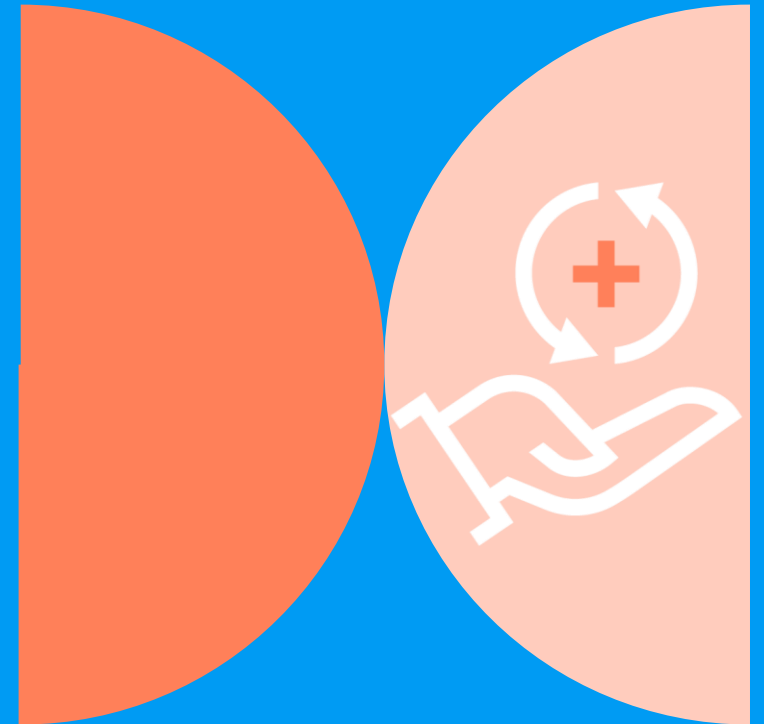


Backup as a Service Sales Playbook für intern und Partner

Version 1.5, Januar 2026

NICHT FÜR ENDKUNDEN

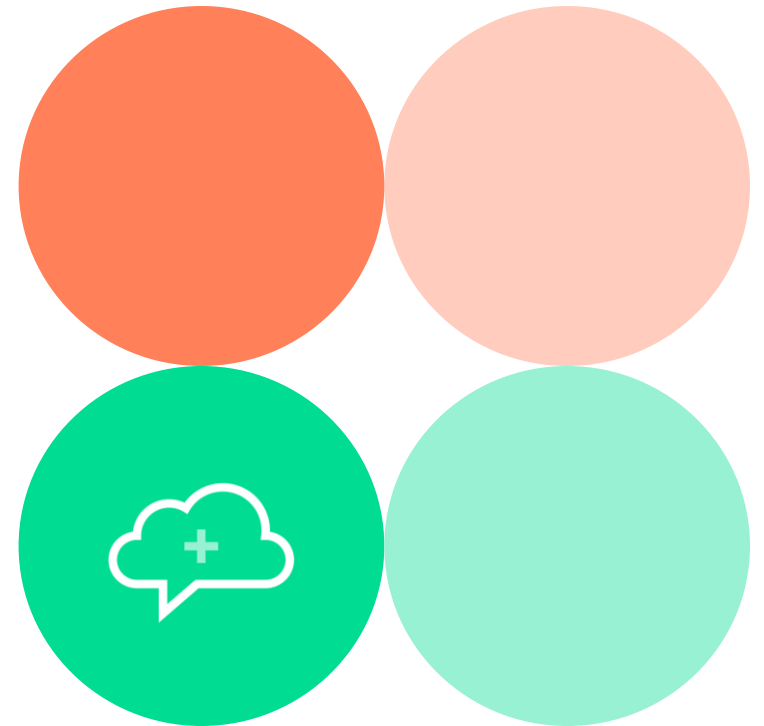


Was ist ein Sales Playbook?

Dieses Dokument dient der internen Benutzung bei plusserver und Partner-Unternehmen. Es enthält essenzielle Informationen zu Produkten und soll helfen, die Erstgespräche mit Kunden und Interessenten vorzubereiten.

Die Inhalte des Dokuments sind nicht zur Weiterleitung an den Kunden gedacht, dienen vielmehr dem Aufbau eigener Argumentationsketten und sollen u. a. folgende Fragen beantworten:

- + Was kann das Produkt?
- + Für wen ist das Produkt?
- + Wie kann ich die Zielgruppe von den Vorzügen des Produkts überzeugen?
Welche Argumente und Antworten helfen im Gespräch mit dem Kunden?
- + Wie grenzt sich das Produkt vom Wettbewerb ab?



Backup as a Service

... warum es ein Door Opener für Sales ist

Backup ist ein Evergreen ...

- + Gibt es schon immer, seit es IT gibt
- + Es ist schon immer das ungeliebte Kind, für das Geld ohne direkt sichtbaren Nutzen ausgegeben werden muss
- + Und viele Firmen werden schon eine Lösung in irgendeiner Form im Einsatz haben

... der aber brandaktuell ist

- + Ransomware-Angriffe machen Daten unzugänglich
- + DSGVO: Datenverlust kann ein meldepflichtiger Verstoß sein
- + IT-zentrische Produktion verursacht bei IT-Ausfällen enorme Kosten oder Schwierigkeiten

Backup leicht gemacht

- + Der Kunde braucht wenig bis kein technisches Know-how
- + Externes Backup inkl. Georedundanz/Immutability für doppelte Sicherheit
- + Bedarfsorientiertes OPEX-Modell statt schwer zu planende CAPEX-lastige Investitionen



Vorteile & Potenziale von Backup as a Service

Argumente auf einen Blick

Technologische Vorteile

- + Gemanagte Plattform: Kunde muss sich nicht darum kümmern, keine eigene Infrastruktur nötig, kein Personal für Administration
- + Automatische georedundante Kopie (immutable, Ransomware-protected) in einem zweiten plusserver-Datacenter
- + Support für Windows, Linux und Mac Clients sowie VMware ESXi mit Veeam B&R Server
- + Disaster Recovery eines VMware vCenter zur pluscloud möglich (in Entwicklung)
- + Skalierender Speicherplatz
- + Self-Service-Portal für schnelle Einrichtung und flexible Anpassungen
- + Veeam Enterprise-Technologie als verlässlicher Standard

Potenziale für Kunden

- + Einfache Nutzung ohne umfangreiches Fachwissen
- + Pay-as-you-go: Kunden zahlen nur den tatsächlichen Verbrauch, ohne Investitionskosten
- + Dynamische Skalierung ohne langwierige Bedarfsplanung
- + DSGVO-konform in den technischen und organisatorischen Maßnahmen
- + Hohe Compliance: ps-Datacenter in Deutschland
- + Deutschsprachiger 24/7 Support

Pricing-Modell

- + Fair und übersichtlich ohne versteckte Kosten nach drei Metriken:
 - + Speicherplatzverbrauch im Monatsmittel
 - + Anzahl gesicherter Systeme
 - + Lizenzgebühren für Workstation, Server oder VM-Replizierung, sofern der Kunde keinen lizenzierten Veeam-Server nutzt
- + Rabatte bei Mindestabnahmen über Laufzeiten
- + Rein OPEX, kein CAPEX notwendig

plusserver steht für digitale Souveränität mit Cloud Services made in Germany

Was steckt hinter Backup as a Service?

Technische Spezifikationen

Typische Anwendungsszenarien	Ablösung eigener Backup-Umgebung
Basis-Technologie	Veeam Agent Based + Streaming Backup
Backup-Quellen	<ul style="list-style-type: none"> VM in pluscloud VMware VM in pluscloud open Hyperscaler (AWS, Azure, GCP) Onprem VMs (VMware) Server Onprem / Server plusserver (dedicated) Onprem Client (Windows, Unix Mac)
Erstes Backuptarget	Festplatten im Veeam shared Repo in der selben Geolokation
Zweites Backuptarget	S3-Speicher in einer anderen Geolokation

Backup-Konsistenz	Application Aware Backup
Managed Support	Operational Support und Full Managed Backup möglich, wenn die Quelle bei plusserver liegt und Operational Support/Full Management für die Quelle gebucht ist.
Self-Service	ja
Abrechnung	Commitment und/oder Pay-as-you-go

Technische Kombinationsmöglichkeiten

... mit anderen plusserver-Produkten

Security & Storage

Security

- + EDR as a Service
- + SOC as a Service
- + Security Scanner
- + DDoS-Schutz
- + Web Application Firewall

Storage

- + S3 Storage / Object Storage
- + Network Storage

Compute

- + pluscloud open
- + pluscloud VMware
- + Dedicated Server

Datenbanken & Container

Datenbanken

- + alle DBaaS

Container

- + Managed Kubernetes

Ausgangssituation

... von Unternehmen und öffentlichen Auftraggebern

Anforderungen von Unternehmen und öffentlichen Auftraggebern an Datenhoheit, Datensicherheit sowie Rechtsraumsicherheit rücken deutlich in den Vordergrund und dienen immer mehr als Entscheidungsgrundlage für Cloud-Infrastrukturen.

- + **Vendor Lock-in:** Unternehmen haben den Wunsch, in die Cloud zu migrieren, sind aber durch Vendor Lock-ins und/oder externe Vorschriften geblockt, internationale Anbieter zu nutzen.
- + **Compliance:** Strenge Vorgaben gerade im Behördenbereich verlangen starken Datenschutz, lokale Datenhaltung und Transparenz bei der Auswahl einer geeigneten Lösung.
- + **Maintenance:** Unternehmen möchten sich auf ihr Geschäftsmodell konzentrieren. Der 24/7-Betrieb eines IaaS bleibt oftmals außen vor und wird somit zu einem Risiko für das Unternehmen.
- + **Fehlendes Personal:** Der anhaltende Fachkräftemangel wirkt sich hierbei zusätzlich negativ aus, wenn Unternehmen und der öffentliche Sektor sich neben der Entwicklung von neuen Anwendungen auch um den Betrieb und die Wartung der zugrundeliegenden Infrastruktur kümmern müssen.
- + **Kostenschungel:** Der Aufbau und die Wartung einer eigenen Infrastruktur sind mit hohen Investitions- und Wartungskosten verbunden, während intransparente Kostenübersichten bei manchen Cloud-Anbietern für Verwirrung und böse Überraschungen auf der Rechnung sorgen können.
- + **Auf dem Laufenden bleiben:** Unternehmen haben zwar den Wunsch, technologisch auf dem neuesten Stand zu sein. Den Überblick über die neuesten Updates und notwendigen Patches zu behalten, bleibt im Tagesgeschäft jedoch oft auf der Strecke und kann Risiken für den Betrieb bedeuten.

Die Lösung liefert plusserver

Ihr Business läuft, was auch passiert

Mit plusserver Backup as a Service sichern Sie Daten von verschiedenen Endgeräten souverän, zuverlässig und flexibel, ohne dass Sie eine eigene Infrastruktur aufbauen müssen. Das Besondere: Eine georedundante Zweitkopie und Immutability sind bereits inklusive. Damit erfüllen Sie Best Practices für Ausfallsicherheit und Ransomware-Schutz, ohne zusätzliche Budgets einplanen zu müssen. Basierend auf Veeam Cloud Connect steuern Sie Ihr Backup bequem über ein Self-Service-Portal oder lassen es optional von plusserver managen. So verbinden Sie höchste Sicherheit und Compliance mit maximaler Flexibilität – zu transparenten, planbaren Kosten.

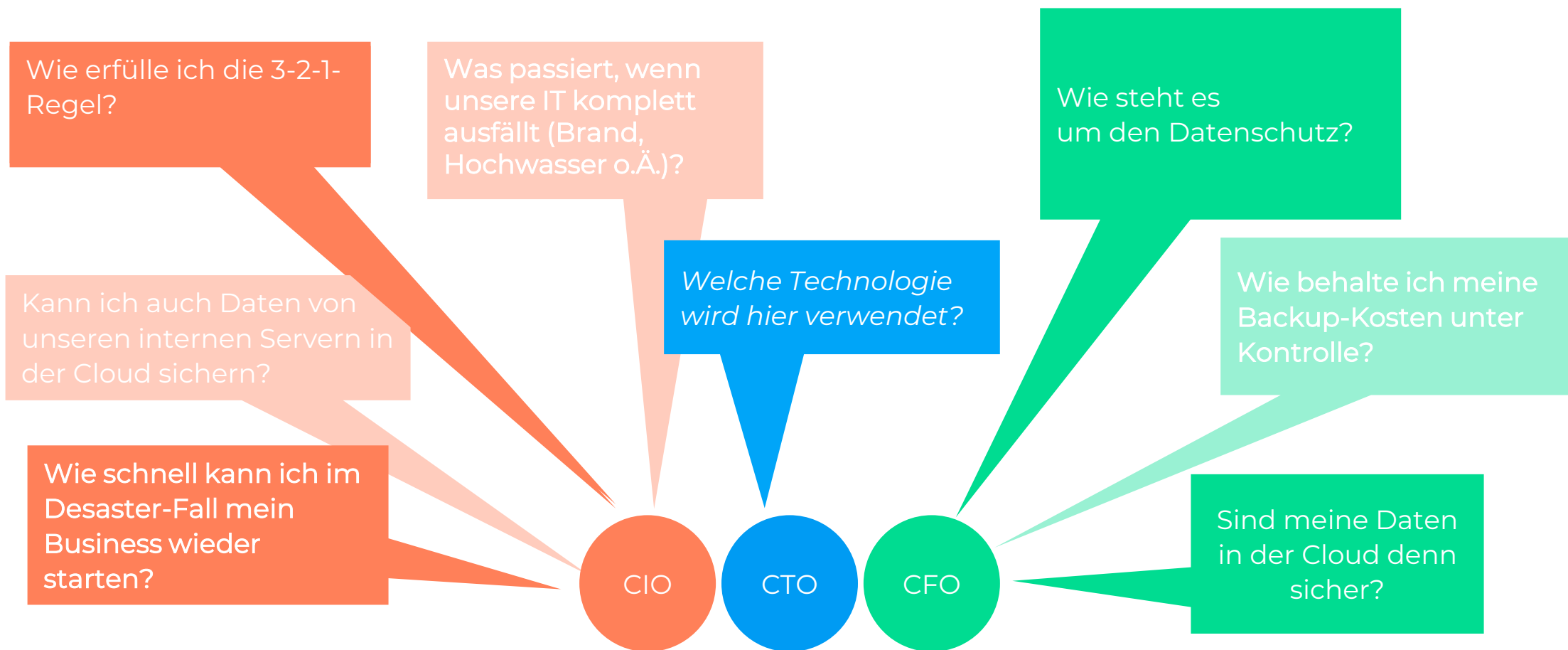
plusbackup basiert auf Veeam Cloud Connect

Veeam Cloud Connect macht es denkbar einfach, Backups von VMs, Servern oder Dateien in einem externen Cloud Repository in der pluscloud VMware abzulegen. Dabei sind alle Daten bei der Übertragung durch eine TLS-verschlüsselte Verbindung zum Cloud Connect Gateway bei plusserver geschützt. Wenn Sie Veeam bereits im Unternehmen nutzen, erhalten Sie die Option, die pluscloud VMware in Ihrem Interface als zusätzlichen Speicherort auszuwählen.



Fragestellungen von Entscheidenden zum Produkt,

die Cloud-Technologieführer beantworten sollten:



Argumentationsmatrix – Fragen + Mehrwerte

Fragen & Antworten sowie ...

... weitere wesentliche Mehrwerte

Wie erfülle ich die 3-2-1-Regel?

Die Regel sieht vor, dass von allen Daten drei Kopien bestehen (ein Original und zwei Backups), die auf mindestens zwei unterschiedlichen Medien gespeichert sind und ein Backup extern aufbewahrt wird. Beim plusbackup werden die Backups immer automatisch an einem zweiten Standort gesichert, sodass die Regel erfüllt wird.

Kann ich auch Daten von unseren internen Servern in der Cloud sichern?

Mit plusbackup lassen sich Daten von On-premises-Infrastrukturen, Cloud-Ressourcen von Drittanbietern oder aus der pluscloud open bzw. dedizierten Servern bei plusserver sichern. Unterstützt werden sowohl Server als auch Workstations.

Erschließung neuer Märkte

- ✓ Durch die Sicherheit, dass keinerlei Daten den Rechtsraum Deutschland verlassen, können Unternehmen neue Kunden in Branchen ansprechen, die mit besonders sensiblen Daten arbeiten, wie bspw. Finanz- oder Gesundheitsdaten.
- ✓ Deutschland genießt international ein hohes Ansehen hinsichtlich seiner strengen Sicherheitsvorgaben und Gesetze. Dies kann für Interessenten auch ein wichtiges Argument sein bezüglich des Datenschutzes.

Hilfe ohne Sprachbarriere und Zeitzoneprobleme

- ✓ Durch deutschen 24/7 Support gibt es keine Missverständnisse. Für internationale Kunden bietet plusserver schnelle Hilfe auf Englisch.
- ✓ Bei ausgelagerten Support-Zentren in anderen Ländern, oft auf anderen Kontinenten, gibt es oft nicht nur Sprachprobleme. Durch die unterschiedlichen Zeitzone kann es länger dauern, bis Hilfe vor Ort organisiert werden kann.

Argumentationsmatrix – Fragen + Mehrwerte

Fragen & Antworten sowie ...

... weitere wesentliche Mehrwerte

Sind meine Daten in der Cloud denn sicher?

Die eigenen plusserver-Rechenzentren in Deutschland sind mehrfach zertifiziert und weisen ein Sicherheitsniveau auf, das Firmen-Rechenzentren in der Regel nicht erzielen. Zudem werden alle Daten schon vor der Übertragung verschlüsselt (in flight und at rest). Der Schlüssel ist nur dem Kunden bekannt.

IT-Transformation mit voller Transparenz und allen Freiheiten

✓ Kein Vendor Lock-in: Kunden haben die maximale Souveränität über Daten und ihre eigene digitale Transformation, abgestimmt auf individuelle Bedürfnisse.

Wie steht es um den Datenschutz?

plusbackup ermöglicht Unternehmen DSGVO-konforme und CLOUD-Act-neutrale Datensicherung. Sowohl der Hauptsitz als auch die RZ von plusserver liegen in Deutschland. Dritte haben keinen Zugriff auf bei plusserver gespeicherte Daten.

Argumentationsmatrix – Fragen + Mehrwerte

Fragen & Antworten sowie ...

... weitere wesentliche Mehrwerte

Welche Technologie wird hier verwendet?

Veeam Cloud Connect ist die bewährte Technologie, um Backups sicher und leistungsstark an einen BaaS-Anbieter zu senden.

Wie behalte ich meine Backup-Kosten unter Kontrolle?

Im Vergleich zu Lösungen im Eigenbetrieb bietet Cloud Backup den Vorteil, die Hardware nicht selbst anzuschaffen und zu warten, sondern Ressourcen nach Bedarf zu nutzen und zu bezahlen (Pay-as-you-go).

Mehr Widerstandsfähigkeit durch Skalierung nach Maß

- ✓ Planbare Betriebskosten statt hoher Investitionskosten für Hardware (deren Preise stark schwanken können) machen Unternehmen resilienter gegenüber unvorhersehbaren Ereignissen
- ✓ Gleichzeitig können Cloud-Ressourcen flexibel an den aktuellen Bedarf und die finanzielle Situation des Unternehmens angepasst werden, egal ob durch eine Erhöhung oder Senkung der Ressourcen. Durch den Einsatz eines Cloud-Anbieters entfällt der komplette Arbeits- und Betriebsaufwand sowie der Zeitfaktor zur Auf-/Abwärtsskalierung von physischer Hardware für die eigene IT-Abteilung.
- ✓ Ist ein langfristiger Ressourcenbedarf bekannt, können Verträge mit Commitments für eine feste Zusicherung von Ressourcen abgeschlossen werden. Entsprechend können Laufzeiten für Preisvorteile und -sicherheiten vereinbart werden.

✓ Sind

Argumentationsmatrix – Fragen + Mehrwerte

Fragen & Antworten sowie ...

... weitere wesentliche Mehrwerte

Was passiert, wenn unsere IT komplett ausfällt (Brand, Hochwasser o.Ä.)?

In Entwicklung: Disaster Recovery bietet die Möglichkeit, selbst dann geschäftsfähig zu bleiben, wenn die IT am Produktivstandort komplett ausfällt. plusserver unterstützt dabei, eine zweite Umgebung in der pluscloud VMware vorzubereiten und im Notfall hochzufahren. (Geht nur für gesicherte VMware VMs)

Wie schnell kann ich im Disaster-Fall mein Business wieder starten?

In Entwicklung: Mit einem reinen Backup kann die Wiederherstellung der Geschäftsfähigkeit eine Weile dauern. Durch eine konsistente Replikation aller Daten und Anwendungen im Rahmen eines DRaaS-Plans kann das Business relativ schnell und mit nahezu aktuellem Datenstand wiederhergestellt werden (kurzes RTO und RPO = Recovery Time Objective, Recovery Point Objective).

Mehr Raum für Innovationen

- ✓ Durch die Auslagerung von Day-2-Operations an den Cloud-Anbieter sowie den Einsatz von Managed Services entlasten Unternehmen ihre eigenen IT-Mitarbeitenden. Ohne die mentale und operative Last von Routineaufgaben und Maintenance haben diese mehr Zeit und kognitive Kapazitäten, an Innovationen und anderen geschäftsfördernden Projekten zu arbeiten.

Mehr Mitarbeiterbindung und neue Talente

- ✓ Weniger Routinearbeiten und mehr Freiraum allgemein erhöhen die Mitarbeiterzufriedenheit und steigern die Bindung zum Unternehmen.
- ✓ Teilen Mitarbeitende ihre positiven Erfahrungen auf Plattformen wie LinkedIn oder Kununu, macht dies das Unternehmen auch attraktiv für Nachwuchskräfte.

Anhang: Was ist die 3-2-1-Regel?

Die 3-2-1-Regel ist eine oft angewandte Best Practice, da sie unterschiedliche Bedrohungen adressiert:

- + Menschliche Fehler oder versehentliches Löschen -> einfache, schnelle Wiederherstellung
- + Ausfall der Backuphardware, Bugs oder Serienfehler -> Zweite Backup-Kette muss zur Wahrung der Recovery-Fähigkeit vorhanden sein
- + Ausfall der Produktionshardware -> Wiederherstellung auf anderer Hardware am Originalstandort
- + Ausfall des Produktionsstandortes -> Wiederherstellung entfernt gesicherter Daten am Ausweichstandort

Um diese Punkte zu erfüllen, müssen zwei Backups erstellt werden, wovon eines mit hoher Geschwindigkeit mit dem Originalstandort verbunden sein muss. Eines muss sich an einem anderen Standort befinden.

Zur Abdeckung von Bugs oder Hardwarefehlern sollten die Backups auf unterschiedlichen Speichertechnologien beruhen. plusbackup erreicht dies durch eine Kopie des ersten Backups zu einem entfernten S3-Standort in einem unserer RZ.



3

**Kopien
der Daten**



2

**Verschiedene
Speichermedien**



1

**Externe
Aufbewahrung**

Anhang: GFS-Prinzip

Das Generationenprinzip sorgt dafür, dass immer mehrere Sicherungen in verschiedenen zeitlichen Abstufungen (Grandfather, Father, Son) vorhanden sind, um verschiedene Versionen für eine mögliche Wiederherstellung zur Verfügung zu haben.

Das GFS-Prinzip beim plusbackup arbeitet nicht mit Wechselmedien, sondern stellt durch bestimmte Speicherverfahren (RAID, erasure coding, backup copy) immer eine Verfügbarkeit des gesamten Datenbestands sicher.

Normalerweise werden mit plusbackup tägliche Sicherungen (= Sohn) angelegt. Um eine versehentlich gelöschte Datei wiederherzustellen, die erst nach Monaten vermisst wird, müssten sehr viele Söhne über einen langen Zeitraum aufbewahrt werden, die Speicherplatz benötigen und damit Kosten verursachen.

Im GFS-Prinzip werden daher einzelne Backups bestimmter Intervalle, z. B. wöchentlich (Father) und monatlich (Grandfather) mit separat einstellbaren Vorhaltezeiten, aufgehoben. So können z. B. Backups vom Mittwoch immer für acht Wochen und das jeweils letzte monatliche für ein ganzes Jahr aufbewahrt werden.

Configure GFS

Keep weekly full backup for: 8 weeks

If multiple full backups exist, use the one from: Wednesday

Keep monthly full backups for: 12 months

Use weekly full backup for the following week of a month: Last

Keep yearly full backups for: 1 year

Use monthly full backup for the following month: January

OK Cancel