Schnellere Realisierung von **Multicloud-Monitoring**

splunk>
turn data into doing™

Der Trend geht zu **Multi-Cloud**

Die Migration in die Cloud ist auf dem Vormarsch – und zwar so rasant, dass Gartner prognostiziert, dass 80% der Unternehmen bis 2025 komplett in die Cloud migriert sein werden und keinerlei lokale Infrastruktur mehr unterhalten. Die jüngste Entwicklung im Bereich Cloud Computing ist dabei der Trend zu Multicloud-Umgebungen. Bei dieser Strategie nutzt ein Unternehmen mindestens zwei Cloud-Services innerhalb einer Architektur – es werden also verschiedene Cloud-Stacks für unterschiedliche Aufgaben verwendet, z. B. die Google Cloud Platform für unternehmensinterne Anwendungen und Amazon Web Services (AWS) für kundenseitige Anwendungen. Dieser Ansatz ist sehr beliebt und wird derzeit von mehr als 80 % der Unternehmen verfolgt.

Eine Multicloud-Umgebung kann aus verschiedenen Arten von Cloud-Lösungen bestehen. Zu den öffentlichen Cloud-Services gehören AWS, Microsoft Azure, Google Cloud Platform und andere Cloud Computing-Services von Drittanbietern. Private Clouds beschränken den Zugang dagegen auf bestimmte Unternehmen. Services und Infrastruktur werden in einem privaten Netzwerk verwaltet, was im Vergleich zu öffentlichen Clouds mehr Sicherheit und Kontrolle bietet.

Verschiedene Stacks
für unterschiedliche Aufgaben

Warum Organisationen mehrere öffentliche Clouds nutzen

AWS für die Entwicklung
Microservices
Container
EC2, VMs, Speicherung

GCP für interne Services
G Suite, Workday, Salesforce

Azure für „Lift and Shift“-Aufgaben
Senkt Kosten
Disaster Recovery

Multicloud-Umgebungen verstehen

Es macht Sinn, zunächst die Begriffe „hybride Cloud“ und „Multi-Cloud“ zu definieren. Eine hybride Cloud-Lösung bedeutet, dass ein Unternehmen eine Mischung aus lokaler, öffentlicher und privater Cloud-Infrastruktur nutzt. Multi-Cloud besagt dagegen, dass Unternehmen mehrere Cloud-Anbieter für mehrere Cloud-Bereitstellungen desselben Typs verwenden, indem sie zum Beispiel öffentliche Clouds von zwei verschiedenen Anbietern nutzen. Unterschiedliche Teams haben unterschiedliche Anforderungen, so dass sie in der Regel den Cloud-Anbieter wählen, der ihre spezifischen Kriterien am besten erfüllt.

Worin liegt der Unterschied?

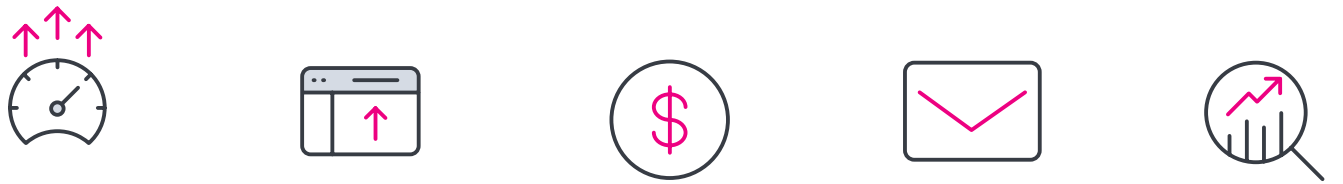
Multi-Cloud	Hybride Cloud
Workloads können ohne Interoperabilität zwischen Anbietern in Cloud-Plattformen verlagert werden	Workloads sind auf mehrere Cloud- und lokale Umgebungen verteilt – dies macht die Umgebung äußerst portabel und austauschbar
Beispiel: zwei öffentliche Clouds, AWS + Azure	**Beispiel:** eine öffentliche Cloud UND eine lokale, vom Kunden unterhaltene Rechenzentrums-infrastruktur

Welche Vorteile haben Unternehmen von einem Multicloud-Ansatz?

Performance-Optimierung: Falls eine primäre Cloud ausfällt oder Leistungsprobleme verzeichnet, kann eine passive Cloud als Ausweichlösung genutzt werden. Mit dieser Strategie können Ausfallzeiten reduziert oder verhindert werden, bis die primäre Cloud wieder online ist.

Kosteneinsparungen: Die Kombination aus erhöhter Zuverlässigkeit und optimierter Performance bedeutet Kosteneinsparungen für das Unternehmen. Ein Systemausfall bei einer Bank kann Umsatzeinbußen verursachen, während er bei einem Krankenhaus nicht nur zu Umsatzeinbußen, sondern auch zur Gefährdung von Menschenleben führen kann. Völlig unabhängig vom jeweiligen Anwendungsfall ist die Aufrechterhaltung des Netzwerkbetriebs entscheidend für den anhaltenden Unternehmenserfolg.

Flexibilität: Durch den Multicloud-Ansatz wird eine Anbieterbindung vermieden, bei der das Unternehmen von der Infrastruktur und den Services eines bestimmten Cloud-Providers abhängt und ein Anbieterwechsel eventuell mit erheblichen Kosten und Einschränkungen verbunden ist. Die Nutzung mehrerer Anbieter bietet Unternehmen zudem Möglichkeiten zur Performance-Optimierung, da sie Services so kombinieren können, dass ihre spezifischen Bedürfnisse erfüllt werden. Ein Unternehmen könnte beispielsweise Microsoft-Tools für einen Use Case einsetzen und Google oder AWS für einen anderen (z. B. Infrastruktur und Entwicklung).



Die größten Herausforderungen bei **Multicloud-Umgebungen**

Eine Multicloud-Strategie bietet zwar viele Vorteile, ist jedoch auch mit signifikanten Herausforderungen verbunden. Genau die Merkmale, die für mehr Flexibilität und Zuverlässigkeit sorgen, verursachen zusätzliche Sicherheitsrisiken und IT-Herausforderungen.

Sämtliche Herausforderungen, die IT-Teams beim Cloud Computing zu bewältigen haben, treten auch bei Multicloud-Umgebungen auf, und zwar in größerem Umfang. Dadurch wird es für die Teams schwieriger, kritische Probleme in der Cloud zu identifizieren, zu untersuchen und zu lösen. Mehr Services bedeuten mehr Komplexität, und Silo-Systeme erschweren ganzheitliches Monitoring erheblich.

Was die Sicherheit angeht, so zeigen aktuelle Studien, dass es einen Zusammenhang zwischen der Anzahl der genutzten Cloud-Services und der Wahrscheinlichkeit einer Sicherheitsverletzung gibt: Eine 2019 von Nominet durchgeführte Studie ergab, dass es bei 52 % der Multicloud-Umgebungen innerhalb des letzten Jahres zu einer Sicherheitsverletzung kam, während dies nur bei 24 % der Hybrid-Cloud-Systeme und 24 % der Single-Cloud-Nutzer der Fall war. Bei Multicloud-Umgebungen ist zudem die Wahrscheinlichkeit für das Auftreten mehrerer Sicherheitsverletzungen höher: 69 % der Unternehmen mit Multicloud-Umgebungen berichten von 11 bis 30 Sicherheitsverletzungen, wohingegen der Wert bei Single-Cloud-Systemen bei 19 % und bei Hybrid-Cloud-Umgebungen bei 13 % liegt.

Die Herausforderungen, die Multicloud-Umgebungen mit sich bringen, haben unterschiedliche Auswirkungen auf die IT- und Sicherheitsteams:

Mehrere Systeme führen zu Silobildung: Ein Multicloud-Ansatz kann die Sicherheit und Systemzuverlässigkeit verbessern, da Services auf mehrere Cloud-Lösungen verteilt sind. Ein solcher Ansatz kann aber auch Risiken bergen, da er es Unternehmen erschwert, Transparenz über alle ihre Hosts und Services hinweg zu erhalten.

Die Nutzung unterschiedlicher Cloud-Lösungen mit jeweils eigenen nativen Tools für Monitoring und IT-Sicherheit bedeutet, dass IT-Teams nicht effizient über den gesamten Stack hinweg feststellen können, ob Service-Verschlechterungen oder -Ausfälle auf einen bestimmten Service zurückzuführen sind oder das System wie beabsichtigt funktioniert.

Die herkömmlichen Grundlagen der Cybersicherheit sind auf Multicloud-Umgebungen nicht unbedingt anwendbar. Ein Unternehmen könnte mehrere Lösungen für das Monitoring seiner Cloud-Services einsetzen, dies macht Teams allerdings langsamer und verursacht Kosten, besonders wenn zeitkritische Probleme auftreten.

Höhere MTTR (Mean-Time-to-Resolution): Es kann IT- und Sicherheitsteams enorme Schwierigkeiten bereiten, einem Multicloud-System Informationen über einen Ausfall oder einen Sicherheitsverstoß abzuringen. Zudem kann dies das Unternehmen Zeit, Geld und die Zufriedenheit und das Vertrauen der Kunden kosten.

Durch die eingeschränkte Transparenz innerhalb des gesamten Stacks müssen Teams viel mehr Zeit aufwenden, um herauszufinden, wo und warum es zu Ausfällen kommt, da sie zwischen mehreren Monitoring-Systemen wechseln müssen, um sich durch Korrelieren und Analysieren von Event-Daten ein vollständiges Bild des Problems machen zu können. Da bei einem Service-Ausfall oder einem böswilligen Angriff jede Minute zählt, wirkt sich die zusätzliche Komplexität eines Multicloud-Systems direkt auf das Geschäftsergebnis aus.

Data Governance, Compliance und Verwundbarkeit der Infrastruktur: Zudem erschwert die mangelnde Transparenz über mehrere Stacks hinweg die Erfüllung von Compliance-Anforderungen und die Abwehr von Hackern, die in der verteilten Infrastruktur des Unternehmens leichter Schwachstellen finden und ausnutzen können. Jeder zusätzliche Cloud-Service erhöht die Zahl der Zugangspunkte eines Netzwerks.

Mangelnde Transparenz führt außerdem zu Problemen bei Data Governance und Compliance. Mehrere Clouds bieten zwar eventuell mehr Flexibilität, können sich aber in regulatorischer Hinsicht als schwierig erweisen. Es könnte beispielsweise passieren, dass ein Unternehmen eine Anwendung versehentlich in einer nicht genehmigten Umgebung ausführt und damit gegen die Bestimmungen der Datenschutz-Grundverordnung (DSGVO) verstößt. Verstöße gegen diese und andere Richtlinien können empfindliche Geldstrafen nach sich ziehen.

Monitoring mit unterschiedlichen **nativen Cloud-Tools führt zu:**

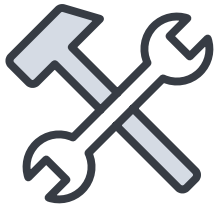
- **Silobildung bei Ansichten**
- **Silobildung bei Teams**
- **Silobildung bei Daten**

Für Teams ist es schwierig, kritische Probleme in der Cloud zu identifizieren, zu untersuchen und zu beheben.

Mangelnde Transparenz

Sie sehen nicht, ob Service-Verschlechterungen oder -Ausfälle tatsächlich von Cloud-Services verursacht werden.

Komplexe Tools



Bei der Nutzung mehrerer Cloud-Services ist es schwierig, eine einheitliche Monitoring-Strategie zu verfolgen.

Schlechte MTTR

Es ist zu zeitaufwendig festzustellen, wo und warum Ausfälle auftreten.

Skalierungsprobleme

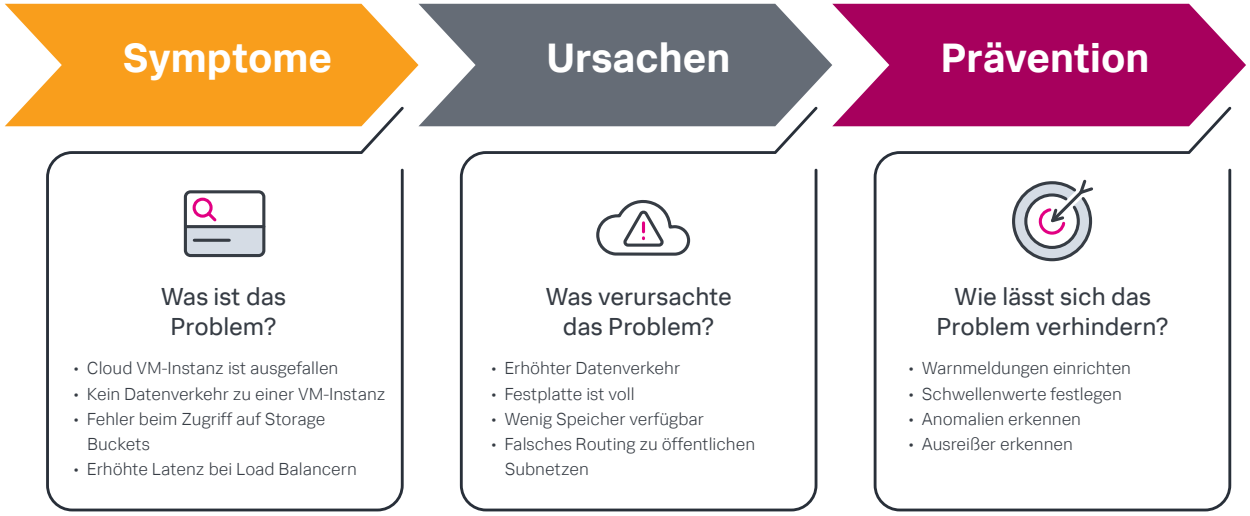
Es ist schwierig, Daten über mehrere Regionen, Accounts und Clouds hinweg zu erfassen.

So meistern Sie **Cloud-Monitoring**

Wie bekommen Unternehmen diese Herausforderungen nun in den Griff? Aufgrund des zunehmenden Umfangs und der wachsenden Komplexität von Cloud-Infrastrukturen wird es für Unternehmen entscheidend, über umfassende Monitoring-Lösungen und -Strategien zu verfügen, die Multicloud-Anforderungen und -Herausforderungen gerecht werden.

Da die Komplexität moderner IT-Infrastrukturen immer mehr zunimmt, ist eine zentralisierte Methode für Monitoring und Troubleshooting der gesamten Multicloud-Umgebung unerlässlich. Ohne die richtige Lösung wird es für moderne Unternehmen schwieriger, die Daten zu beobachten und auszuwerten, die sie für das Vorbeugung und Handeln von Ausfällen und Incidents benötigen. Unternehmen, die in moderne IT- und DevOps-Tools investieren, können positive Kundenerfahrungen schaffen und letztendlich Innovationen und Umsatz maximieren.

Schritte zur Verringerung von Monitoring-Problemen



Splunk Infrastructure **Investigation and Monitoring**

Cloud-Tools beinhalten oftmals eigene Tools und Services für Monitoring und Troubleshooting. In der Umgestaltung befindliche Unternehmen benötigen jedoch eine Lösung, die über mehrere Clouds und Services hinweg in Echtzeit funktioniert und eine vollständige Sicht und Plattform bereitstellt, von der aus Handlungen umgesetzt werden können.

Genau diese Anforderungen erfüllt Splunk Infrastructure Investigation and Monitoring (IIM). Es bietet eine konsolidierte Lösung für das Monitoring der gesamten Infrastruktur, die viele Monitoring- und Troubleshooting-Tools ersetzen kann. Werden für Monitoring und Fehlerbehebung zwei unterschiedliche Tools eingesetzt, kann dies die Komplexität unnötig erhöhen und Teams bei kritischen Problemen Zeit kosten. Wenn beide Funktionen mit derselben Lösung erledigt werden können, kann dies die Abläufe deutlich vereinfachen und die Ressourcenbelastung reduzieren. Außerdem werden dadurch Reibungsverluste bei der Datenbeschaffung verringert, da Daten von mehreren Cloud-Anbietern erfasst und in einer Ansicht präsentiert werden können. Dies ermöglicht Unternehmen, Betrieb, Sicherheit und Kosten ihrer verschiedenen Cloud-Umgebungen in Echtzeit im Blick zu behalten.

Splunk erreicht dies durch Echtzeit-Monitoring des gesamten Cloud-Stack und bietet den Benutzern damit Transparenz und Kontrolle durch die Nutzung sämtlicher Daten aus beliebigen Quellen, in beliebigem Maßstab, gekoppelt mit KI-gesteuerten Echtzeitanalysen. Sie erhalten so ein besseres Bild der Cloud-Infrastruktur, kürzere MTTD- und MTTR-Zeiten und die notwendige Flexibilität und Skalierbarkeit, um sich an das Unternehmenswachstum in jeder Phase seines Wegs in die Cloud anzupassen.

Erfahren Sie wie.

Das Monitoring von Multicloud-Umgebung kann sich schwierig gestalten. Unternehmen brauchen jedoch kein umfangreiches Arsenal an Tools, um über die Abläufe in ihren Cloud-Infrastrukturen auf dem Laufenden zu bleiben.

Überzeugen Sie sich selbst von den Möglichkeiten, die Splunk für Infrastructure Investigation und Monitoring bietet. Registrieren Sie sich für eine kostenlose Testversion von Splunk Infrastructure Monitoring.

Oder kontaktieren Sie uns unter sales@splunk.com, um zu erfahren, wie Sie Ihre Multicloud-Initiativen schnell und wirkungsvoll realisieren können.

20-132~1

splunk> turn data into doing™