ADITO Betriebsmodelle und ADITO Cloud

ADITO Akademie

Version 1.1 | 21.04.2022

Inhaltsverzeichnis

© 2022 ADITO Software GmbH

Dieses Dokument unterliegt urheberrechtlichem Schutz. Sie dürfen die Inhalte für den vorgesehenen Zweck wie z.B. eine ADITO Schulung oder ein ADITO Projekt nutzen (insbesondere auch speichern und vervielfältigen), aber nur nach Absprache mit ADITO verändern, an Dritte weitergeben, veröffentlichen oder für andere Zwecke verwenden.

Version	Änderungen
1.1	Erweiterung um Architekurkonzept ADITO Cloud C1
1.0.2	Errata
1.0.1	Neue Grafiken
1.0	Initiale Erstellung

1. Vorwort

Der Markt zeigt, dass Unternehmen sich weniger mit dem Betrieb einer Software auseinandersetzen möchten und daher Lösungen präferieren, die Out-of-the-box funktionieren.

Hierzu zählen vor allem Cloud Lösungen wie unsere ADITO Cloud, die für den Kunden keinerlei Betriebsaufwand erzeugen. Das Pendant für Kunden, die ihre Systeme On-Premise betreiben möchten, bietet unsere ADITO Appliance Lösung. Des Weiteren sind für den On-Premise-Betrieb weitere Betriebsmodelle auf Basis der Kubernetes-Cluster-Plattform oder DOCKER Containern möglich.

Zum Stand 01.12.2021 betreibt die ADITO Software GmbH in ihrer eigenen Cloud-Infrastruktur ca. 500 ADITO Systeme (mit kontinuierlichem Wachstum). Insgesamt werden Clusterressourcen in der Dimension von ca. 1.000 CPUs, 5 TB RAM und 50 TB SSD Storage für unsere Kunden und Partner bereitgestellt.

© 2022 ADITO Software GmbH

2. Überblick Betriebsmodelle ADITO

Alle Betriebsmodelle bieten die Vorteile einer leicht skalierbaren Lösung unabhängig davon, ob sich das Kundensystem in der Cloud betreiben lässt oder der Kunde diese selbst in seinem (eigenen) Rechenzentrum hostet.

Wir empfehlen ausdrücklich die Nutzung der Betriebsmodelle ADITO Cloud oder ADITO Appliance mit Full Application Support für On-Premise-Lösungen, da diese auf dem Software-as-a-Service-Ansatz basieren und für unsere Kunden “einfach funktionieren”.

Die alternativen Betriebsmodelle für einen individuellen Betriebs auf Kubernetes-Cluster-Plattform oder DOCKER Containern benötigten ein hohes Maß an praktischer Erfahrung und Kompetenz. Die Verantwortung für die Implementierung der Betriebsumgebung, Betrieb und Service kann hierbei nicht von ADITO übernommen werden und obliegt folglich dem Kunden.

		Verantwortung und Kompetenz				
	Betriebsmodelle	ADITO Cloud	On-Premise ADITO Appliance mit Full Application Support	On-Premise ADITO Appliance	On-Premise Kubernetes Cluster mit ADITO	On-Premise Container Plattform mit ADITO
	Hardware/ Infrastruktur	A	K	K	K	K
Bestandteile der Betriebsumgebung	Services					
Datenbank	Datenbank Service	A	K & A	K & A	K	K
ADITO Applikation	ADITO Service	A	A	K & A	K	K
Index	Solr Service	A	A	K & A	K	K
Workflow	Flowable Service	A	A	K & A	K	K
E-Marketing-Mail-Editor	Mosaico Service	A	A	K & A	K	K

Legende Abkürzungen zu Verantwortung und Kompetenz:

A = ADITO | K = Kunde | K & A = Kunde primär & ADITO mitwirkend

Abbildung 1. Betriebsmodelle - Infrastruktur und Bestandteile der Betriebsumgebung

© 2022 ADITO Software GmbH

3. Leistungen für Hochverfügbarkeit und Skalierbarkeit

Der hochverfügbare und skalierbare Betrieb des ADITO Systems für seine Anwender wird durch Leistungen im Kontext von IT-Strategie, Support und Service, sowie Health und Status möglich.

Diese Leistungen sind Bestandteil der Betriebsmodelle ADITO Cloud und ADITO Appliance mit Full Application Support und werden durch ADITO sichergestellt.

Bei den Betriebsmodellen auf Basis Kubernetes-Cluster-Plattform oder DOCKER Containern sollten diese Leistungen ebenfalls sichergestellt sein und obliegen hier dem Kunden.

	Verantwortung und Kompetenz				
Betriebsmodelle	ADITO Cloud	On-Premise ADITO Appliance mit Full Application Support	On-Premise ADITO Appliance	On-Premise Kubernetes Cluster mit ADITO	On-Premise Container Plattform mit ADITO
Health und Status					
Monitoring	A	A	K (A)	K	K
Baselining	A	A	K (A)	K	K
Zentrales Logging	A	A	K (A)	K	K
Support und Service					
Bereitschaft	A	A	K	K	K
Reaktionszeiten	A	A	K	K	K
Offsite Backup	A	A	K (A)	K	K
Alarmierung	A	A	K (A)	K	K
Desaster Recovery Strategie	A	A & K	A & K	K	K
Strategie/ Umgebungs-Design					
Bare Metal Umgebung	A	K	K	K	K
Betriebssystem Wartung	A	A	K (A)	K	K
Anbindung an Drittsysteme durch VPN Container	A & K	A & K	A & K	K	K

Legende Abkürzungen zu Verantwortung und Kompetenz:

A = ADITO | K = Kunde | K (A) = Kunde und optionale Mitwirkung ADITO

A & K = ADITO primär & Kunde mitwirkend | K & A = Kunde primär & ADITO mitwirkend

Abbildung 2. Betriebsmodelle - Leistungen

© 2022 ADITO Software GmbH

4. Architekturkonzept ADITO Cloud

Die Architektur der ADITO Cloud hat den Anspruch, sich stark an den Empfehlungen der Cloud Native Computing Foundation zu orientieren. Dazu zählen verteilte Services, resiliente Container und ein hoher Automatisierungsstandard zur Sicherstellung von Prozessen und Minimierung von Fehlern durch manuelle Eingriffe.

Die ADITO Cloud wurde nach dem Design Pattern Infrastructure-as-Code entworfen. Alle Komponenten sind in einer Beschreibungssprache definiert und werden über diese entsprechend bereitgestellt. Das Modell beschreibt auch alle Um-Komponenten wie Storage, Firewalls oder Jump-Host-Mechanismen. Die Architektur lässt sowohl horizontale als auch vertikale Skalierung zu. Alle relevanten Komponenten (wie Server, Switches, etc.) sind mindestens 2-fach-redundant ausgelegt.

Architekturdiagramm ADITO Cloud (C1)

Die ADITO Cloud (C1) wurde aus den Erfahrungen der letzten Jahre Clusterbetrieb komplett neu gedacht und aufgebaut. Ziel war es ein größtmögliches Maß an Sicherheit, Verfügbarkeit und Performance zu bieten. Die Umgebung ist komplett dediziert aufgebaut und wird in einem ISO-27001-zertifizierten Rechenzentrum betrieben.

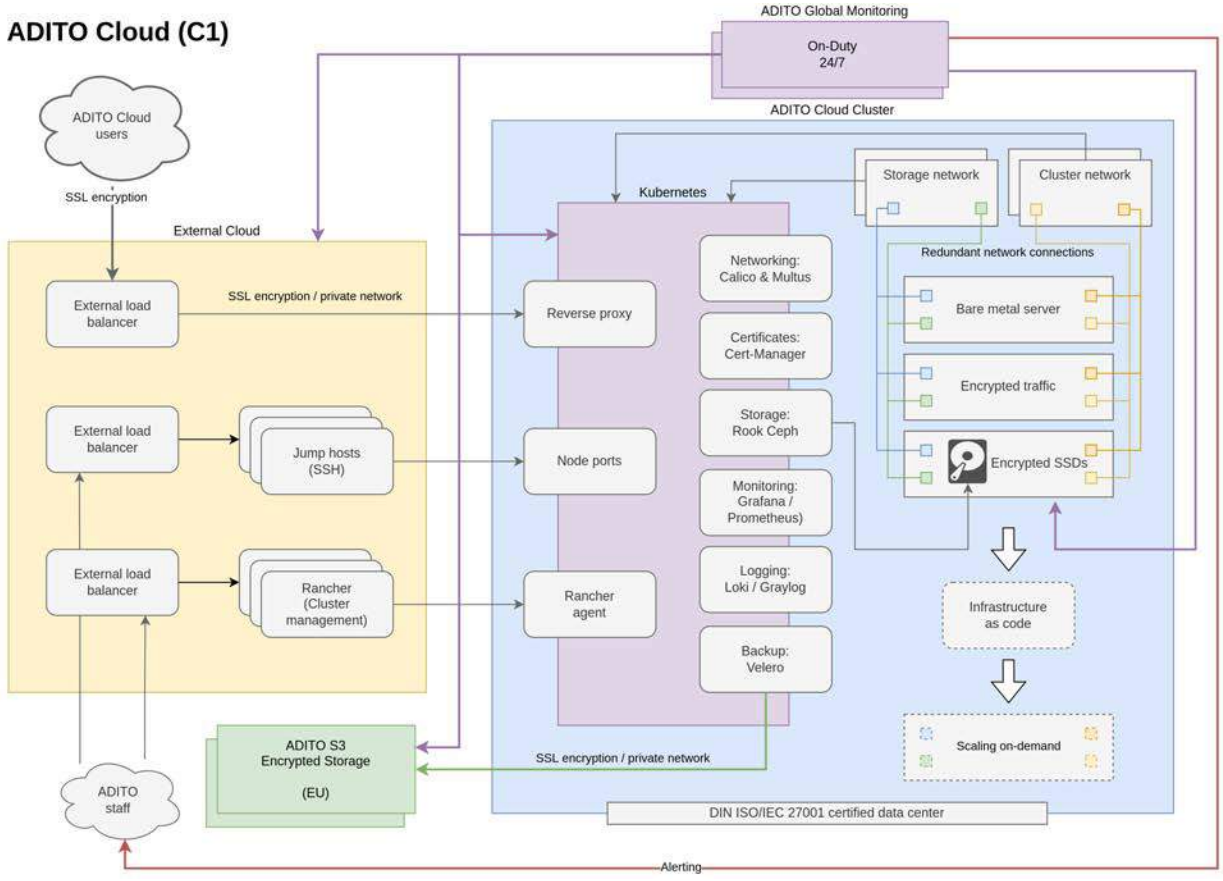

Abbildung 3. Architektur ADITO C1-Cluster

Infrastruktur

Die gesamte Infrastruktur wird auf sogenannten „Bare Metal Servers“ betrieben. Wir bedienen uns keiner Cloud-Services wie z. B. AWS oder GKE. Dadurch stellen wir sicher, dass wir jederzeit für die gesamte Infrastruktur die Hoheit innehalten. Die Skalierung dieser Bare-Metal-Infrastruktur geschieht automatisiert mit klassischen, aus dem Cloud-Nativ Umfeld bekannten, Tools (wie Terraform und Ansible). Manuelle Eingriffe finden an der Infrastruktur im Regelbetrieb nicht statt.

Für unsere Systeme wird auf Clusterebene eine HA Infrastruktur (HA = High availability) betrieben. Auf Namespace/Kundenebene wird eine sogenannte „resiliente Infrastruktur“ genutzt. Dies bedeutet, dass viele Komponenten nicht redundant ausgelegt sind, jedoch so strukturiert sind, dass das System Probleme selbst erkennt und entsprechende Services z.B. neugestartet oder neu initialisiert werden. Dies führt zu einem "selbstheilenden" System, wodurch selbst im Fall einer Störung diese i.d.R. < 10 Minuten ohne Eingriff gelöst wird.

Bei Bedarf kann auf Namespace/Kundenebene ebenfalls eine HA Struktur verwendet werden: Hierbei werden 3 Datenbanknodes (die sich in einem Clusterverbund befinden) betrieben und alle betriebsrelevanten Rollen stehen in mehrfacher Redundanz (mind. 3) zur Verfügung.

Sicherheit der Umgebung

Jegliche Kommunikation des internen Clusters läuft auf eigener Hardware, die isoliert von außen und zudem transportverschlüsselt stattfindet. Alle Server sind gehärtet und kein Server ist vom Internet direkt erreichbar. Für den Zugang werde spezielle Jump-Hosts genutzt.

Zugriffe auf ADITO Cloud Systeme werden zur Lastverteilung in der ersten Phase durch einen Load Balancer gesteuert. Im Load Balancer finden auch diverse Schutzmaßnahmen gegen unter anderem DoS- und DDoS-Attacken statt. Lediglich der Load-Balancer kann direkt mit den Nodes kommunizieren und den Traffic (VPN und HTTPS) zu den Nodes durchleiten. Entsprechende Maßnahmen wie Zugangskontrollen sind implementiert.

Es gibt darüber hinaus ein strenges AUDIT-Verfahren, das auffällige Aktivitäten auf den Nodes überwacht und im Fall des Eintretens entsprechend alarmiert. Für die Infrastruktur existieren Standardmaßnahmen zur DDoS-Erkennung wie auch ein IDS (Intrusion Detection System).

Im nächsten Schritt erreichen die Zugriffe unsere Reverse Proxys (aktuell betreiben wir hier rund 25 Stück). Diese sorgen dafür, dass nur definierter Verkehr über 443/https an die Cloud Server geroutet wird. Auf den Cloud Servern selbst schützt zusätzlich eine Firewall vor unautorisierten Zugriffen. Alle Cloud Server sind entsprechend gehärtet und lassen nur Maintenance-Zugänge mit Zertifikat zu.

Isolierung und Authentifizierung

Innerhalb der Cluster-Infrastruktur bedienen wir uns des Best-Practice-Ansatzes der Namespace

© 2022 ADITO Software GmbH

Isolierung. Jedes System wird hierbei in einem eigenen Bereich gekapselt und so durch Netzwerkisolierung von anderen Systemen getrennt. Jedes Kundensystem wird in einem eigenen “Ökosystem” (d.h. mehrere Systeme wie Development, Test, Produktiv mit jeweils eigenen Datenbanken) in einem eigenen Namespace mit isoliertem Netzwerkbereich betrieben. Ein Zugriff kann innerhalb des Namespaces durch DNS-Auflösung gesteuert werden. Somit isolieren wir nicht nur Kunden von Kunden, sondern auch Stages von Stages und schaffen damit ein hohes Maß an Isolation, was den Schutz von Daten und Umgebungen stark erhöht.

Um Verbindungen ins eigene Unternehmen bzw. zu anderen externen Rechenzentren aufzubauen, unterstützen wir entsprechend die IPSec-VPN-Verbindung. Über diese können problemlos andere Systeme angebunden werden. Als Fallback bieten wir gegen Aufwand SSH Tunnel und OpenVPN als Pfad an. Neben den klassischen Authentifizierungsmethoden (LDAP, Kerberos, AD) steht auch eine OAuth-2.0-Authentifizierung zur Verfügung (z.B. für Anmeldungen über Azure AD).

Ausfallsicherheit

Unser Cluster stellt ein verteiltes, mehrfach redundantes Speichernetzwerk bereit. Dies stellt sicher, dass ein Ausfall von bis zu 40 % der Disk Storage zu keinem Verlust von Daten führt.

Unsere Cluster werden durch extra gesteuerte, verteilte Lasttests geprüft. Dies findet durch automatisierte Browser-Umgebungen mit entsprechenden Cloudressourcen statt. Wir sind durch entsprechende Cloud Skalierung in der Lage, bis zu 1.000 zeitsimultane Zugriffe auf ein System zu simulieren. Zugriffe finden i.d.R. nie zeitsimultan statt. Die Zugriffe bilden in etwa das Geschehen einer Last von bis zu 30.000 Usern im Regelbetrieb ab.

Wir prüfen stetig neue Technologien auf die Robustheit zur Steigerung unserer Ausfallsicherheit. Diese Arbeiten finden in einem separiertem Test-Cluster statt. In diesem Test-Cluster werden auch bewusst Ausfälle provoziert und ausgewertet. Ergebnisse werden mittels Staging-Verfahren zuerst in den Sekundär-Cluster übernommen, bevor sie final im Haupt-Cluster zum Einsatz kommen.

Notfallkonzept

Unser vollständig ausgearbeitetes Notfallkonzept bietet eine Orientierung im Ausnahmezustand und gibt zu definierten Ausfallstufen feste Prozesse und Maßnahmen vor. Zu allen Ausfall- und Desaster-Szenarien wurden ausführliche Failover-Tests und Desaster-Recovery-Tests durchgeführt.

Final bildet unsere Cloud-Disaster-Recovery-Strategie den Bereich eines Totalverlustes ab. Hier kann auf nächtliche Backups aller Cloudsysteme (die sich an einem anderen Standort befinden) zugegriffen werden, um ein System in einem anderen Cluster wiederherzustellen (aktuell betreibt ADITO vier unabhängige Cluster).

© 2022 ADITO Software GmbH

Stufe 1: Ausfall bis zu 20 % der Clusterinfrastruktur und maximal 33 % Ausfall der etcd und controlplane Nodes.

- Eintrittswahrscheinlichkeit: höchstwahrscheinlich
- Durch entsprechende Dimensionierung unseres Clusters und die Pufferung entsprechender Ressourcen ist bei diesem Szenario keinerlei Beeinträchtigung zu erwarten.
- Das Szenario unterliegt einem generellen Betriebsrisiko. Durch Redundanz und LoadBalancer wird eine Kundenbeeinträchtigung ausgeschlossen.

Stufe 2: Ausfall von über 20 % aber weniger als 40 % der Clusterinfrastruktur und maximal 33 % Ausfall der etcd und controlplane Nodes.

- Eintrittswahrscheinlichkeit: unwahrscheinlich
- Je nach Clusterauslastung kann es zu einer kurzen Beeinträchtigung beim Kunden kommen.
- Die Ausfalldauer wird höchstwahrscheinlich unter 10 Minuten betragen.

Stufe 3: Ausfall von über 20 % aber weniger als 40 % der Clusterinfrastruktur und mehr als 33 % Ausfall der etcd und controlplane Nodes.

- Eintrittswahrscheinlichkeit: unwahrscheinlich
- Je nach Clusterauslastung kann es zu einer längeren Beeinträchtigung beim Kunden kommen.
- Unter Umständen müssen einzelne Systeme gestoppt werden. Dies betrifft lediglich Demo- und/oder Testsysteme.
- Die Ausfalldauer wird höchstwahrscheinlich unter 30 Minuten betragen.

Stufe 4: Ausfall von mehr als 40 % der Clusterinfrastruktur und mehr als 33 % Ausfall der etcd und controlplane Nodes.

- Eintrittswahrscheinlichkeit: höchstunwahrscheinlich
- Es wird zu einer längeren Beeinträchtigung beim Kunden kommen.
- Einzelne Systeme müssen gestoppt werden. Dies Betrifft voraussichtlich Demo-, Test-, Dev- und/oder QA-Systeme.
- Die Ausfalldauer wird höchstwahrscheinlich unter 60 Minuten betragen.

Stufe 5: Komplettausfall der Clusterinfrastruktur.

- Eintrittswahrscheinlichkeit: höchstunwahrscheinlich
- Es wird zu einer längeren Beeinträchtigung beim Kunden kommen.

© 2022 ADITO Software GmbH

- Die Ausfalldauer wird ursachenabhängig bis zu 4 Stunden betragen.

Stufe 6: Totalverlust einer RZ Site.

- Eintrittswahrscheinlichkeit: denkbar, aber nahezu ausgeschlossen
- Es wird zu einer längeren Beeinträchtigung beim Kunden kommen.
- Die Ausfalldauer wird ursachenabhängig bis zu 14 Stunden betragen.

© 2022 ADITO Software GmbH

5. Betriebskonzept ADITO Cloud

Der Betrieb der Umgebung findet einzig durch die IT-Abteilung der ADITO Software GmbH statt. Die Betriebsumgebung und das Rechenzentrum sind für einen Tier-3-Betrieb skaliert.

Verfügbarkeit

Der Betrieb der ADITO Cloud ist für 99,99 % Verfügbarkeit und 24/7 ausgelegt. Unsere Systeme erreichen bereits eine Verfügbarkeit von > 99,80 % (aktuell 99,98 %/garantiert 99,50 %).

Bereitschaft

Der Bereitschaftsdienst der ADITO IT stellt sicher, dass bei Störungen 24/7 eine Reaktion binnen 15 Minuten erfolgt. Die Alarmierung erfolgt durch unsere Monitoring Infrastruktur und stellt sicher, dass wir schnellstmöglich im Störungsfall reagieren können. Der Großteil der Störungen, die in der Bereitschaft abgearbeitet werden, haben keine Auswirkung auf das Kundensystem und sind proaktive Eingriffe, um den HA Status unserer Umgebung beizubehalten. Auch im „Worst-Case“ steht der Bereitschaftsdienst der ADITO IT bereit und greift schnellstmöglich ein. Diese Eingriffe sind jedoch äußerst selten.

Monitoring

Zur Sicherstellung der Betriebsumgebung findet ein großflächiges, proaktives Monitoring der Umgebung statt. Hierfür werden rund 2,4 Millionen Metrikpunkte erfasst und in Echtzeit ausgewertet, um den Zustand unseres Clusters und der einzelnen Kundensysteme zu überwachen und ein Baselining durchzuführen.

Die erfassten Werte dienen primär der proaktiven Erkennung und der direkten Verbindung zum Bereitschaftsdienst, den die ADITO allen Cloud Kunden im Standard zur Verfügung stellt. Beim Eintritt eines clustergefährdenden Events (auch vorsorglich, z.B. Ausfall einer Node) wird die Bereitschaft alarmiert und veranlasst entsprechend weitere Schritte. Für den Fall einer Störung im Clusterumfeld erstellt die ADITO IT immer eine Post-mortem-Analyse, um die Ursache zu identifizieren und ggf. Marker zur Früherkennung zu setzen.

Backup und Georedundanz

Die Datensicherung findet mithilfe von Snapshots und Point-in-Time-Backups (mind. 1x täglich, auf Wunsch ist bis zu alle 2 h möglich) statt. Diese Sicherung umfasst die gesamte Datenbank des ADITO Kundensystems. Die Backups werden verschlüsselt im lokalen Umfeld erstellt.

Als kostenfreie Option können regelmäßig (mindestens täglich) Backups georedundant im EU-Raum (die Off-Site befindet sich in Helsinki) verteilt werden. Im Verlustfall kann so am georedundanten Backup-Standort der Betrieb von Produktivsystemen mit einer kurzen Anlaufzeit gewährleistet werden.

© 2022 ADITO Software GmbH

Die Anlaufzeit ist abhängig von der Datenmenge der Systeme.

Alle zum Storage-Interface gehörenden Festplatten sind verschlüsselt. Ein Prozess zur Entsorgung von Datenträgern ist vorhanden. Zudem sind die Server mit einer USV-Anlage vor Stromschwankungen und kurzen Stromausfällen geschützt.

Ersatzteilversorgung

Zur Sicherstellung einer schnellen Ersatzteilversorgung und ggf. dem Wechsel von Komponenten arbeiten wir direkt mit dem Rechenzentrum zusammen. Ein Austausch von Komponenten findet 24/7 statt, alle Ersatzteile sind hierfür vor Ort lagernd. Ein Austausch ist damit i.d.R binnen 30 Minuten möglich. Ein Ausfall von Komponenten ist jedoch durch das High-Availability-Konzept nicht von Belang.

© 2022 ADITO Software GmbH

6. Betriebskonzept ADITO Appliance

Die ADITO setzt aktuell für onPremise Kunden eine Möglichkeit um, welche einen vergleichbaren Funktionsumfang analog der ADITO Cloud anbieten wird. Technologisch ist die Appliance auf den gängigen Hypervisoren einsetzbar, darunter fallen unter anderem: Hyper-V, ESXi und Proxmox.

Der Kunde stellt in diesem Fall den Betrieb der Hypervisoren sicher. Die ADITO Appliance besteht aus mindestens 3 VMs mit je 8 Cores und 32 GB RAM. Der Plattenplatz ist abhängig von der zu erwartenden Datenmenge. Die Disc kann hyperkonvergent durch einen ceph Objektspeicher durch die Appliance bereitgestellt werden oder extern angebunden sein. Es gibt hier jedoch gewisse Merkmale zu erfüllen. Im Speziellen ist dies neben einer Latenz < 1 ms auch die Möglichkeit Filesysteme zu mounten (z.B. NFS), ein reiner Blockspeicher reicht nicht aus.

Für Early-Adapters wird voraussichtlich Q2/2022 die Möglichkeit zum Produktiveinsatz bestehen. Weitere Zeitpläne sind – Stand heute – noch zu vage.

© 2022 ADITO Software GmbH

7. Leistungsbeschreibung der ADITO Cloud

ADITO stellt dem Kunden während der Vertragslaufzeit die Software ADITO in der jeweils aktuellen Version sowie alle notwendigen Updates und Patches auf von ADITO betriebenen Servern zur Verfügung.

Dabei übernimmt ADITO folgende Leistungen:

a. Betrieb der Software ADITO auf Servern in Deutschland gemäß Abs. 3 DSGVO
b. Einrichten und Betrieb einer kundeneigenen Serverinstanz
c. Zur Verfügung Stellung von 2 GB Server-Festplattenspeicher pro Nutzer
d. SSL-Verschlüsselung der Übertragungswege zwischen Client und Server
e. Sicherung der Software und der Daten des Kunden einmal täglich

Die gewährleistete Verfügbarkeit (Service Level) gilt als erfüllt, wenn folgende Werte im Messzeitraum von einem Kalenderjahr erreicht werden:

Indikator	**Service Level**
Verfügbarkeit der Software in %	99,50 %
Verfügbarkeit der Software in Servicezeit	Mo bis So 00:00 - 24:00 Uhr
Wartungsfenster	Täglich 22:00 - 05:00 Uhr

Zur Messung des Service Levels wird die Verfügbarkeit durch ADITO eigene Prozesse überwacht. Explizit ausgenommen sind hierbei:

- Wartungsarbeiten (angekündigte Wartungsfenster finden i.d.R weniger als 4x jährlich stattfindenund Datensicherungen
- Faktoren, die außerhalb des angemessenen Einflussbereichs von ADITO verursacht wurden
- Zeitweilige Ausfallzeiten von maximal 10 Minuten

© 2022 ADITO Software GmbH

8. Einhaltung von Standards

Die ADITO Cloud orientiert sich in Aufbau und Struktur am BSI C5 Standard. Die ADITO Software GmbH plant hier zukünftig eine Zertifizierung nach diesem Standard.

Die ADITO pflegt einen sehr verantwortungsvollen Umgang mit ihren Kundensystemen und den damit verbundenen Kundendaten. Zur Sicherstellung der Datensicherheit, Datenintegrität und Datenverfügbarkeit sind entsprechende Regelungen in einem Datensicherungskonzept verankert. Dieses gewährleistet unter anderem die verschlüsselte Ablage der Datensicherungen, den Test der Rücksicherungen, ein generelles Backup-Konzept und ein Disaster-Recovery-Sicherungskonzept.

Unser Rechenzentrumsbetreiber ist entsprechend nach ISO 27001 zertifiziert. Des Weiteren stellt unser RZ-Betreiber alle Dienste CO^2 neutral bereit.

© 2022 ADITO Software GmbH

9. DSGVO

ADITO nimmt den Schutz personenbezogener Daten sehr ernst: ADITO schließt mit seinen Kunden grundsätzlich einen Auftragsverarbeitungs-Vertrag nach Art. 28 DSGVO ab, um sicherzustellen, dass die Daten in entsprechendem Maße geschützt sind und räumt dem Auftraggeber diesbezüglich Kontrollrechte ein. ADITO garantiert die Umsetzung der technischen und organischen Maßnahmen nach Art. 32 DSGVO.

Der Hosting Anbieter HETZNER, der von ADITO als Cloud-Anbieter beauftragt wurde, garantiert die Umsetzung der technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO (https://www.hetzner.com/AV/TOM.pdf), die Speicherung der Daten erfolgt innerhalb Deutschlands.

© 2022 ADITO Software GmbH

10. Frequently Asked Questions (FAQs)

Wie sind die Erfahrungswerte hinsichtlich der Laufzeit (Performance der Aufrufe) bei Einbindung von Drittsystemen per Webservice oder Datenbankanbindung, gibt es kritische Themen / Systeme aus der Erfahrung?

Zum Einbinden von Drittsystemen kann ein VPN/Tunnel zum Kunden/Drittsystem aufgebaut werden. Hier haben wir Erfahrungen mit IPsec, SSH-Tunnel und OpenVPN. Mit WireGuard befinden wir uns zum aktuellen Zeitpunkt in der Testphase. Die größte Erfahrung haben wir aktuell mit IPsec und SSH-Tunnel gesammelt. Wichtig ist: Pro SSP-System wird ein VPN benötigt.

Zwischen Cloud-System und Kunden findet dann nochmal ein Nating statt. Das bedeutet, dass nicht automatisch auf den vom Kunden freigegebenen Service (bspw. 192.168.40.10:8080) zugegriffen werden kann, sondern erst die ADITO-IT informiert werden muss, welche den Service vom Kunden unter einem Hostname am Cloudsystem erreichbar macht (bspw. ipsec.systemname.cluster.local:8080).

Die Latenz bei Datenbanken und Networkshares ist stark von der Internetanbindung des Kunden abhängig, auch das verwendete VPN kann hier eine große Rolle spielen. Die ADITO ist hier mit 1 GBit ans Internet angeschlossen. Aktuell konnten wir keine negativen Auswirkungen bei den von uns vorgeschlagenen Site-2-Site Verbindungen feststellen. Jedoch ist hier eine Einschätzung vorab notwendig, um sicher zu gehen.

Wie geht die ADITO Cloud mit dem Thema Hochverfügbarkeit um (Verfügbarkeit von Datenbank und Applikationsserver)? Was passiert bei Ausfällen von Servern?

Unsere Multi-Cluster Umgebung besteht aktuell aus mehr als 70 Nodes (Server). Fällt eine Node aus, werden die durch den Ausfall gestoppten Services auf die anderen Nodes umverteilt. Vor unserem Cluster wird durch einen Load Balancer, der HTTPS-Anfragen auf die laufenden Nodes verteilt, sichergestellt, dass die abgebrochenen Verbindungen auf eine verfügbare Node umgeleitet werden.

Services und Datenbank: Services wie auch Datenbank werden automatisiert gestartet, sollten diese wegen eines Fehlers beendet worden sein. Darüber hinaus bieten wir auf Anfrage für Prod- und QA-Systeme statt einer alleinstehenden Datenbankinstanz auch Datenbank-Cluster an.

Aufteilen in Frontend- und Background-ADITO-Server: Neben dem normalen ADITO-Server bieten wir an, einen Background-ADITO-Server zu betreiben. Darauf werden Hintergrundprozesse wie zum Beispiel Mailbridge oder Importer-Prozesse ausgeführt, um im denkbaren Fall eines kritischen Fehlers eines Prozesses nicht die Clients zu beeinträchtigen.

Autostart/Autorestart: Alle unsere Cloud-Services, werden im Störungsfall automatisiert gestartet und durchgestartet, sollte ein kritischer Fehler vorkommen. Sollte einmal ein Ausfall stattfinden, ist der

© 2022 ADITO Software GmbH

ADITO Server nach wenigen Augenblicken von selbst, ohne Zutun seitens ADITO, wieder erreichbar.

Welche Ausnahmefälle wurden bereits berücksichtigt?

Die ADITO Cloud wird durch die ADITO IT betrieben, gewartet und weiterentwickelt. Hier machen wir uns stetig Gedanken welche Probleme im Detail auftreten können. Die wichtigsten Worst-Case-Szenarien wurden im Notfallkonzept zusammengefasst und Lösungen entwickelt. Darüber hinaus existieren klare Vorgehensweisen zu folgenden Sonderfällen:

- BSI G 0.27 Ressourcenmangel
- BSI G 0.40 Verhinderung von Diensten (Denial of Service)
- BSI G 0.45 Datenverlust DER.4 Notfallmanagement
- BSI OPS.1.1.6 Software-Tests und –Freigaben (hier Last- und Funktionalitätstests, sowie Überprüfung der Ausfallsicherheit)

Welches Betriebssystem empfiehlt die ADITO beim Betrieb der ADITO On-Premise-Lösung?

Generell müssen wir hier darauf hinweisen, dass wenn ein Betrieb außerhalb einer Kubernetes Infrastruktur umgesetzt werden soll, dass entsprechende Know-How beim Kunden vorhanden sein muss. Alle unsere Dienste sind als Container zu betreiben. Wir empfehlen daher Linux. Wir nutzen für unsere Umgebungen überwiegend Debian, jedoch ist die Distributionswahl für die Docker oder ContainerD Umgebung nicht allzu relevant. Wichtig ist auch, dass der Kunde über eine Infrastruktur zur Lastverteilung verfügen muss, da sonst ggf. Seiteneffekte einen HA Betrieb unterbinden.

© 2022 ADITO Software GmbH

11. Rechtliches und Regulatorisches

Alle Daten sind auf verschlüsselten Datenträgern abgelegt. Es ist zu jederzeit sichergestellt, dass ADITO die Lokalisation der Daten kennt und weiß wo sich die Daten physisch befinden. Alle Daten für den Betrieb der Cloud Systeme sind am Standort in Deutschland. Der Kunde kann auf Wunsch einen georedundanten, verschlüsselten Abzug in Helsinki ablegen lassen. Dies gewährt im Falle eines Totalverlustes des RZ eine Wiederinbetriebnahme des Systems. Verzichtet der Kunde auf die Georedundanz kann dies im Falle des Totalverlustes zum Gesamtverlust seiner Daten führen. Für diesen Service fallen keine zusätzlichen Kosten an.

© 2022 ADITO Software GmbH