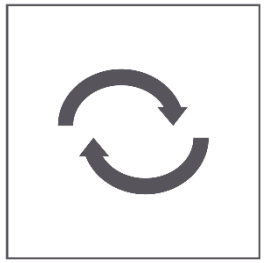
d.velop

d.velop cloud storage

Herausforderungen

Hardware-Storage verursacht hohe Kosten:

- Investment und Wartung
- Strom und Kälte
- Administration
- Platz



Zyklische Migrationskosten
von Hardware zu Hardware

Risiko der **Unterlizenzierung** von **Storage-Kapazität**

Multiredundantes
Hardware-Storage-System ist komplex zu erstellen

- Brandabschnitte
- verschiedene Standorte
- Synchronisierungsanforderungen

Die Antwort: d.velop cloud storage

Was wäre, wenn Ihre **wichtigen Unternehmensinformationen** in Zukunft ohne eigene lokale Storage-Systeme **revisionssicher** und **rechtskonform** archiviert werden könnten?

- ✓ Vieles wäre **einfacher**
- ✓ Vieles wäre **flexibler**
- ✓ Vieles wäre **günstiger**
- ✓ Vieles wäre **sicherer**

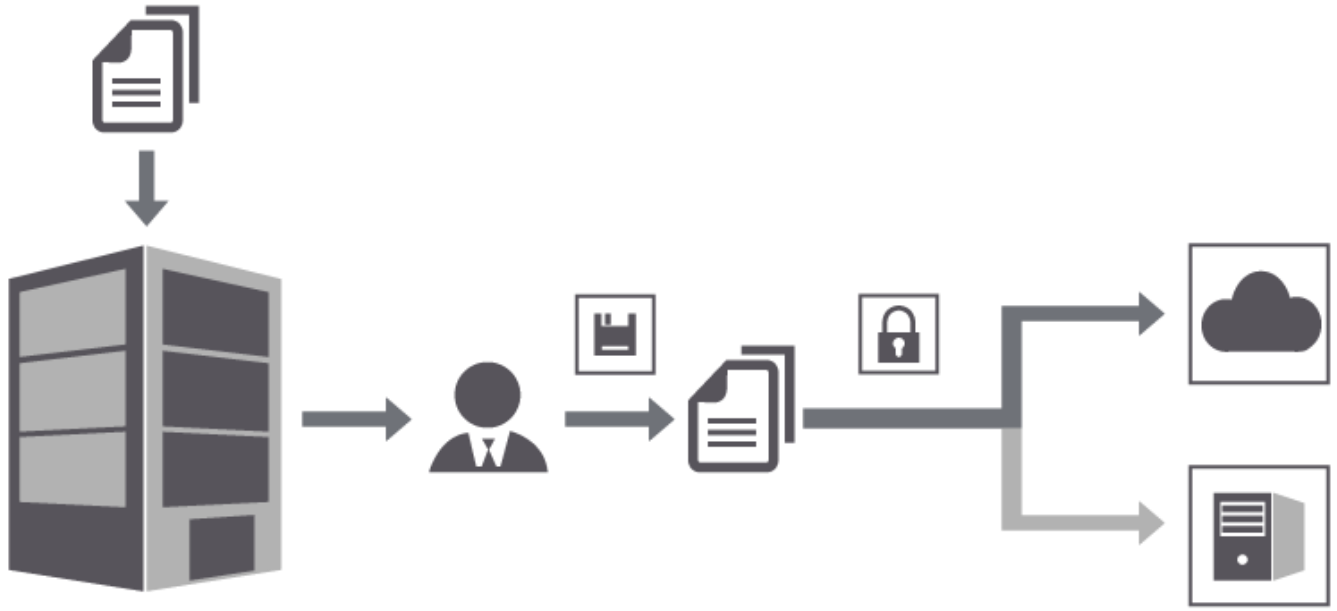
Mit dem d.velop cloud storage können Sie **ab sofort** auf eigene Storage-Systeme verzichten und Ihre Daten **sicher, performant und revisionskonform in der d.velop Cloud archivieren**.

Die kostspielige Beschaffung und Wartung von Hardware-Storage-Systemen **entfällt!**.

Allgemeine Beschreibung

Wir bieten Ihnen mit zwei verschiedenen Einsatzszenarien die Flexibilität zu Entscheiden, in welchen Schritten Sie Ihren Weg in die Cloud gestalten:

- entweder nutzen Sie d.velop cloud storage als zusätzliches **Backup** für Ihr weiterhin bestehendes lokales Storage System **(hybride Variante)**, oder
- Sie lagern Ihren Storage gleich **vollständig** aus **(Cloud-only-Variante)**:



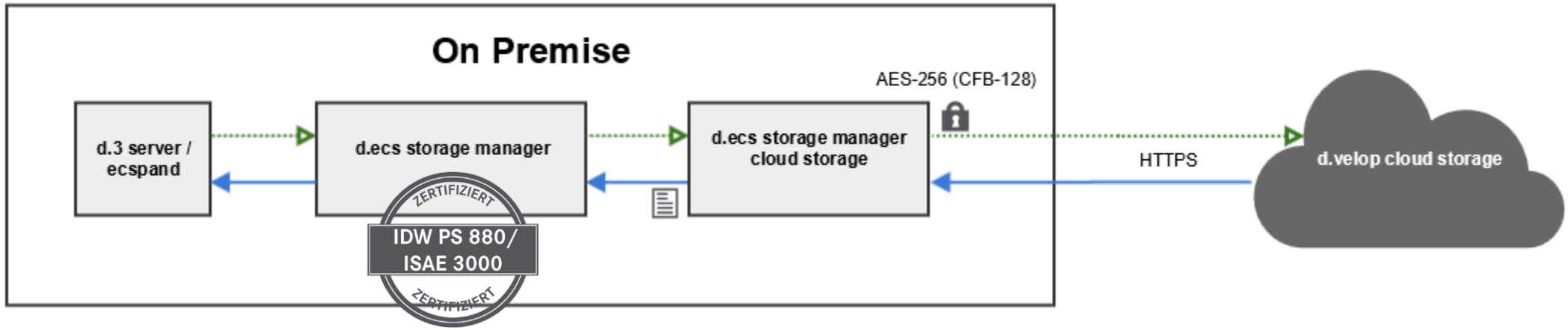
Dokumente im Unternehmen werden von Mitarbeitern verarbeitet und revisionssicher gespeichert. Entweder hybrid als Backup (hellgrau+dunkelgrau) oder "Cloud-only" (dunkelgrau).

Vorteile

- **Flexibles Volumen** - Im Gegensatz zum eigenen Hardware-Storage steht Ihnen unlimitierter Speicher flexibel buchbar zur Verfügung. Zahlen Sie also nur für das, das Sie benötigen.
- **Beständiges System** - d.velop cloud storage wird von d.velop betrieben und laufend aktualisiert. Um die Beschaffung oder Wartung von Hardware müssen Sie sich keine Gedanken mehr machen.
- **Kostengünstig** - Sie zahlen nur den Speicher, den Sie aktuell buchen und belegen. Hohe und wiederkehrende Investitionen in Hardware fallen komplett weg.
- **Einfache Verwaltung** - Die komplette Administration von d.velop cloud storage verantwortet d.velop. Ihr IT-Team konfiguriert lediglich den d.velop storage manager - wie gewohnt.
- **Sicher und hochverfügbar** - Als SaaS liegt die Verantwortung des Betriebs bei der d.velop.
- **Speicherort Deutschland** - d.velop cloud wird auf zertifizierten Systemen in Deutschland betrieben. Dort werden Ihre Daten abgelegt, dort bleiben sie – mit Sicherheit.
- **Verschlüsselt** - Ihre Dokumente werden in Ihrer Hoheit ver- und entschlüsselt. Der zugehörige Schlüssel wird auf Ihren Systemen generiert und ist nur Ihnen bekannt.
- **Support** - d.velop unterstützt Sie auf Wunsch bei der Einrichtung.

Schematische Darstellung

- Die verwendeten Komponenten werden aktuell auf die Anforderungen der EU-DSGVO angepasst
- Die OnPremise verwendete Software *d.ecs storage manager* ist gemäß PS880 zertifiziert
- Das eingesetzte Rechenzentrum ist gemäß ISO27001, ISO27017, ISO27018 und weiteren Standards zertifiziert



KPMG IDW PS 880 und ISAE 3000

- Die für den d.velop cloud storage verwendete d.velop Software *d.ecs storage manager 3.2.0* ist von der KPMG erfolgreich geprüft worden.

  Die Berichte sind unter den folgenden Links erhältlich:

- IDW PS 880:
  https://www.kpmg.de/bescheinigungen/RequestReport.aspx?91ED39525DC64C8F9C559D5807E30F70

- ISAE 3000:
  https://www.kpmg.de/bescheinigungen/RequestReport.aspx?477027009DD14E7F8FFBEFCAF97079B9

Datenschutz

- Die Daten werden **redundant** auf **mehreren Servern** und in mehreren Rechenzentren im **Großraum Frankfurt am Main** gespeichert.

- **Datenschutz und Datensicherheit** wird bei d.velop groß geschrieben - seit 25 Jahren. Und das gerade in der Cloud. Mit den bewährten d.velop Encryption Services werden Ihre Daten **bereits mit dem Upload verschlüsselt** und bleiben es solange bis sie durch Ihre Initiative entschlüsselt werden.

- Damit sind die Voraussetzungen für die Realisierung eines **revisionssicheren Speichers** gegeben. Gerne unterstützt d.velop Ihren Wirtschaftsprüfer mit einer entsprechenden Dokumentation.

Verschlüsselung

- Zur Vermeidung von unberechtigter Einsicht der Dokumente können diese bei der Auslagerung in den d.velop cloud storage **verschlüsselt** werden. Dabei wird eine **AES-256-Verschlüsselung** mit CFB-128 (Cipher Feedback) verwendet.

- Die Verschlüsselung findet "on the fly" während der Auslagerung On Premises statt. Die Daten **verlassen** somit **das Kundensystem nicht unverschlüsselt** und werden auch nur auf dem Kundensystem wieder entschlüsselt!

- Der Schlüssel, der zur Ver- und Entschlüsselung verwendet wird, ist auf dem **Kundensystem** in **verschlüsselter Form** gespeichert. Er **kann nicht** auf ein anderes System **kopiert werden**, da er dort nicht mehr entschlüsselt werden kann. Will man den Schlüssel auf einem anderen System verwenden, dann muss man im Besitz der **"Security ID"** sein. Dies ist ein Schlüssel, der beim Aktivieren der Verschlüsselung generiert, ausgedruckt und sicher verwahrt werden muss. Bei Verlust dieses Schlüssels können die zuvor verschlüsselten Daten nicht wieder entschlüsselt werden. Die d.velop AG hat **grundsätzlich keine Möglichkeit, die Daten zu entschlüsseln**.

Sicherheit

- d.velop cloud storage nutz die S3-Technology, welche lt. AWS eine **Objektlebensdauer von 99,999999999%** gewährleistet. Die Wahrscheinlichkeit für einen Objektverlust liegt damit bei 0,000000001%. Dies entspricht bei 10.000 Dokumenten dem Verlust von 1 Dokument in 10.000.000 Jahren. Durch eine redundante Speicherung der Datenobjekte, kann ein gleichzeitiger Verlust in verschiedenen Standorten nahezu vollständig ausgeschlossen werden.

- Die Referenzen der in d.velop cloud storage abgelegten Dokumente werden in der Referenz-Tabelle von d.ecs storage manager gespeichert. Über diese Referenzen ist d.ecs storage manager in der Lage, die Dokumente anzufordern und bereitzustellen. Die Referenzen werden bei der Auslagerung in **chronologischen Referenz-Logdateien** protokolliert und in einem konfigurierbaren Intervall auf d.velop cloud storage ausgelagert.

- Sollte die Datenbank und somit die Referenz-Tabelle von d.ecs storage manager verloren gehen oder durch das Einspielen eines Backups auf einen früheren Stand zurückgesetzt werden, kann sie durch die **Referenz-Logdateien** wieder aufgebaut werden.

AWS – Sicherheit und Compliance

AWS-Programme zur Bestätigung der Sicherheit

CSA
Cloud Security Alliance-Kontrollen

ISO 9001
Weltweiter Qualitätsstandard

ISO 27001
Sicherheitsmanagement kontrollen

ISO 27017
Cloud-spezifische Kontrollen

ISO 27018
Schutz personenbezogener Daten

PCI DSS Level 1
Payment Card-Standards

SOC 1
Prüfungskontrollbericht

SOC 2
Sicherheits-, Verfügbarkeits- und Vertraulichkeitsbericht

SOC 3
Allgemeiner Kontrollbericht

C5 [Deutschland]
Testierung der Betriebssicherheit

Cyber Essentials Plus [UK]
Cyber-Bedrohungsschutz

G-Cloud [GB, Nordirland]
Britische Regierungsstandards

IT-Grundschutz [Deutschland]
Grundlegende Schutzmethode

https://aws.amazon.com/de/compliance/pci-data-privacy-protection-hipaa-soc-fedramp-faqs/, 03.04.2018

Informationsanfragen bei Amazon

„Bei Amazon sind wir uns bewusst, dass Privatsphäre und Datenschutz unseren Kunden wichtig sind. Daher optimieren wir unsere Bemühungen, auf diesem Gebiet den Bedürfnissen unserer Kunden gerecht zu werden.

Amazon gibt Kundeninformationen nicht weiter, es sei denn, wir sind aufgrund einer gültigen und bindenden juristischen Entscheidung dazu verpflichtet. Außer wenn es uns nicht gestattet ist oder es klare Anzeichen für illegales Verhalten in Verbindung mit den Produkten und Diensten von Amazon gibt, benachrichtigt Amazon seine Kunden vor der Offenlegung ihrer Inhalte.

Wenn wir öffentlich tätig werden müssen, um Kunden zu schützen, tun wir dies. Amazon war niemals Teil des PRISM-Programms der NSA. Wir haben wiederholt Einspruch gegen Vorladungen eingelegt, bei denen unserer Meinung nach zu weit gefasste Kundeninformationen offen gelegt werden sollten. Dabei konnten wir Urteile zu unseren Gunsten verzeichnen, bei Entscheidungen, die zur Etablierung gesetzlicher Standards beim Schutz von Meinungsfreiheit und Privatsphäre von Kunden beigetragen haben. Wir setzen uns auch im US-Kongress dafür ein, veraltete Privatsphäre-Gesetze zu modernisieren, damit Strafverfolgungsbehörden einen gerichtlichen Durchsuchungsbeschluss benötigen, um Einsicht in die Inhalte von Kundenkommunikation zu erhalten. Dieser Standard ist angemessen und es ist der Standard, nach dem wir uns richten.

Wir erkennen die legitimen Bedürfnisse von Strafverfolgungsbehörden bei der Untersuchung krimineller und terroristischer Aktivitäten an und kooperieren mit diesen Stellen, wenn bei der Durchführung der Ermittlungen die gesetzlichen Schutzbestimmungen geachtet werden. Wir stellen uns allerdings gegen Gesetzgebung, die Sicherheits- und Verschlüsselungstechnologien verpflichtend macht oder verbietet und durch die die Sicherheit von Produkten, Systemen und Diensten beeinträchtigt würde, die unsere Kunden nutzen, seien es Privatpersonen oder Geschäftskunden. Wir bieten AWS-Kunden als eine von vielen Standardsicherheitsfunktionen zuverlässige Verschlüsselungstechnik an und geben ihnen die Möglichkeit, ihre Verschlüsselungsschlüssel selbst zu verwalten. Wir veröffentlichen Dokumente zu bewährten Sicherheitsmethoden auf unserer Website und ermutigen unsere Kunden, mithilfe dieser Verfahren sensible Inhalte zu schützen.

Wir sind Mitglied in zahlreichen Vereinigungen zum Schutz von Privatsphäre und Datensicherheit. AWS besitzt zudem mehrere international anerkannte Zertifizierungen und Akkreditierungen, die eine Einhaltung der Richtlinien für die Prüfung durch externe Dritte nachweisen. AWS-Kunden haben die Kontrolle über ihre Inhalte und deren Speicherort. "

https://aws.amazon.com/de/compliance/amazon-information-requests/, 03.04.2018

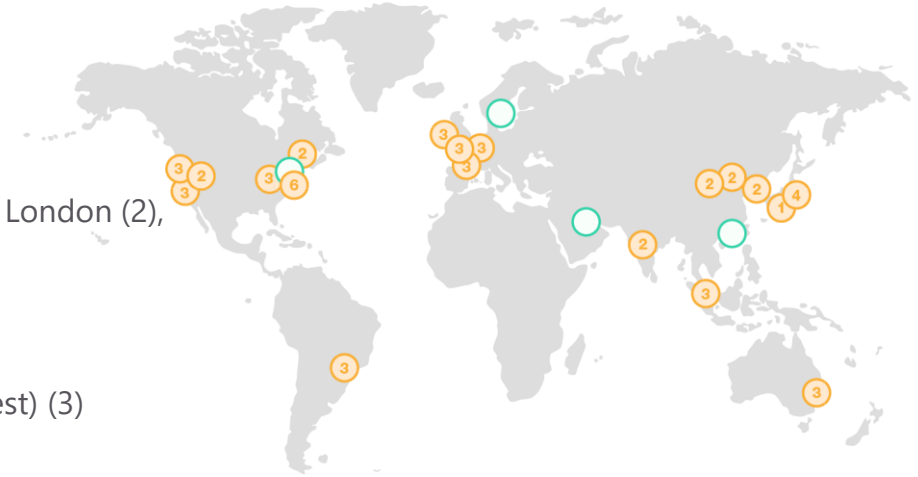
AWS – Infrastruktur

AWS-Regionen und Availability Zones (Verfügbarkeitszonen)

*„Im Zentrum der AWS Cloud-Infrastruktur stehen **Regionen** und **Availability Zones** (Verfügbarkeitszonen, "AZs"). Die AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die mit geringer Latenz, hohem Durchsatz und hochredundanten Netzwerken miteinander verbunden sind. Diese Availability Zones bieten AWS-Kunden eine einfachere und effektivere Möglichkeit, **Produktionsanwendungen** sowie **Datenbanken** zu entwickeln und zu betreiben, die verglichen mit herkömmlichen Infrastrukturen mit einem oder mehreren **Rechenzentren** hochverfügbar, fehlertolerant und skalierbar sind. Die AWS Cloud ist in **54 Availability Zones in 18 geografischen Regionen** weltweit verfügbar."*

Region und Anzahl der Availability Zones

- USA Ost
  Nord-Virginia (6), Ohio (3)
- USA West
  Nordkalifornien (3), Oregon (3)
- Asien-Pazifik
  Mumbai (2), Seoul (2), Singapur (3), Sydney (3), Tokio (4), Osaka-Lokal (1)
- Kanada
  Zentral (2)
- China
  Peking (2), Ningxia (2)
- Europa
  Frankfurt (3), Irland (3), London (2), Paris (3)
- Südamerika
  São Paulo (3)
- AWS GovCloud (US-West) (3)



https://aws.amazon.com/de/about-aws/global-infrastructure/, 04.03.2018

VIELEN DANK

Disclaimer

Alle Angaben dieser Präsentation sind freibleibend.

Inhalte sind nach aktuellem Planungs- und Entwicklungsstand erstellt worden und können sich jederzeit ändern.

Insbesondere Zeitangaben beziehen sich auf die aktuellen Planungen, Anforderungen und Ressourcenverfügbarkeit. Sollten sich die genannten

Parameter ändern, behalten wir uns vor, die Termine entsprechend anzupassen.

Die Überlassung der Präsentation erfolgt nur für den internen Gebrauch des Empfängers.