Frozen Release - Deutsch

Strategy

Exported on 01/24/2024

Table of Contents

1 Accxia ONE Cloud als Plattform für Frozen Release

Um die Sicherheit der Atlassian Instanzen zu gewährleisten, ist es zwingend notwendig, daß die Lizenzen in der Accxia ONE Cloud in Deutschland gehostet werden. Dies bedeutet, daß Ihre existierenden Instanzen vom Kundenserver in die Accxia ONE Cloud überführt werden müssen. Accxia wird dies übernehmen.

Die Accxia ONE Cloud ist die größte Private Cloud für Atlassian Hosting. Wir differenzieren uns dadurch, dass wir keine Public Cloud wie AWS/Azure/Google verwenden. Unsere Kunden besitzen die volle Kontrolle.

Die Accxia ONE Cloud bietet folgende Leistungen an:

- Hostingbetrieb des gesamten Atlassian Stack (Full Managed Hosting)
- Hostingbetrieb von Drittanwendungen und Services (Full Managed Hosting)
- Microservices im Bereich Datenverarbeitung und Datenaufbereitung
- Cybersecurity-Optimierung, Verwaltung und Management der gesamten Hardware in Ihrem Unternehmen, gestützt durch Acronis Cyber-Security
- Accxia Cyber Disaster Recovery Cloud gestützt durch Acronis
- Standorte in Deutschland und den USA
- Daten werden in den jeweiligen Standorten verbleiben, d.h. sie werden Deutschland oder die USA nicht verlassen

Unser Fokus liegt auf den Bereichen "Private Cloud", Sicherheit und Datenschutz. Im Gegensatz zu AWS/ Azure/Google bieten wir ausschließlich von uns verwaltete Umgebungen an. Alle Umgebungen arbeiten in einem eigenen Bereich und werden nicht unter den Benutzern aufgeteilt. Die Ressourcenbereitstellung erfolgt zwar flexibel und skalierbar, es werden aber keine Ressourcen zur gemeinsamen Benutzung bereitgestellt. Jede Umgebung erhält ihre fest zugewiesenen Ressourcen, die jederzeit zur Verfügung stehen. Engpässe bei Leistungsspitzen durch den Kunden werden somit vermieden.

Zudem federn wir flexibel, ohne weitere Kosten, zweitweise anfallende Peaks automatisch ab. Dies inkludiert auch zusätzliche, temporäre Test- oder Staging Server.

Alle Accxia Standorte sind untereinander direkt per Glasfaseranbindung erreichbar. Das heißt für Sie, Ihre Applikation kann aus Nürnberg kommen, Ihre Datenbank aus Falkenstein und wenn Sie möchten, kann ein Fall-Back-Standort Helsinki sein.

Unsere Kundenumgebungen werden Docker gestützt betrieben. Alle Kundenumgebungen sind voneinander getrennt. In unseren Rechenzentren setzen wir auf die Sicherheit und die Vorteile einer containergestützten Umgebung. Die bietet Ihnen, als Kunden, eine hohe Flexibilität, sowie eine sehr gute Skalierbarkeit.

Alle Umgebungen können in unseren Rechenzentren in Nürnberg, Falkenstein oder in Helsinki betrieben werden. Als Option bieten wir hier die Möglichkeit das Backup geo-redundant auch in Frankfurt/Main als Cyber Disaster Recovery Cloud zu speichern. Hierdurch entsteht eine hohe Ausfallsicherheit, da Instanzen, innerhalb von wenigen Minuten, an einem anderen Standort wieder zur Verfügung stehen. Alle Backupdateien werden jeweils getrennt von den Produktionsinstanzen aufbewahrt. Als Beispiel: Produktionssystem am Standard A, Backupdaten am Standort B.

Der Zugriff ist ausschließlich verschlüsselt möglich, zertifikatsbasiert. Einen weiteren Zugang zum System stellen wir ausschließlich nicht bereit. Die Verwaltung und Pflege der Server wird nur duch autorisiertes Personal der Accxia GmbH vorgenommen.

In all unseren Rechenzentren existiert eine zentrale Brandschutzanlage, sowie ein ausreichendes Kühlsystem. Die Stromversorgung ist redundant ausgelegt und wird durch eine Netzersatzanlage ergänzt. Alle Systeme sind grundsätzlich redundant ausgelegt. Bei eintretenden Naturkatastrophen sind wir, durch unsere Backup-Site in der Lage Ihren Betrieb, nach einer kurzen Unterbrechung, sofort an einem anderen Standort weiterzuführen.

Die gleiche Technik erlaubt es uns ein standort-übergreifendes Multi-Node-Cluster aufzubauen. Redundante Load-Balancer garantieren Ihnen einen unterbrechungsfreien Zugriff auf Ihre Applikationen.

2 Support der Instanzen

Der Support der Instanzen kann ausschließlich durch die Accxia GmbH erfolgen. Aufgrund verschiedener Sicherheitsimplementierungen (Zugriff, Datenhaltung, gekapselte Container) können wir kleinere Sicherheitsrisiken bereits vor dem Zugriff auf das System abfangen. Ein kontinuierlicher Scan auf Sicherheitslücken findet durch einen Dienstleister statt, welcher uns laufende Berichte zur Verfügung stellt.

Als Atlassian Partner bekommen wir die CVEs direkt von Atlassian, die wir analysieren, um die beste Sicherheitslösung für unsere Kunden zu erarbeiten. Die Bereitstellung von Patches erfolgt durch Apps oder Systemeinspielungen durch die Accxia.

Zusätzlich ist der Zugriff auf die Applikationen durch eine Web Application Firewall beschränkt. Der Traffic wird automatisch analysiert und durch eine KI bewertet.

Auf all unseren Umgebungen betreiben wir ein laufendes Monitoring welches uns bei Fehlern oder Problemen benachrichtigt.

Auf Wunsch können wir monatliche Backups zum Download zur Verfügung stellen, so dass Sie Ihre Daten wie gewohnt in Ihr eigenes Backup einbinden können.

3 Sicherheitskonzept

Um die Sicherheit unserer Kundeninstanzen zu gewährleisten, setzt die Accxia auf selbst verwaltete Server. Alle Mitarbeiter der Accxia mit Server- oder Datenzugriff sind der Accxia bekannt und besitzen einen Accxia Arbeitsvertrag und die entsprechenden Sicherheitsunterweisungen. Der Zugang über Benutzerkonten wird ausschließlich durch die Accxia geregelt.

Darüberhinaus setzen wir eine WAF (Web Application Firewall) ein, die einen zusätzlichen Schutz vor Angriffen darstellt. Die WAF schützt vor einer Reihe von Angriffen effektiv und hilft auch, wenn Die Atlassian ihre Software nicht rechtzeitig patcht. Die WAF wird so an die Applikationen angepasst, dass sie optimal funktionieren kann, um die Anzahl der False-Negatives, also nicht erkannte Angriffe, sowie False-Positives (das Blocken gültiger Anfragen) zu minimieren. Um die WAF effektiv einstellen zu können, wird die Atlassian Software eine Zeit lang im Monitoring laufen müssen. Durch ein permanentes Monitoring nach Freigabe wird können wir das System permanent anpassen, um professionelle Angreifer rechtzeitig zu erkennen und Gegenmaßnahmen einzuleiten.

Kundendaten verlassen Deutschland nicht. Um unseren Standort in Helsinki nutzen zu können, setzen wir stets das schriftliche Einverständnis unserer Kunden voraus, dass eine Datenhaltung innerhalb anderer EU-Länder gewünscht ist. Alle Live- und Backup-Standorte befinden sich standardmäßig in Deutschland.

Falls nötig, und wie oben schon erwähnt, wird Accxia Apps entwickeln, um die durch die CVEs kommunizierten Sicherheitslücken zu schliessen. Mit anderen Worten, in keinem Fall wird Accxia in den Source Code der Atlassian Instanzen eingreifen. Sämtliche Sicherheitsbedürfnisse werden entweder über unsere Infrastruktur des Datenzentrums, also der Accxia ONE Cloud gemanagt, oder, in den wenigsten Fällen über Apps, die dann wie die üblichen Marketplace Apps in der Instanz verwaltet werden.

Darüberhinaus können Kundendaten, optional, auch durch die Cyber Disaster Recovery Cloud bei Acronis in Frankfurt gesichert werden. Diesen können wir mit unseren Rechenzentren Nürnberg, Falkenstein oder Helsinki verbinden. Die Übertragung erfolgt immer verschlüsselt.

Auf Wunsch kann die Verbindung zu Ihren Servern/Instanzen auf festgelegte öffentliche IP-Adressen beschränkt werden. Eine weitere Sicherheitsstufe wäre das Vorhandensein eines Client-Zertifikates um die Verbindung zu Ihren Instanzen überhaupt herstellen zu können.

Die Systemumgebung der Accxia wird außerdem durch regelmäßige Scans auf Sicherheitsrisiken und durch regelmäßige Penetrationstests geschützt. Unsere Pen-Tests sind KI unterstützt und laufen permanent und automatisiert.

==========

Der international anerkannte Standard für Informationssicherheit bescheinigt der Hetzner Online GmbH und der Hetzner Finland Oy, dass ein geeignetes Informationssicherheits-Managementsystem, kurz ISMS, implementiert wurde und gelebt wird. Das ISMS findet an den Standorten Nürnberg und Falkenstein sowie Helsinki unter dem Scope “Der Anwendungsbereich des Informationssicherheits-Managementsystems umfasst die Infrastruktur, den Betrieb und den Kundensupport der Rechenzentren.” seine Anwendung. Das entsprechende Zertifizierungsverfahren wurde durch die FOX Certification GmbH durchgeführt.

Das Zertifikat weist ein adäquates Sicherheitsmanagement, die Sicherheit der Daten, die Vertraulichkeit der Informationen und die Verfügbarkeit der IT-Systeme nach. Es bestätigt zudem, dass die Sicherheitsstandards kontinuierlich verbessert und nachhaltig kontrolliert werden.

4 Voraussetzungen und Limitierungen

Beim Weiterbetrieb der Atlassian Server Instanzen über das Supportende Februar 2024 hinaus entstehen gewisse Voraussetzungen und Limitierungen, an die wir gebunden sind.

4.1 Voraussetzungen:

- alle Atlassian Instanzen werden in unserem Rechenzentrum gehostet
- der Support erfolgt ausschließlich über die Accxia GmbH
- entsprechende Server-Lizenzen sind vorhanden für die Atlassian Produkte sowie alle benötigten Plugins/Addons/Apps
- eine eventuelle Weiterentwicklung kann nur über die Entwicklung von Apps erfolgen (eine eventuelle Entwicklung wird separat berechnet)

4.2 Limitierungen:

- das System befindet sich auf dem letzten veröffentlichten Stand durch Atlassian, eine Weiterentwicklung bzw. die neusten Änderungen können nicht implementiert werden
- Upgrade oder Downgrade von Lizenzen ist nicht möglich
- der Neuerwerb von Lizenzen ist nicht möglich
- neue Plugins sind nicht mehr verfügbar und können nicht erworben werden

4.3 Ausnahmen:

Die Accxia kann Sie dabei unterstützen neue Anforderungen in Form von Addons zu entwickeln und bereitzustellen. Diese Addons werden von Accxia nach Ihrer Vorgabe entwickelt.

Um eine über der Lizenzgrösse hinausgehende Anzahl von Benutzern in den Systemen verwalteten zu können, haben wir unsere Lösung „Intelligent User Manager“ im Portfolio, welches wir Ihnen auf Wunsch gerne vorstellen und implementieren können.Die Lizenzen sind damit sklalierbar. Dies hat den grossen Vorteil, dass ein zukünftig zu erwartendes Benutzerwachsum auch im Frozen Release abgedeckt werden kann.

5 Preisrahmen

Der Preisrahmen für das Frozen Release liegt bei im Bereich der normalen Renewal-Kosten der Atlassian Lizenzen, also Jira, JSM, Confluence, Bitbucket, inklusive des Hostings, sowie Pen-Tests, WAF, etc in der Accxia ONE Cloud. Dadurch dass die Atlassian Marketplace Apps nicht in den Kosten des Frozen Release enthalten sind, liegt das Frozen Release unter den Atlassian Renewal Kosten und natürlich weit unter Atlassian Cloud oder Data Center Lizenzkosten.