

Astaro Mail Archiving

Process Documentation v1.0

Introduction

Astaro Mail Archiving (AMA) offers to archive e-mails as a service provided by Astaro Services AG (Astaro). E-mails to be archived are transmitted in encrypted form to the archiving service which can be accessed centrally via the Internet. The e-mails are then indexed, archived and made available at any time for authorized user inquiries by the Customer.

As a cloud-based solution, AMA offers great administration, scalability, availability and security advantages. Astaro has many years of experience in Internet security-related matters. This extensive expertise particularly enables Astaro to safeguard the data protection, access protection and availability of AMA.

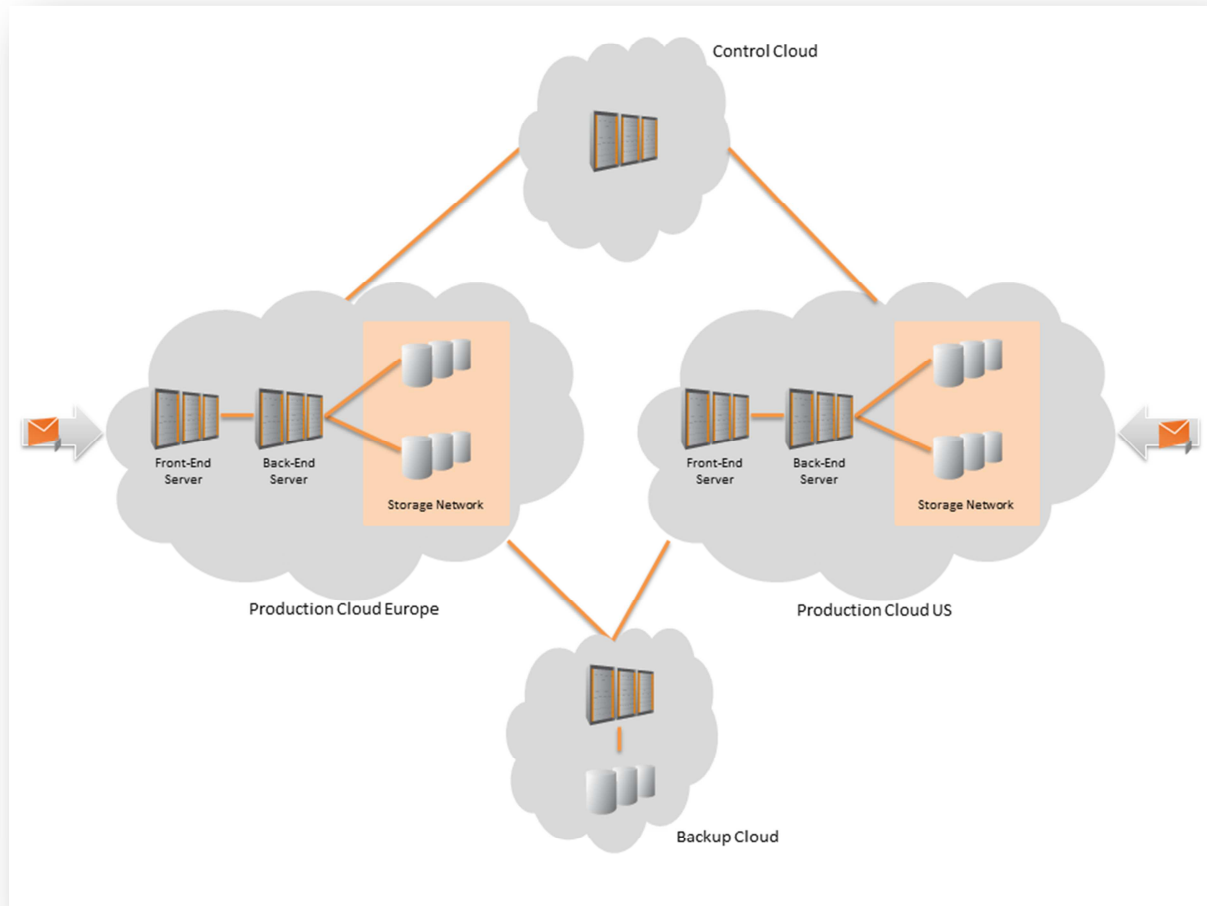
This document explains the internal processes and structure of AMA, as well as protective measures for comprehensive data and access protection.

Table of Contents

1. Overview.....	2
1.1 Production Cloud.....	2
1.2 Backup Cloud	3
1.3 Control Cloud	3
1.4 Access protection.....	3
2. Processes.....	3
2.1 Data transmission & processing	3
2.2 Data storage	4
2.3 Accessing data (User/Export/Deletion)	4
3. Failure protection & availability	4

1. Overview

The AMA infrastructure comprises a number of servers which process different areas of tasks.



Astaro differentiates here between Production, Backup and Control Clouds whose operations are separated physically and geographically in separate hosting environments. This separation also serves to divide powers in order to maximize access and data protection.

This section will describe the tasks of the different cloud components before examining the individual processes.

1.1 Production Cloud

Astaro operates two independent AMA infrastructures in the USA and the European Union (EU). This ensures that data belonging to a customer in the EU is stored in its entirety and exclusively in an EU member state at all times. Customers from the United States or from other non-EU countries use the AMA infrastructure in the USA. The same processes, guidelines and technical measures also apply there. At no point is data exchanged between the regions.

There is a complete, redundant production environment in place in each region. The highly scalable server instances in the Production Cloud can be extended any time and are responsible for the acceptance, processing and encrypted storage of e-mails.

Data cannot be accessed via the individual physical systems in the IT datacenter within the production environment. All access must take place via the Control Cloud. Customer keys for cryptographic processing of the e-mails which are being archived are saved exclusively in the Control Cloud, and access is only granted temporarily to the system during the processing time.

A distinction is made between front-end servers, back-end servers and a separate storage network within the Production Cloud. All servers work with encrypted data partitions whose keys are stored centrally in the Control Cloud and are only transmitted during runtime.

When processing customer e-mails, the customer-specific key for encrypting and decrypting e-mails is also required. Astaro ensures that this key is only ever stored on closed back-end servers which are externally inaccessible. Access takes place exclusively in runtime via special program interfaces.

1.2 Backup Cloud

The Backup Cloud is operated within the EU, geographically separated from both production regions. All archived e-mails are automatically backed up in this additional stage of security. The data stored here is encrypted at all times.

1.3 Control Cloud

The control system is a component which is important for compliance with data protection guidelines. It also works in a separate Control Cloud. Central tasks are access protection, administration and control of data keys, as well as monitoring of the overall system.

1.4 Access protection

Astaro has implemented extensive mechanisms for protecting both physical access to the cloud systems, as well as data access. Where legally permitted, operators at Astaro, who are contractually bound, have been vetted and been carefully selected.

Physical access to the individual systems in the Production Cloud is limited to local operators. Central administration of all data access via the Control Cloud prevents access to the data on site or the release of data to third parties with court authorization.

Physical access to the individual systems in the Backup Cloud is limited to local operators. Since this solely involves the backup of data which has already been encrypted, saved data cannot be processed or released to third parties with court authorization.

The Control Cloud supports physical access and restricting access to selected Astaro operators. The surrender of data keys or the enabling of third-party data access can only take place exclusively within the scope of legitimate legal means.

2. Processes

2.1 Data transmission & processing

E-mails are transmitted from the customer's e-mail server to the AMA Production Cloud in an encrypted form. AMA does not support the acceptance of unencrypted data!

During the acceptance process, the data is protected against loss and unauthorized access at any time by a redundant and encrypted queue.

During the processing phase, the e-mails are indexed, compressed and are then encrypted individually with the corresponding customer key. It should be noted that each customer is assigned a separate key, which means that data is always filed away in the correct customer archive. It prevents the possibility of accidental, cross-customer access to e-mails.

2.2 Data storage

The archived data is stored definitively in encrypted and redundant form in high-availability storage systems in each cloud region. Parallel to storage, an encrypted backup copy of each archived e-mail is created in the Backup Cloud in order to afford customer data optimum protection.

2.3 Accessing data (User/Export/Deletion)

Once e-mails have been archived, they can be accessed in a variety of ways:

- By authorized, authenticated end users (for example, for research purposes)
- By authorized, authenticated auditors (for example, for requesting deletions)
- Via automatic AMA processes for the reliable deletion of e-mails once the period of compulsory retention has elapsed
- By way of a request from the customer to export the archive.

Users are authenticated either via the customer's login server or alternatively via local user databases in the AMA system. In all cases, the backed-up key for decrypting e-mails is required in order to access archived data. The key can only be requested temporarily on back-end servers and via defined program interfaces.

3. Failure protection & availability

All the systems in AMA are redundant in design and distributed geographically. Furthermore, routine, automatic data backups guarantee enhanced protection against unforeseen events. The redundant and highly scalable system architecture provides for constant availability and flexible scaling as requirements increase. Both server and storage resources that are required are adapted automatically and guarantee high-performance access.

Maintenance work is generally executed in such a way that archive access is not hindered. Where work requires brief interruptions to the AMA service, this takes place outside main business hours by prior notification, where possible.