colada®

Confidential

Version 2.2 - 2019

IT & Security Briefing

Kern Fakten

HR und Governance

- Für alle Mitarbeiter
- Spezielles, regelmässiges Informationssicherheits-Training
- Strikte Vertraulichkeit der Kundendaten
- Strikte Kündigungsrichtlinie mit sofortiger Sperrung aller Zugangsdaten
- Disziplinarmaßnahmen bis zur Kündigung bei Verstössen
- Designierter interner Datenschutzbeauftragter

R & D-Methodik

- Codeüberprüfung vor Implementierung
- Strenges semantisches Versionierungs- und Versionskontrollsystem
- Änderungsmanagementprozess
- Tests in dedizierter Testumgebung (gleicht den Produktionssystemen)

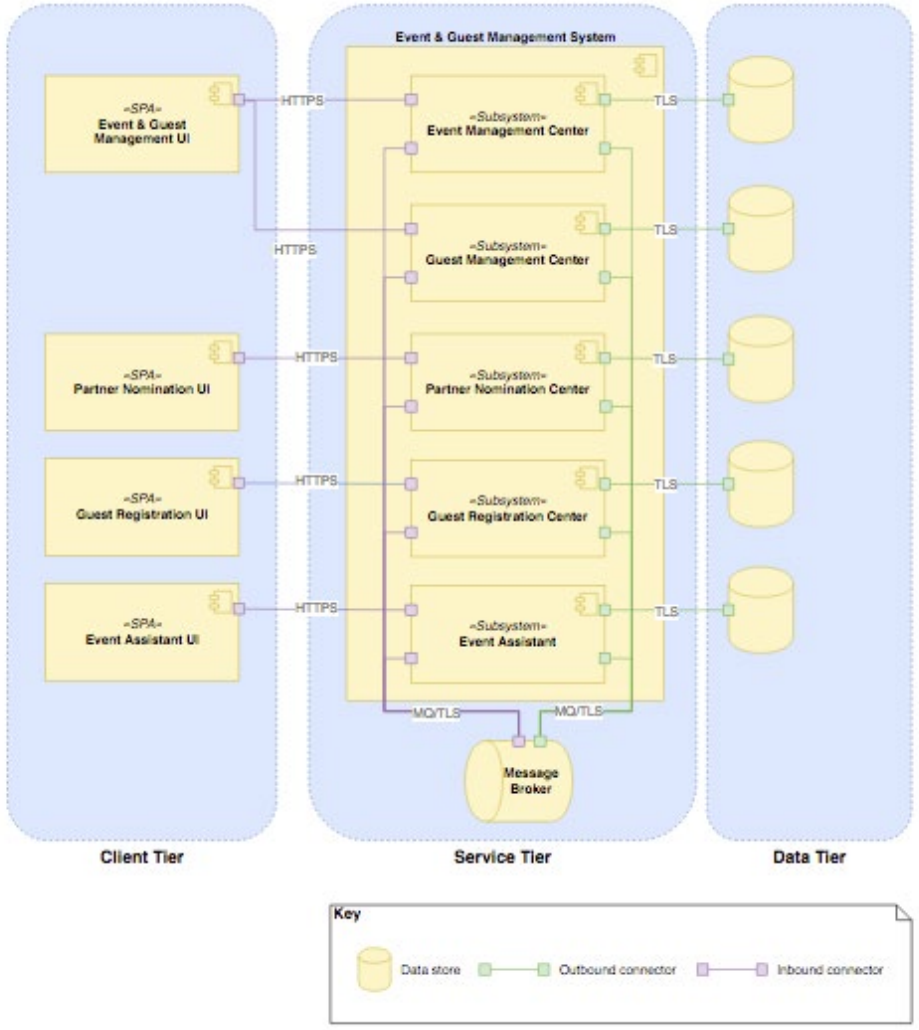
Datenprivatsphäre

- In-App-Datenschutzerklärung
- Kundenspezifische Nutzungsbedingungen und Datenschutzrichtlinie
- GDPR / DSGVO konform
- Flexibler Ort für das Hosting von Daten gemäß den Kundenrichtlinien

Notfallwiederherstellung und Geschäftskontinuität

- Notfallwiederherstellung und Business Continuity-Plan verfügbar
- Tägliches Backup an einem externen Standort
- Service Level Agreement (SLA) verfügbar

Architektur



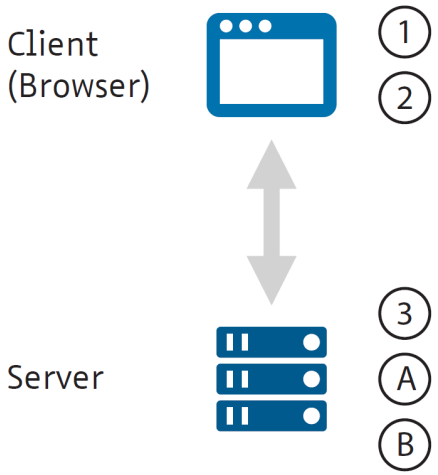
Allgemeine Architektur

- Cloud basierte Infrastruktur / Google Could Engine (Kubernetes)
- Skalierbare Hochverfügbarkeitsarchitektur
- MongoDB-Datenbanken (3 Node Replica Set / Data Encryption at Rest)
- Elasticsearch-Engine
- Microservice Anwendungsarchitektur
- TLS gesicherte Kommunikation zwischen allen Services
- NGINX-Frontend-Controller
- Alle Kommunikation mit dem Kunden durch min. 128bit SSL

Vorteile des Containerkonzeptes (Docker)

- Vereinfachung der Konfiguration
- Produktivität der Entwickler
- Server-Konsolidierung
- Vereinfachtes Code-Pipeline-Management
- App-Isolierung
- Containerbasiertes privates Netzwerk
- Schnelle Bereitstellung

Datenerhebung, -transfer & Speicherung



Datensammlung

1. Import aus Tabellen über das colada-Backend oder manuelle Erstellung im Backend

2. Daten, die von Gästen während der Registrierung eingegeben werden

3. Automatisierter Datenaustausch mit Drittanbieteranwendungen über die colada- API

Datenspeicherung

A Cloud Storage – gehostet in Deutschland / Replication in definierten Regionen möglich

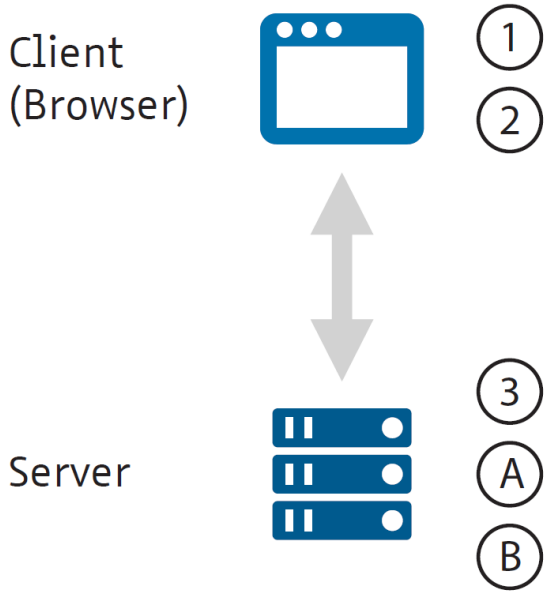
B Client-Installation vor Ort (erfordert SSH-Zugriff von colada)
colada stellt im Rahmen der Verantwortlichkeiten die Konsistenz, Verfügbarkeit und Sicherheit der Datenverarbeitung sicher. Dies umfasst die Betriebskontinuität, Zugriffsmanagement, Löschfristen (definierbar gemäss Anforderungen) sowie Möglichkeiten zur Änderungsverfolgung und dem erfassen von Useraktivitäten(bspw. Exporte).

Data Encryption at Rest, gesicherte Datenbankzugriffe mit dedizierten Key für jeden Mandanten

Datentransfer

Alle zwischen Client und Server, sowie innerhalb der Microservices, übertragenen Daten werden über SSL/TLS verschlüsselt.

Datenerhebung



- colada erhebt, speichert und verarbeitet nur die zum Zwecke der Vertragserfüllung nötigen Benutzer- und Abrechnungsdaten.
- Art, Umfang und Verarbeitungszweck der darüber hinaus erfassten, verarbeiteten und gespeicherten Daten obliegen dem Nutzer.
- Hinsichtlich der Datenverarbeitung im Auftrag schliesst colada mit dem Auftraggeber einen spezifischen ADV-Vertrag
- Ein Mustervertrag steht im Community Bereich unter www.colada.info bereit.

Betrieb & Support

Alarme & Anfragen

colada empfängt Alarme und Anfragen von den internen Überwachungssystemen sowie von internen und externen Benutzern.

Support für Anwendungen und Systemadministration

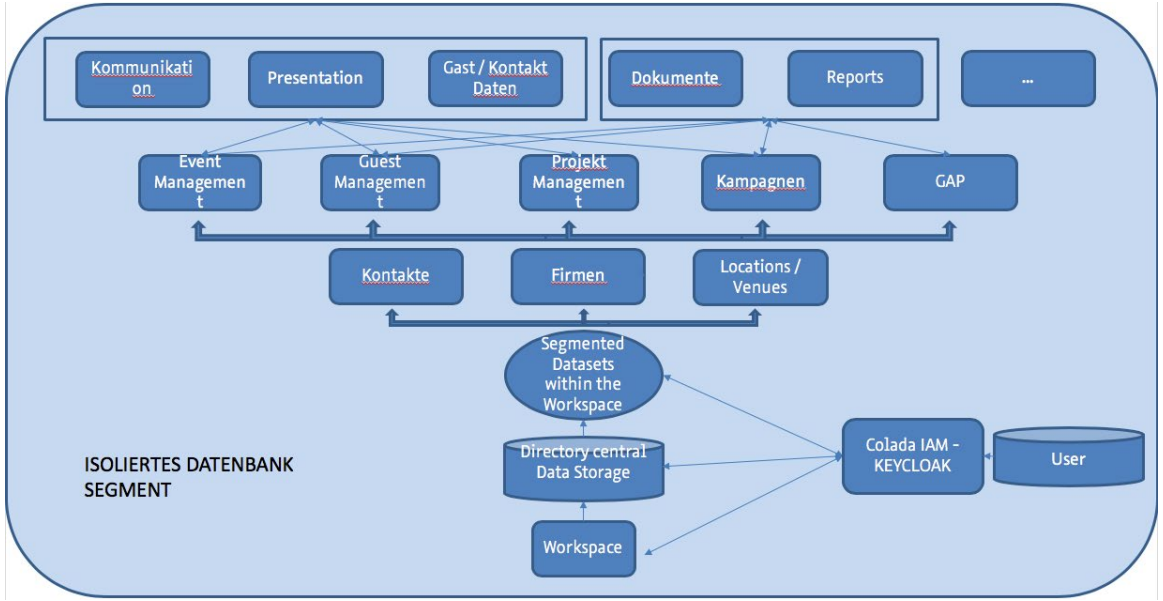
1. Stufe: Service Desk macht Alarmierung / Anfrage
2. Stufe: behandelt Anwendungsfragen, Funktionen und Funktionen
3. Stufe: (technischer Support) behandelt Probleme und Fehler
4. Stufe: (Entwicklung und Infrastruktur), aus 3. Ebene eskaliert

Service Desk-Prozess

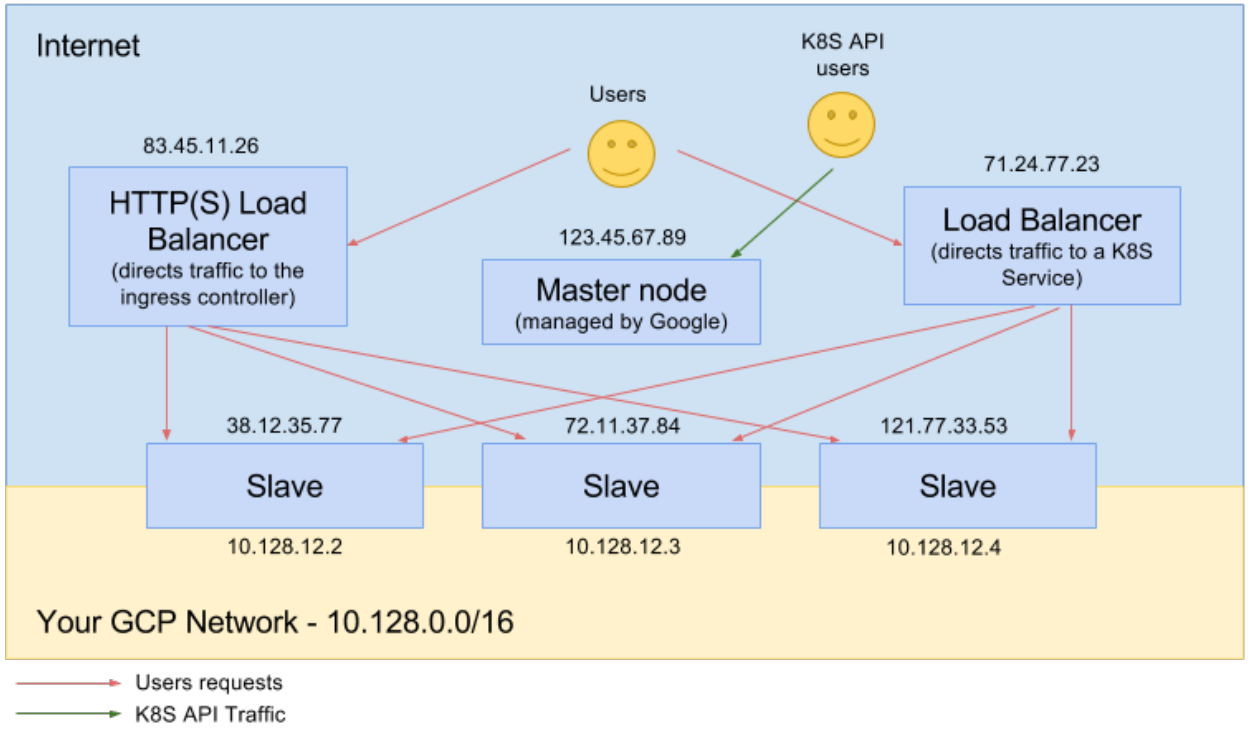
- Serviceanfragen werden zentral vom Serviceteam verwaltet
- Benutzer- / Kundenschnittstelle per Telefon / Online - erhält ein Serviceticket
- Triage auf der 1. Ebene (SLA, benutzerdefiniertes Projekt usw.)
- Feedback und Lösung nach vorheriger Absprache und Vereinbarung

Applikationsbereitstellung

Grundlegendes Applikationsmodell



Basisschema Bereitstellung via Kubernetes



Applikationsbereitstellung

- Die Applikation wird mittels Google Coud Engine bereitgestellt
- Applikationshosting: Region Zurich/Switzerland
- Datenspeicherung:
  - Schweiz: Region Zürich
  - Deutschland: Frankfurt
- Daten logisch segregiert:
  - 1 Workspace per client
  - Datenspeicherung nur innerhalb des Workspaces
- colada verpflichtet keine weitere Subdienstleister mit Datenverarbeitungsaufgaben

Datenaufbewahrung und Wiederherstellung

- Die Daten, die von den colada-Benutzern und Gästen beim Import oder bei der Registrierung eingegeben werden, gehören dem Benutzer.
- colada erstellt regelmäßig, automatisiert, verschlüsselte Sicherungen der aktuellen Datenbanken um die Verfügbarkeit des Dienstes sicherzustellen (diese Sicherungen werden für maximal 30 Tage aufbewahrt).
- colada speichert die Informationen für den Zeitraum, der erforderlich ist, um die Zwecke der entsprechenden Dienstleistungen und Events sowie gesetzliche Aufbewahrungsfristen zu erfüllen.
- Nach Ablauf der durch den Kunden oder den Zweck bedingten Haltezeiten, löscht colada die kunden- bzw. eventspezifischen Daten.
  Bei Bedarf wird ein Löschungszertifikat für die Löschung ausgestellt.

Zugriffsteuerung

- Das Standard-Authentifizierungskonzept basiert auf einem persönlichen Aktivierungscode, der per E-Mail an den Benutzer gesendet wird, der ein colada-Konto beantragt.
- Die Rechte- und Rollenverwaltung erfolgt innerhalb der Applikation auf Workspace-, Lizenz-, Modul-, Projekt und Userebene
- Eine Datensegmentierung innerhalb eines Workspaces kann auf Userebene für Kontakte, Organisationen, Lokationen, Kampagnen und Events vorgenommen werden.
- Auf Anfrage sind zusätzliche Integrationslösungen für Unternehmen in eingebundener oder Single Sign-On-Umgebung (SSO) verfügbar.
- Zusätzliche In-App-PID-Authentifizierung für Gäste (Consumer) kann hinzugefügt werden.
- Innerhalb der bereitgestellten Formulare kann die Sichtbarkeit und Bearbeitbarkeit von Informationen eingeschränkt werden.

Software Stack

Software Komponenten

- Keycloak
- Vault
- Java - JRE 8u192
- Java Script
- Consul (Service Discovery)
- Rabbit MQ
- Elastic Search
- Froala Editor (3rd Party License)
- Itext (3rd Party License)
- Mongo DB >= 3.6
- Jenkins Puppet und Maven für provisioning CI/CD- Pipeline
- Grafana / Logstash für metrics und health Information des Application Monitoring
- Hazelcast

Libraries

- React.js
- React redux
- Material UI
- jQuery

Lebenszyklus, Betrieb & Wartung

- Kernsystementwicklung und kundenspezifische Entwicklung basierend auf agilen Entwicklungsprozessen.
- Das Ecosystem wird ständig mit den neuesten Updates und Korrekturen aktualisiert. (CI/CD Pipeline)
- Etappenweise Veröffentlichung von Features und Fixes (Entwicklung, Test, Pre-Produktion und Produktion) durch das gesamte Ökosystem inkl. identischer Infrastrukturen für Pre-Produktions- und Produktionssystem.
- Neue Funktionen und Fehlerbehebungen können nach durchlauf aller Phasen und der Qualitätssicherung auf der Pre-Produktionsumgebung getestet und dann in der Produktionsumgebung freigegeben werden.

Auditing und Zertifizierungen

- colada führt laufend 3rd party Audits im Zusammenhang mit Kunden durch. Darin enthalten sind neben spezifischen Tests auch Penetrationtest nach den Kriterien des Kunden
- Bis Ende 2019 ist die Zertifizierung von colada nach ISO27001 voraussichtlich abgeschlossen.
- Für Q1/2020 ist die TISAX Zertifizierung in Vorbereitung, welche auf ISO27001 aufbaut.

Contacts

Questions, enquiries, abuse and vulnearbility disclosure: infosec@colada.biz

colada

Product management

Frank Zander

Frank.zander@colada.biz

+41 52 632 06 56