DIE „DOS AND DON'TS" IN SACHEN HYBRID CLOUD

NUTANIX™
YOUR ENTERPRISE CLOUD

DIE WAHL ZWISCHEN EINER PRIVATE CLOUD UND EINER PUBLIC CLOUD IST FÜR VIELE IT-MANAGER EINE URALTE FRAGE – SOFERN SIE NOCH NIE VON EINER HYBRID CLOUD GEHÖRT HABEN

Aber der Übergang in das Hybridzeitalter beginnt mit einer soliden Grundlage vor Ort, und von dort aus erfordert der Aufbau Ihrer Hybrid Cloud sorgfältige Planung und langsame, wohlüberlegte Schritte.

Lesen Sie weiter für 7 der größten „Dos and Don'ts“, damit Ihre Hybrid-Cloud-Initiativen reibungslos umgesetzt werden können.


DO

Do #1

IMPLEMENTIEREN SIE ZUERST EINE LEISTUNGSFÄHIGE PRIVATE CLOUD

Der Trend zur Private Cloud ist schwer zu ignorieren. Laut **Forrester investieren 79% der IT-Führungskräfte in die Private Cloud**. Bevor Sie also zu einer Hybrid Cloud übergehen, muss Ihre lokale Architektur vor Ort robust und sicher sein.

Heute können robuste Private Clouds die Agilität und Flexibilität bieten, die Unternehmen von Public Clouds erwarten. Tatsächlich können Sie Automatisierung, Self-Service und KI in Ihre private Cloud integrieren und so die Agilität einer Public Cloud in Ihr eigenes Rechenzentrum bringen. Sie behalten jedoch weiterhin die Kontrolle, die Sie benötigen, um sensible Daten, Kunden- und Finanzinformationen und vieles mehr zu schützen.

Sobald Sie eine hochleistungsfähige Private Cloud eingerichtet haben, können Sie die Funktionalitäten auf die Public Cloud ausdehnen, aber stellen Sie sicher, dass Sie die Kontrolle über Ihre firmeninterne Umgebung behalten. **O'Reilly** empfiehlt beim Übergang einen dreistufigen Ansatz:

1. Wählen Sie eine zentrale Grundstruktur – ein „Cloud-Betriebssystem" –, die es Ihnen ermöglicht, Workloads vor Ort und in der Cloud zu verwalten.

2. Modernisieren Sie Ihre Vor-Ort-Umgebungen in Übereinstimmung mit dieser Grundstruktur.

3. Wählen Sie nur Public Clouds und CSPs, die mit dieser Grundstruktur kompatibel sind.

Warum? Sie müssen die Interoperabilität zwischen Ihren Clouds aufrechterhalten, sonst verpassen Sie den „Hybrid"-Teil der Hybrid Cloud. Ein zentrales Betriebssystem bedeutet, dass Sie jede Ihrer Cloud-Umgebungen mit einem einzigen, einfachen Satz von Tools überwachen, verwalten und orchestrieren können.

Do #2

STANDARDISIEREN SIE HYBRID CLOUD-PROZESSE

Dies scheint ein offensichtliches „Do“ zu sein, aber aus gutem Grund – die Art der Prozesse, die Sie anfordern oder einleiten, sollte wichtiger sein als nur die Art der Cloud, und Standardisierung kann Ihnen helfen, Ihre Arbeitsabläufe zu vereinfachen.

Verwenden Sie einen gemeinsamen Satz von Werkzeugen in Ihrer Private und Public Cloud, anstatt einfach nur Private Cloud-Tools in die Public Cloud zu übertragen. Schließlich sind nicht alle Toolsets Cloud-fähig, unter Umständen sind Sie daher vielleicht nicht in der Lage, nach Bedarf horizontal und vertikal zu skalieren. Außerdem betrachtet diese Denkweise Ihre Public Cloud als eine Erweiterung Ihres Rechenzentrums, und obwohl sie ein leistungsstarkes Asset ist, muss sie wie die separate, einzigartige Architektur behandelt werden, die sie darstellt.

Die Umsetzung von Standardisierungslösungen kann Ihnen helfen, ein besseres Gleichgewicht zu erreichen. Einige Beispiele hierfür sind Identitäts- und Zugriffsmanagement (IAM), Management des Anwendungslebenszyklus, Einhaltung von Sicherheitsvorschriften, Überwachung und Kostenkontrolle. Diese können dabei helfen, die Umgebungen sowohl in Ihren Private als auch Public Clouds zu operationalisieren.

Do #3

NUTZEN SIE EINE ZENTRALE MANAGEMENT-EBENE

Die Verwaltung einer beliebigen Cloud kann den Einsatz mehrerer Kräfte erfordern, aber die Hybrid Cloud hat ihre eigenen einzigartigen Herausforderungen. In diesem **GigaOm-Paper** wird festgestellt, dass eine Hybrid Cloud bei unsachgemäßer Verwaltung Implementierungsfehler, hohe Kosten und sogar hohe Risiken mit sich bringen kann.

Glücklicherweise kann eine zentrale Managementebene helfen, die Ihnen einen besseren Einblick in Ihre Kosten und Ihren Ressourcenverbrauch gibt. Heutzutage bieten viele Dashboards sogar maßgeschneiderte Optimierungsempfehlungen, reservierte Instanzen und andere Funktionen.

Eine gute Ausgangsbasis ist **Nutanix Beam**, das den Teams Einblicke und Transparenz in ihre Hybrid- und Multi-Cloud-Umgebung bietet. Mit richtlinienbasierter Governance gibt Beam Unternehmen in Echtzeit Empfehlungen für die richtige Dimensionierung von Cloud-Ressourcen und die Behebung von Sicherheitslücken, bevor diese zu Problemen werden.

Sie können Beam zwei Wochen lang hier kostenlos testen

Do #4

VERWALTEN SIE DIE SICHERHEIT VON EINEM PUNKT AUS

Private Cloud hier, Public Cloud dort – es kann schwierig sein, Sicherheitslücken in der Hybrid Cloud ohne ein automatisiertes Tool zur Bewertung und Behebung der Sicherheitslage im Auge zu behalten. Menschliches Versagen und die mangelnde Einhaltung von Sicherheitsrichtlinien über Cloud-Grenzen hinweg sind häufig für Lücken verantwortlich, die sich ausbreiten und kostspieligen Datenverstößen Tür und Tor öffnen.

IT-Teams sind für eine endlose Reihe sich wiederholender, mühsamer Aufgaben verantwortlich, dazu gehören die Verwaltung von Cloud-Ressourcen, die Einrichtung von VM-Konfigurationen, die Erstellung virtueller Netzwerke, die Bereitstellung von Cloud-Workloads, die Aufrechterhaltung von Verfügbarkeits- und Leistungsstandards und vieles mehr. Es ist menschlich unmöglich, die Einhaltung eines Sicherheitskonzepts über Tausende von Ressourcen und Hunderte von Anwendern hinweg manuell festzulegen und aufrechtzuerhalten.

Ohne ein zentral verwaltetes Sicherheitsprogramm oder einen zentral verwalteten Sicherheitsdienst bleibt das Risiko menschlichen Versagens hoch, wodurch Sicherheitslücken entstehen können, die die Cloud möglicherweise gefährden. Und wenn sie auftreten, werden die Unternehmen Fehler beheben müssen, was wertvolle Zeit kostet.

Die Möglichkeit, die Sicherheit über Clouds hinweg zentral zu verwalten, bedeutet, dass Unternehmen nicht in mehrere Sicherheitstools investieren müssen und auch nicht das Risiko eingehen, diese aufgrund einer Sicherheitsverletzung einzusetzen. Automatisierte Cloud-Sicherheitsüberprüfungs- und -korrekturservices wie **Xi Beam** von Nutanix gewährleisten und wenden hohe Sicherheitsstandards auf die Cloud an, durch:

- Über 1.000 automatisierte Cloud-Sicherheitsüberprüfungen
- Behebung von Sicherheitslücken mit einem Klick
- Überwachung der Einhaltung regulatorischer Richtlinien wie HIPAA, PCI-DSS, NIST und mehr


DON'T

Don’t #1

LASSEN SIE WISSENS-SILOS NICHT DIE HYBRID-EINFÜHRUNG VERHINDERN

Die Kluft zwischen den absoluten Verfechtern von Hybrid Clouds und jenen, die sie auch tatsächlich eingeführt haben, ist enorm. Tatsächlich ergab der **Enterprise Cloud Index 2019**, dass 85% der Befragten die Hybrid Cloud als ihr bevorzugtes Cloud-Computing-Modell nannten. Derselbe Report stellte jedoch auch fest, dass nur 12,6% dieses Modell tatsächlich schon übernommen hatten – 5,4% weniger als im Report von 2018.

Warum? Viele Unternehmen befürchten, dass sie nicht über die Manpower oder das Wissen verfügen, die für das Management einer Hybrid Cloud erforderlich sind. Unternehmen befürchten, dass eine Hybrid Cloud ein eigenes Management-Team oder teure Spezialisten benötigt, um sie (und vor allem der Bereich der Public Cloud dahinter) am Laufen zu halten. Und da nur wenige Organisationen über ein unerschöpfliches IT-Budget verfügen, sind sowohl die Bezahlung von Spezialisten als auch die Umschulung von bestehenden Teams legitime Befürchtungen.

Es gibt jedoch zahlreiche Möglichkeiten, den Betrieb und das Management vonHybrid Clouds mühelos zu gestalten. **GigaOm** erklärt, wie wichtig Investitionen in Automatisierung sind, wenn es um Hybrid Cloud-Management geht, insbesondere im Hinblick auf die Reduzierung von Cloud-Ausgaben, Zeitaufwand für das Management und Sicherheitslücken.

Don’t #2

BEHANDELN SIE DIE PUBLIC CLOUD NICHT WIE DIE PRIVATE CLOUD

Manchmal behandeln Unternehmen die Public Cloud als Lösung für ihre Probleme vor Ort und „übergeben“ ihre Bedenken im Wesentlichen an ihren Public-Cloud-Anbieter.

Doch realistischerweise erfordern Private und Public Cloud-Architekturen unterschiedliche Ansätze. Ihre Private Cloud mag Sicherheitsstandards und vielleicht sogar Sicherheits-automatisierungstools etabliert haben, aber mit der Zusammenführung mit der Public Cloud übernehmen Sie mehr Verantwortung für die Sicherheitsüberwachung.

Insbesondere sollten Sie ein Modell mit geteilter Verantwortung einrichten und kontinuierlich Überprüfungen auf Fehlkonfigurationen von Ressourcen durchführen, um Ihre Workloads in der Public Cloud zu schützen. Denken Sie daran: Der Public Cloud-Anbieter ist für die Sicherheit der Cloud verantwortlich, aber Sie sind für die Sicherheit der Ressourcen in der Cloud verantwortlich. Aus diesem Grund sind Tools zur Verwaltung der Sicherheit in der Cloud wichtig, um zu gewährleisten, dass Ihr Übergang von der Private Cloud zur Hybrid Cloud die Einhaltung von Sicherheits- und regulatorischen Richtlinien nicht gefährdet.

Die Verantwortung, Geschäftsprozesse und Compliance-Anforderungen ordnungsgemäß abzuwickeln, liegt auf Ihren Schultern. Etablieren Sie Tools zur Verwaltung Ihrer Hybrid Cloud in Echtzeit und besprechen Sie die Möglichkeiten mit Ihrem Cloud-Partner, um zu erfahren, wie diese Tools funktionieren, bevor Sie kritische Workloads migrieren.

Don’t #3

VERNACHLÄSSIGEN SIE NICHT DIE EINZIGARTIGEN OPERATIVEN ASPEKTE DER HYBRID CLOUD

Eine Hybrid Cloud ist eine wunderbare Sache, aber sie ist mit unterschiedlichen Kosten, Sicherheits- und Compliance-Maßnahmen und Möglichkeiten zur Messung und Optimierung von Funktionalität und Verfügbarkeit verbunden. Diese sind nicht notwendigerweise komplexer – jedoch einzigartig!

Weshalb? Ihre Hybrid Cloud stützt sich auf zwei völlig unterschiedliche Arten von Clouds: Private und Public Clouds. Beide haben unterschiedliche Strukturen, Komponenten, Lizenzmodelle, und unterschiedliche Workloads funktionieren auf der einen besser als auf der anderen bzw. umgekehrt.

Aber ihre Unterschiede bedeuten nicht, dass man sie in Silos einführen sollte, wodurch letztlich zwei Gruppen von komplexen operativen Standards und Verbrauchsmodellen entstehen.

Sie wollen nahtlose Interoperabilität – keine unzusammenhängenden Clouds. Die Einrichtung von Automatisierung kann Ihnen helfen, die einzigartigen Umgebungen in beiden Clouds zu bewältigen und Workloads in der am besten geeigneten Umgebung bereitzustellen. Und während Automatisierung zwar in jeder Umgebung sinnvoll ist, ist sie besonders nützlich in einer Hybrid Cloud.

DER WEG ZU EINER ECHTEN HYBRID CLOUD

Wenn Sie davon gehört haben, wie komplex es ist, eine Hybrid Cloud-Umgebung zu betreiben, haben Sie sich wahrscheinlich bisher zurückgehalten, den Schritt tatsächlich zu wagen.

Kontaktieren Sie uns und wir helfen Ihnen gerne, den Wechsel mühelos zu vollziehen.

NUTANIX™
YOUR ENTERPRISE CLOUD