Frozen Release - English

Strategy

Exported on 04/18/2024

Table of Contents

1 The Accxia ONE Cloud to be the Platform for Frozen Release

In order to ensure the security of the Atlassian server instances Accxia requires that the instances are being hosted in the Accxia ONE Cloud in Germany. This means that the existing instances are to be ported over to the Accxia ONE Cloud from the client's servers. Accxia will take care of this.

The Accxia ONE Cloud is the largest private cloud for Atlassian Hosting. We differentiate ourselves by not using a public cloud like AWS/Azure/Google. Our customers have full control. Accxia ONE Cloud offers the following services:

- Hosting operation of the entire Atlassian stack (fully managed hosting)
- Hosting of third-party applications and services (fully managed hosting)
- Microservices in the area of data processing and data preparation
- Cybersecurity optimization, administration, and management of all hardware in your company, supported by Acronis Cyber-Security
- Accxia Cyber Disaster Recovery Cloud supported by Acronis
- Locations in Germany and the USA
- Data will remain in the respective locations, i.e. it will not leave Germany or the USA

Our focus is on the areas of private cloud, security, and data protection. In contrast to AWS/Azure/Google, we only offer environments managed by us. All environments work in their own area and are not shared between clients. Although the provision of resources is flexible and scalable, no resources are provided for shared use. Each environment is allocated its own fixed resources, which are always available. This avoids bottlenecks during performance peaks caused by the customer. In addition, we automatically and flexibly absorb user peaks at no additional cost. This also includes additional, temporary test or staging servers.

All Accxia locations can be reached directly via a fibre optic connection. For our clients, this means that your application can come from Nuremberg, your database from Falkenstein and, if you wish, a fall-back location can be Helsinki.

Our customer environments are operated with Docker support. All customer environments are separated from each other. In our data centers, we rely on the security and advantages of a container-based environment. This offers you, the customer, a high degree of flexibility and excellent scalability.

All environments can be operated in our data centers in Nuremberg, Falkenstein or Helsinki. As an option, we also offer the possibility to store the backup geo-redundantly in Frankfurt/Main as a cyber disaster recovery cloud. This ensures a high level of reliability, as instances are available again at another location within a few minutes. All backup files are stored separately from the production instances. For example: production system at standard A, backup data at location B.

Access is exclusively encrypted and certificate-based. We do not provide any other access to the system. The administration and maintenance of the servers is only carried out by authorized Accxia GmbH personnel.

All our data centers have a central fire protection system and an adequate cooling system.

cooling system. The power supply is redundant and is supplemented by an emergency power system.

All systems are designed to be redundant. In the event of natural disasters, we are protected by Our backup site is able to continue your operations immediately at another location after a brief interruption.

The same technology allows us to set up a cross-site multi-node cluster. Redundant load balancers guarantee you uninterrupted access to your applications.

2 Support for your Instance

Support for the instances can only be provided by Accxia. Due to various security implementations (access, data storage, encapsulated containers), we can intercept minor security risks even before the system is accessed. A continuous scan for vulnerabilities is carried out by a well-known cyber security provider who provides us with ongoing reports.

As an Atlassian partner, we receive the CVEs directly from Atlassian, which we analyse in order to develop the best security solution for our customers. The provision of patches takes place via apps or system imports by Accxia.

In addition, access to the applications is restricted by a web application firewall. Traffic is automatically analysed and evaluated by AI.

We run ongoing monitoring on all our environments, which notifies us in the event of errors or problems.

On request, we can provide monthly backups that can be download so that you can integrate your data into your own backup as usual.

3 Security Concept

To ensure the security of our customer instances, Accxia relies on self-managed servers. All Accxia employees with server or data access are known to Accxia and have an Accxia employment contract and the corresponding safety instructions. Access via user accounts is regulated exclusively by Accxia.

We also use a WAF (Web Application Firewall), which provides additional protection against attacks. The WAF effectively protects against a number of attacks and also helps if Atlassian does not patch its software in a timely manner. The WAF is adapted to the applications so that it can function optimally in order to minimize the number of false negatives, i.e. unrecognized attacks, and false positives (blocking valid requests). In order to set up the WAF effectively, the Atlassian software will have to run in monitoring for a while. Through permanent monitoring after approval, we can permanently adapt the system in order to identify professional attackers in a timely manner and initiate countermeasures.

Customer data does not leave Germany. In order to be able to use our fall-back location in Helsinki, we always require the written consent of our customers that data storage within other EU countries is desired. By default, all live and backup locations are in Germany.

If necessary, and as mentioned above, Accxia will develop apps to close the security vulnerabilities communicated by the CVEs. In other words, under no circumstances will Accxia interfere with the source code of the Atlassian instances. All security needs are managed either via our data center infrastructure, i.e. the Accxia ONE Cloud, or, in very few cases, via apps, which are then managed in the instance like the usual marketplace apps.

In addition, customer data can optionally be backed up using the Cyber Disaster Recovery Cloud at Acronis in Frankfurt. We can connect this to our data centers in Nuremberg, Falkenstein or Helsinki. The transmission is always encrypted.

If desired, the connection to your servers/instances can be limited to specified public IP addresses. A further security level would be the presence of a client certificate in order to be able to establish the connection to your instances.

The Accxia system environment is also protected by regular scans for security risks and regular penetration tests. Our pen tests are AI-supported and run permanently and automatically.

The internationally recognised standard for information security certifies that our data center provider, Hetzner Online GmbH and Hetzner Finland Oy, has implemented and are implementing a suitable information security management system, or ISMS for short. The ISMS takes place at the locations in Nuremberg and Falkenstein as well as Helsinki with the following remit "The scope of application of the information security management system includes the infrastructure, operation and customer support of the data centers." The certification process was carried out by FOX Certification GmbH.

The certificate proves adequate security management, the security of the data, the confidentiality of the information and the availability of the IT systems. It also confirms that safety standards are continuously improved and sustainably monitored.