeitig die Ausfallzeiten.

Mit einer modernen Cloud-Data-Management-Lösung können RTO nahe Null erreicht werden, da alle Daten – einschließlich VMs, Anwendungen und Datenbanken – direkt auf die Plattform gemountet werden können, anstatt sie erst in einer Produktionsumgebung zu rehydrieren.

Continuous Data Protection

Continuous Data Protection (CDP), auch bekannt als kontinuierliches Backup, ermöglicht einen kontinuierlichen Echtzeitstrom von Wiederherstellungspunkten, um den Datenverlust bei einem Ausfall oder Ransomware-Angriff zu minimieren. Da alle Änderungen oder Schreibvorgänge für einen bestimmten Zeitraum in einer Journaldatei gespeichert werden, können mit CDP Wiederherstellungspunkte (RPO) nahe Null erreicht werden. Bei einem herkömmlichen auf Snapshots basierenden Ansatz hingegen werden weniger Wiederherstellungsziele erreicht – je nachdem, wie oft Snapshots erstellt werden (z. B. alle 4 Stunden).

CDP ist jedoch keine für alle Workloads geeignete Technologie. Um entscheiden zu können, wo CDP in einer Umgebung eingesetzt werden sollte, müssen Sie die Vor- und Nachteile der Technologie kennen. Einige Vorteile von CDP sind:

- Es gibt praktisch keinen Datenverlust
- Daten können von ab jedem beliebigen Zeitpunkt wiederhergestellt werden.
- Daten können innerhalb von Sekunden wiederhergestellt werden

CDP hat jedoch auch einige Nachteile:

- Der Netzwerkverkehr nimmt zu
- Es kann die Leistung der geschützten Anwendung beeinträchtigen
- Der Speicherbedarf für Sicherungsdaten kann sich schnell erhöhen

Nutzung der Cloud zur langfristigen Datenarchivierung

Unternehmen nutzen zunehmend Cloud-Speicher, um ihre langfristigen Archivierungsanforderungen in der Zentrale, in Zweigstellen und an Remote-Standorten zu erfüllen. Die Cloud bietet praktisch unbegrenzte Kapazität und Skalierbarkeit, einfachen Zugriff auf Daten und unterschiedliche Optionen hinsichtlich der Leistung und Zuverlässigkeit – und das alles zu Preisen, die immer günstiger werden.

Allerdings bietet jede Cloud unterschiedliche Speicherebenen, Programmierschnittstellen (APIs) und Kostenmodelle, die der Kunde nicht nur verstehen, sondern an die er sich auch so gut wie möglich anpassen muss. Es ist wichtig, eine Langzeitarchivierungslösung zu finden, die mit allen wichtigen Cloud-Anbietern funktioniert, damit Sie nicht noch mehr Silos und mehr Komplexität in Ihre hybride Multi-Cloud-Umgebung bringen. Außerdem ist es teuer, Daten aus einem Cloud-Archiv wiederherzustellen (aufgrund der Datenrückholgebühren des Cloud-Anbieters). Mit Metadaten und Indizierung können Sie genau bestimmen, welche Daten sich in Ihren Archiven befinden sollen, und nur jene Daten wiederherstellen, die Sie tatsächlich benötigen. Dadurch werden Ihre Kosten erheblich reduziert.

VERLAGERUNG VON NETWORK-ATTACHED STORAGE (NAS) IN DIE CLOUD

In den letzten beiden Jahrzehnten sind NAS-Dateisysteme in vielen Branchen auf Petabyte-Größe angewachsen. Bei den zu speichernden Dateitypen und Anwendungsfällen handelt es heute bei weitem nicht mehr nur um allgemeine Bürodateien und Hauptverzeichnisse. NAS-Dateisysteme speichern entweder sehr große Multimedia-Dateien wie 4K-Videos oder Milliarden kleiner Dateien wie Bilder von Bankschecks oder IoT-Sensordaten (Internet of Things). Jeder Dateityp oder jeder Workload hat dabei oft ein anderes Leistungs- oder Speicherprofil. Die Sicherung auf NAS ist daher für Unternehmen nicht unproblematisch.

Die schiere Größe von NAS und die Vielfalt der Inhaltsprofile machen die Datensicherung für Backup-Administratoren sehr schwierig. Da alle Enterprise-NAS-Systeme über proprietäre Dateisysteme verfügen und in der Regel Appliance-basiert sind, ist es meist nicht möglich, einen Sicherungsagenten zu installieren, wie man es bei einem herkömmlichen Dateiserver mit Windows, Linux oder Unix tun würde.

Der De-facto-Ansatz zur Sicherung von NAS-Daten – das Network Data Management Protocol (NDMP) – ist nicht effizient genug, um große NAS-Umgebungen zu schützen. NDMP wurde vor über als 20 Jahren konzipiert und entwickelt, als Datenmengen noch wesentlich kleiner waren als die Workloads von heute und als der langfristige primäre Speicherort für Sicherungsdaten noch ein Bandlaufwerk war. Außerdem ist NDMP nur ein Steuerungsprotokoll und schreibt das Format der Daten nicht vor; daher sendet jeder Datensicherungsanbieter den Backup-Datenstrom in seinem eigenen Format.

NDMP erfordert außerdem regelmäßige Voll-Backups. Andernfalls kann die Wiederherstellungskette aus großen Sequenzen inkrementeller Backups die RTOs auf ein inakzeptables Niveau bringen. Außerdem ist NDMP hinsichtlich seiner Performance nur für die Unterstützung von Single-Stream-Backups ausgelegt, was zu Engpässen während des Übertragungsprozesses führen kann, die bei einer modernen Scale-Out-Architektur nicht auftreten.

Eine moderne Cloud-Data-Management-Lösung muss NAS-Daten zuverlässig schützen und bei Datenbeschädigung und Datenverlust eine schnelle Wiederherstellung ermöglichen, ohne sich auf komplexe NDMP-Implementierungen zu stützen. Sie sollte NAS-Sicherungsdaten direkt an einem Archivspeicherort speichern, globale Suchfunktionen bieten und eine schnelle Wiederherstellung ermöglichen. Außerdem muss sie unterschiedliche Speicherdienste wie Amazon Simple Storage Service (S3), Microsoft Azure Blob Storage und Google Cloud Storage sowie Private-Cloud-Objektspeicherlösungen (wie NetApp StorageGRID) und lokale NFS-Speicher unterstützen.

IN DIESEM KAPITEL

- **Selbstverwaltung von Daten durch Anwender**
- **Zugriff und Schutz von Testumgebungen und Remote-Standorten**
- **Erkennung und Klassifizierung sensibler Daten**
- **Schnelle Wiederherstellung zum Schutz vor Ransomware**
- **Vereinfachung des Datenmanagements in der Hybrid- und Multicloud**

Kapitel 5
Erweiterbares Datenmanagement eröffnet neue Anwendungsfälle

In diesem Kapitel erfahren Sie, wie eine erweiterbare Datenmanagementlösung neue Geschäfts- und IT-Anwendungsfälle ermöglicht, darunter Datenmanagement in einer Self-Service-Umgebung, beschleunigte Anwendungsentwicklung, unternehmensweiter Datenschutz, automatisierte Erkennung und Klassifizierung sensibler Daten, zentralisierte Überwachung und Protokollierung, Schutz vor Ransomware und Datenmanagement in Hybrid-Cloud-Umgebungen.

Datenmanagement in einer Self-Service-Umgebung

Unternehmen suchen ständig nach neuen Möglichkeiten zur Nutzung von Automatisierungslösungen. Durch die Automatisierung von Routineaufgaben können Administratoren viel Zeit bei der Verwaltung

sparen, manuelle Fehler reduzieren und sich stärker auf strategische Projekte konzentrieren. Sicherungs- und Wiederherstellungslösungen sind jedoch häufig von zentralisierten IT-Automatisierungssuites wie ServiceNow isoliert. Oft geht beim Warten auf die Wiederherstellung einer Datei wertvolle Zeit verloren – während die Anfrage stunden- oder sogar tagelang unbearbeitet in der Warteschlange des IT-Helpdesks steckt.


TIPP

Durch die Integration der API (Application Programming Interface) mit ServiceNow (und anderen IT-Service-Management-Lösungen) können Unternehmen Helpdesk-Tickets eliminieren und eine Self-Service-Umgebung für Backups und Wiederherstellungen anbieten – und das alles über den Servicekatalog. So wird die Zeit bis zur Lösung eines Problems von Tagen auf Minuten reduziert, der Helpdesk kann sich um dringendere Serviceanfragen kümmern und Unternehmen erholen sich schnell von ungeplanten Störungen. Zu den wichtigsten Funktionen gehören:

- **Automatisierte Datensicherung:** Benutzer sollten in der Lage sein, Service-Level-Agreements (SLAs) direkt über die Benutzeroberfläche zuzuweisen oder zu ändern.
- **Dateiwiederherstellung als Self-Service-Funktion:** Eine prädiktive Suchfunktion auf Dateiebene ermöglicht es Anwendern, Dateien selbst zu finden und wiederherzustellen, wodurch die Wiederherstellungszeiten von Stunden oder Tagen auf wenige Minuten reduziert werden.

Test- und Entwicklungsumgebungen

Um die Anwendungsentwicklung zu beschleunigen, müssen DevOps-Teams in der Lage sein, schnell auf Daten in Entwicklungs- und Testumgebungen zuzugreifen. Mit Legacy-Lösungen sind Unternehmen nicht in der Lage, die schnellen Wiederherstellungsziele (RTO) zu erreichen, die ihre DevOps-Teams für VMs und Datenbanken benötigen. Kostspielige Verzögerungen bei Routineaufgaben wie der Wiederherstellung von Daten, dem Testen von Updates und der Erstellung neuer Tools beeinträchtigen die geschäftliche Agilität und erhöhen die Time-to-Market. Eine erweiterbare Datenmanagementlösung muss in der Lage sein, DevOps-Teams die benötigten Daten sofort zur Verfügung zu stellen. Benutzer sollten die Möglichkeit haben, einen einzigen „Golden Image"-Snapshot zu nutzen, um mehrere Klone direkt auf der Plattform zu mounten und sofort Klone für Test- und Entwicklungszwecke bereitzustellen, ohne Produktionsumgebungen zu rehydrieren.

Schutz von Daten an Remote-Standorten und in Zweigniederlassungen

IT-Administratoren benötigen eine einzige Lösung zum Schutz all ihrer Anwendungen und Daten am Hauptstandort sowie an Remote-Standorten und in Zweigniederlassungen, um die Kosten so gering wie möglich zu halten und die Komplexität zu reduzieren. Außerdem muss die Lösung Datenmanagementfunktionen auf virtuelle und physische Umgebungen ausweiten können. Mit einer einzigen Schnittstelle können Administratoren richtlinienbasiertes Datenmanagement, globale Suchfunktionen, schnelle Wiederherstellung und Compliance-Reporting vor Ort, am Edge und in der Cloud bereitstellen.

Automatisierte Erkennung und Klassifizierung sensibler Daten

Im Zeitalter der Cloud befinden sich sensible Daten an mehr Orten als je zuvor und können aufgrund dynamischer, verteilter Architekturen von mehr Personen eingesehen werden. Dadurch erhöht sich das Risiko von Datenschutzverletzungen und der Nichteinhaltung von Vorschriften, die oft Strafen nach sich ziehen. Unternehmen benötigen einheitliche Prozesse, die eine durchgängige Data Governance gewährleisten. Viele Firmen wenden jedoch zu viel Zeit und Geld für komplexe Klassifizierungs- und Compliance-Aufgaben wie manuelles Tagging, natives Auditing und jährlichen Bereinigungen auf. Automatisierung ist der Schlüssel für den effizienten und angemessenen Schutz sensibler Daten.

TIPP

Halten Sie nach einer Lösung Ausschau, die die Erkennung, Klassifizierung und den Schutz sensibler Daten automatisiert, um eine effiziente Data Governance zu gewährleisten. Diese Lösung sollte maschinelles Lernen anwenden, um Datenrisiken zu identifizieren, ohne die Produktionsumgebung zu beeinträchtigen. Vorgefertigte Vorlagen für Richtlinien zur Datenklassifizierung sollten Vorschriften und Standards wie die Datenschutz-Grundverordnung (DSGVO), Payment Card Industry (PCI), Data Security Standards (DSS), Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA) und California Consumer Privacy Act (CCPA) enthalten. Administratoren können auch ihre eigenen selbstdefinierten Wörterbücher, Ausdrücke und Richtlinien erstellen.

Integration von Services für die zentrale Überwachung und Protokollierung

Sie können das „Konsolen-Hopping“ eliminieren und dieselben Observability-Services zur Überwachung Ihrer Datenschutzlösung nutzen. Eine moderne Cloud-Data-Management-Lösung sollte eine einfache Integration mit gängigen Tools wie Nagios, Prometheus, Splunk, vRealize Log Insight ermöglichen, damit Sie die Überwachung, Protokollierung und Alarmierung mit denselben Tools verwalten können, die Sie bereits in Ihrer Umgebung einsetzen.

Mehrschichtige Ransomware-Abwehr

Die Fähigkeit, Ihre Daten schnell, präzise und vollständig wiederherzustellen, ist im Falle eines Ransomware-Angriffs entscheidend. Ransomware-Angriffe können weitreichende geschäftliche Auswirkungen haben, darunter Daten-, Umsatz- und Produktivitätsverluste. Es dauert oft mehrere Tage oder Wochen, bevor eine Ransomware-Infektion entdeckt wird und das Ausmaß des Schadens eingeschätzt werden kann. Dann dauert es weitere Stunden oder Tage, um die Daten in einem sauberen Zustand wiederherzustellen.

TIPP

Eine erweiterbare Datenmanagement-Plattform sollte die Defense-in-Depth-Sicherheitsstrategie des Unternehmens ergänzen und eine schnelle Datenwiederherstellung ermöglichen. Alle Daten sollten in einem unveränderlichen Format gespeichert werden, um zu verhindern, dass Ransomware die Backups verschlüsseln oder überschreiben kann. Im Falle eines Angriffs müssen Administratoren in der Lage sein, ihre Anwendungen und Daten einfach nach dem letzten sauberen Snapshot wiederherzustellen und den Betrieb schnell und mit minimaler Ausfallzeit wieder aufzunehmen. Suchen Sie nach einer Lösung, die nach einem Ransomware-Angriff eine schnelle und einfache Wiederherstellung ermöglicht. Sie sollte über die folgenden Funktionen verfügen:

- **Erkennung auf der Basis künstlicher Intelligenz (KI):** Mithilfe von maschinellem Lernen, das auf Anwendungs-Metadaten angewendet wird, können ungewöhnliche Aktivitäten identifiziert und Administratoren darauf aufmerksam gemacht werden.
- **Auswirkungsanalyse auf Dateiebene:** Administratoren können die Angriffsfläche schnell mit einfachen Visualisierungen untersuchen, die darstellen, welche Anwendungen und Dateien betroffen waren und wo sie sich befinden.

Wiederherstellung mit einem Klick: Administratoren können einfach alle betroffenen Anwendungen und Dateien auswählen, den gewünschten Wiederherstellungsort angeben und mit nur einem Klick die letzten sauberen Versionen wiederherstellen.

Zentralisiertes Datenmanagement in der Hybrid-Cloud

Unternehmen führen ständig neue Cloud-Initiativen ein. Für Administratoren wird es dadurch immer schwieriger, alle Anwendungen und Daten über mehrere Rechenzentren und Clouds hinweg zu überwachen und zu verwalten. Sie verbringen zu viel Zeit mit der Überwachung von Backups, der Fehlersuche und der Analyse von in Silos befindlichen Informationen und sind daher nicht in der Lage, schnell zu skalieren, um die Anforderungen des Unternehmens zu erfüllen.

TIPP

Halten Sie nach einer Datenmanagement-Plattform Ausschau, die eine einzige SaaS-basierte Verwaltungskonsole für die globale Verwaltung vor Ort, am Edge und in der Cloud bietet. Eine solche Lösung kann Unternehmen dabei helfen, ihre Betriebskosten senken und mehr Zeit für geschäftskritische Projekte freizusetzen. Eine solche Plattform sollte Folgendes enthalten:

- **Globaler Datenbestand** Administratoren arbeiten mit einem einzigen globalen Bestand von Objekten aus dem gesamten Unternehmen. Dies ermöglicht es ihnen, nach Objektnamen zu suchen, um Daten unabhängig vom Standort leicht zu finden, und bietet eine vollständige Transparenz und Kontrolle über alle Anwendungen und Daten.
- **Globale Überwachung und Berichterstattung:** Ein einziges, benutzerfreundliches Dashboard sollte globale Kennzahlen zur Einhaltung von SLAs, zum Zustand der Infrastruktur und zur Leistung liefern. Administratoren sollten in der Lage sein, dynamische Datenfilterungen für Ad-hoc-Analysen mit unterschiedlichen Parametern wie Zeit, Standort, Status und Anwendung durchzuführen.

Kapitel 6
Zehn wichtige Fähigkeiten einer modernen Cloud-Data-Management-Lösung

Auf die folgenden zehn Fähigkeiten sollten Sie bei der Suche nach einer modernen Cloud-Data-Management-Lösung für Ihr Unternehmen besonders achten:

- **Einfache Skalierung:** Administratoren müssen in der Lage sein, durch eine linear skalierbare Architektur, die auf Web-Scale-Technologien basiert, mit wachsenden Datenmengen umzugehen.
- **Schnelle Wiederherstellung:** Eine einfache und schnelle Wiederherstellung ist entscheidend, um Ausfallzeiten zu minimieren und sicherzustellen, dass Recovery Time Objectives (RTOs) und Service Level Agreements erfüllt werden können.
- **Automatisierung des Datenlebenszyklus:** Die Automatisierung routinemäßiger Lifecycle-Management-Aufgaben wie Replikation, Archivierung, Konsolidierung und Verfall ist entscheidend für die Steigerung der Effizienz, die Reduzierung der Kosten und die Vermeidung manueller Fehler.

- **Softwaredefiniert:** Eine moderne Cloud-Data-Management-Lösung muss softwaredefiniert sein, um die Konsolidierung unterschiedlicher Hardware- und Software-Komponenten in On-Premises- und Cloud-Umgebungen in einer einzigen Software-Fabric zu ermöglichen.
- **Cloud-Mobilität:** Eine moderne Cloud-Data-Management-Lösung ermöglicht Cloud- und Anwendungsmobilität. Sie muss in der Lage sein, lokale, hybride und Multi-Cloud-Umgebungen zu umfassen, ohne sich auf proprietäre Technologien verlassen zu müssen, die die geschäftliche Agilität und Flexibilität einschränken, da sie eine Herstellerbindung schaffen.
- **Umfassende Plattformunterstützung:** Eine moderne Backup- und Recovery-Lösung sollte Ihre IT-Umgebung unterstützen, optimieren und vorhandene Elemente integrieren, einschließlich physischer und virtueller Systeme, unterschiedlicher Datenbanken und Dateisysteme sowie hybrider Umgebungen, die aus On-Premises-, Public-Cloud- und Multi-Cloud-Elementen bestehen.
- **Erweiterbarkeit der Programmierschnittstelle (API):** APIs ermöglichen die Integration, Automatisierung, Sicherheit und Self-Service-Funktionen über ein breites Spektrum von Lösungen hinweg. Achten Sie auf branchenübliche OpenAPI-Dokumentation, Beispielcode und vorgefertigte Integrationen mit unterschiedlichen Automatisierungstools.
- **Mehrschichtige Sicherheit:** Die Verschlüsselung von Daten im Ruhezustand und bei der Übertragung, eine sichere und flexible Schlüsselverwaltung und ein Zero-Trust-Cluster-Design sind wichtige Elemente eines mehrschichtigen Sicherheitsansatzes.
- **Unveränderlichkeit und Wiederherstellung nach einem Ransomware-Angriff:** Eine kritischer Bestandteil einer Ransomware-Abwehrstrategie ist ein Backup- und Wiederherstellungssystem, das unveränderliche Backups erstellen kann – also Backups, die nicht durch Ransomware verändert werden können. Das System sollte außerdem auf einer Technologie basieren, die sich auf maschinelles Lernen stützt und die Anwendungs-Metadaten überwachen kann, um anomale Aktivitäten bzw. frühe Indikatoren für einen Ransomware-Angriff zu erkennen und Sie zu warnen.
- **Umfassende Unterstützung für innovative Anwendungsfälle:** Ihre Cloud-Data-Management-Lösung sollte innovative technische und geschäftliche Anwendungsfälle ermöglichen, darunter Self-Service-Funktionen für das Datenmanagement, beschleunigte Anwendungsentwicklung mit Infrastructure-as-Code, Schutz von Daten an Remote-Standorten und in Zweigniederlassungen und die automatisierte Erkennung und Klassifizierung von sensiblen Daten.

Sichern Sie Ihre Daten – ganz gleich, wo sie gespeichert sind

Daten sind eines der wertvollsten Güter Ihres Unternehmens. Ihre Daten sind wahrscheinlich an vielen unterschiedlichen Orten gespeichert – im On-Premises-Rechenzentrum, in SaaS-Anwendungen, in der Cloud, bei File-Sharing-Diensten und sogar auf den persönlichen Geräten Ihrer Mitarbeiter. Die Herausforderung besteht darin, all Ihre Daten optimal zu verwalten und zu sichern, damit sie für die richtigen Personen jederzeit verfügbar sein. *Cloud Data Management für Dummies* stellt Datenmanagement-Lösungen vor, die dafür sorgen, dass Ihre Daten jederzeit gesichert und geschützt sind.

In diesem Buch erfahren Sie...

- Mehrschichtige Datensicherheit
- Datenverfügbarkeit auf Abruf
- Ein deklaratives Modell des Datenlebenszyklus-Managements zur Vereinfachung Ihrer Daten
- Langzeitspeicherung in der Cloud
- Eine Self-Service-Umgebung für Backups
- Unterstützung neuer Anwendungsfälle

rubrik

Lawrence Miller diente als Chief Petty Officer in der US-Navy und ist seit über 25 Jahren in verschiedenen Branchen im Bereich Informationstechnologie tätig. Er ist Mitautor des Buches CISSP *Für Dummies* und hat über 200 weitere *Für-Dummies*-Bücher zu zahlreichen technischen und sicherheitsbezogenen Themen verfasst.

Besuchen Sie Dummies.com®
um sich Videos und schrittweise Bildanleitungen anzusehen oder Produkte zu kaufen!

ISBN: 978-1-119-84959-9

für dummies®

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.