White Paper
DocuWare Cloud

Version 2.0

May 2015

Impressum:

DocuWare GmbH
Therese-Giehse-Platz 2
D-82110 Germering
Telephone: +49.89.89 44 33-0
Fax: +49.89.8 41 99 66
E-Mail: infoline@docuware.com

Disclaimer:

This document was compiled to the best of our knowledge and with great care. All references are to DocuWare Cloud. Essentially, this white paper sets out to describe the basic technical structure and security concept for DocuWare Cloud. There may be small or temporary differences, but only with respect to individual functions in a particular version.

DocuWare

Contents

1 Objectives of this White Paper

Your information is your asset! With our document management solution DocuWare Cloud, we are offering you perfect availability and security for your documents. Data security and performance are and always have been DocuWare GmbH's top priority.

This white paper presents the measures which have been implemented for data security and fail-safety. It includes all preventive measures against accidental or deliberate manipulation of managed content, and against data loss. Security features also include measures that guarantee data protection and ensure that changes within the system are traceable. This should provide readers with a technically sound understanding of the DocuWare Cloud system's structure and security. This white paper addresses clients (users), consulting companies, IT magazines, and distribution partners. It assumes a certain level of technical knowledge about the structure of modern software applications, ideally of document management systems. Detailed knowledge of current or previous DocuWare versions is not necessary.

2 Introduction

Cloud computing is an alternative way to use software: You can use DocuWare Cloud to store, search, display, download, and edit documents, and integrate them into your business processes over the Internet without any traditional software installation on your local computer. Your documents are securely stored in the cloud. Once you have entered your user ID, you will find yourself back in your normal working environment with access to all your documents and processes no matter the place or time.

3 Architecture - Overview

The structure of DocuWare Cloud can be organized into two broad areas:

- The hosting (infrastructure)
- The DocuWare system

In order to offer its customers the greatest possible security and performance, DocuWare GmbH is working in partnership with a professional host. The host will take over the operation of the entire DocuWare Cloud infrastructure at its data center.

3.1 Hosting

After a careful inspection and extensive tests, Microsoft Azure was chosen to be the platform for DocuWare Cloud. This platform offers various services which enable DocuWare Cloud to secure business continuity for their customers.

The hardware is separated from the software using the latest virtualization technology and provided to the customer as an infrastructure service via stable virtualized server resources and cloud services. Unlike real hardware, this virtual infrastructure can be adapted to the customers' current needs flexibly and quickly at any time. This means we are always able to guarantee ideal performance with optimized costs, regardless of how many customers are using our system at any given time.

General

It is imperative for a cloud provider to ensure that the infrastructure is constantly available. To this end, measures have been taken in all areas to prevent the existence of any "single point of failure." In many cases, critical components have as many as three or four backups.

Server

All application servers run on virtual machines. The performance parameters of these machines can be adjusted according to the performance need. Microsoft Azure guarantees that the required performance is actually available.

- The resources allotted to a virtual machine (CPU, memory, etc.) are exclusively available to that machine. Multiple customers never use overlapping resources.
- DocuWare can use a graphical interface to adjust promptly the number of CPU cores or the memory size at any time. The changes take effect immediately after the virtual machine is restarted.

Storage

All documents are stored on the Azure Files service. There are three redundant copies of each file stored here. The files are mirrored from a second location located hundreds of kilometers away and three redundant copies are stored there. The mirrored data also remain in the same economic area, meaning that documents stored in the EU do not leave the EU and data stored in the US do not leave the US.

In addition, we copy the files once a week to Azure Blobs. Once they have been copied, documents are not deleted. Copying the documents protects them from accidental deletion.

More information on the Azure Files and Azure Blobs services to be used can be found under http://azure.microsoft.com/en-us/services/storage

Networks

The network infrastructure is also virtualized. The virtual network is sealed off externally so that the entire data traffic cannot be seen from outside of the network.

The virtual machines within a virtual network are located in a Windows domain. This helps the DocuWare Cloud team to administrate the system when, for example, a new application server is added.

Data Storage / Data Security

To account for local conditions, documents and data are saved in the customer's region. That way the operation of the system and data follow the locally applicable data protection standards:

- All customers from the EMEA region are hosted by our EU data center based in Dublin. Data is synchronized to Amsterdam. In this way, the European data protection guidelines and the German Data Protection Act are respected.
- All customers in the North and South America region are hosted in our United States data center based in Iowa. The data is synchronized to a data center in Virginia and as such are subject to the US data protection guidelines.

DocuWare will ensure that the customer's data never leaves the corresponding economic area without the customer's knowledge.

3.2 The DocuWare System

DocuWare allows companies to tap into the value-adding potential of documents and their contents. The DocuWare document management system is the state-of-the-art software for professional enterprise content management (ECM) and tamper-proof electronic archiving. In designing DocuWare Cloud, it was and has remained our top priority to ensure optimum performance and the highest possible level of fail-safety during the operation of DocuWare.

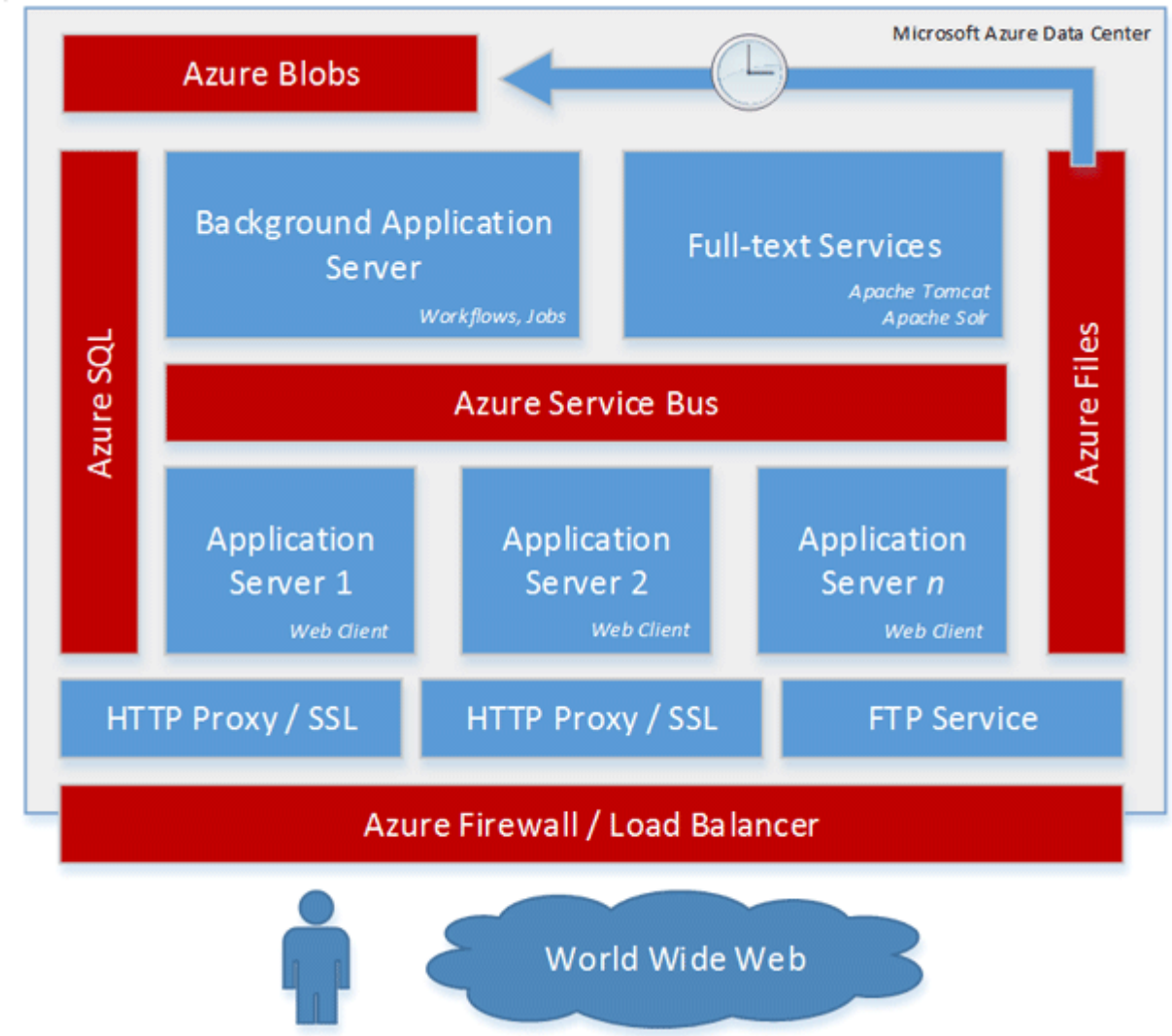
DocuWare Cloud essentially consists of two components:

- The DocuWare organizations contain the encrypted customer data. Each customer has their own specific organization, which only they can access. Each organization can be clearly identified by its organization ID, and is completely separate from other organizations.
- The DocuWare system includes all the servers and services for the operation of DocuWare. All servers are redundantly available to ensure the full functionality of DocuWare Cloud at all times, even in the event of server failure. If a failure does occur, the system continues running uninterrupted on the other available server.

The DocuWare system consists of the following components:

Firewall with round-robin load balancing. The firewall accepts and forwards all incoming requirements to the suitable application server or HTTP proxy.

HTTP Proxy / SSL. All incoming HTTPS queries are taken to one of these servers. The SSL encryption takes place there. The encrypted queries are then delegated to a suitable application server. Once the application service has processed the queries, the answer is supplied to the user by encrypted SSL. Even if this server has a low load, there are multiple instances to ensure the system remains stable.



DocuWare Cloud builds on the Azure platform. The red components belong to the Azure platform, the blue components to the DocuWare Cloud.

Application Server. These servers work on all queries to the WebClient or the DocuWare settings.

Background Application Server. This is a special application server which contains services for background tasks (such as Workflow and Autoindex).

FTP Service. A special server is made available for the ScanToFTP service.

Full Text Services. This machine manages the full text for all users. DocuWare uses Apache Solr for this. One single server is sufficient for the time being as the full text is not used very often. Nevertheless, this solution is easily scalable: If the load is likely to be large, Solr Cloud is used.

Azure Files / Azure Blobs. All users' documents are saved in encrypted form here. Azure Files already stores six redundant copies of the data. In addition to this, the DocuWare team copies all new files to Azure Blobs once a week. The data is also encrypted and stored here. This protects the files from accidental deletion.

Azure SQL is a scalably managed SQL database provided by Microsoft Azure. Each customer has their own database. Database operations carried out by a customer, such as complex searches, do not affect the database operations of other customers.

4 Security Concept

The DocuWare Cloud system's architecture was designed with the primary considerations of data security and administrative process accountability. It is thus guaranteed that documents can only be opened or edited by individuals who are authorized to do so. This applies to users within a customer's system as well as to the system as a whole. There is a strict, fundamental separation between

- Customer data (DocuWare organizations)

and

- System data (the DocuWare system)

Administrators only have access to the data necessary to operate DocuWare Cloud. They are never able to access customer data. Access to the DocuWare Cloud system can be traced at any time using the auditing services.

4.1 Encrypting Communication

The data within the data center are secured by a VPN. Thus there is no way for data or information to be intercepted inside or outside of the system. See also https://msdn.microsoft.com/library/azure/jj156007.aspx

SSL is used to encrypt data traffic between the users and the data center. This applies to both the HTTP traffic and remoting-based traffic. Extended validation technology instantly assures the user that the connection is secure and validated by coloring the address bar green:

4.2 Document Encryption

All documents saved in file cabinets are automatically encrypted using the AES (Advanced Encryption Standard) encryption process. AES is the successor to DES (Data Encryption Standard). AES is currently one of the most secure symmetric encryption processes. It is approved for use by the US government as the US encryption standard for documents with the highest security clearance level (top secret) and meets the strictest security requirements.

An asymmetric key pair is generated for each file cabinet. The private key is used to encrypt the symmetric keys which are created when the documents in a file cabinet are encrypted. The private key for a file cabinet is, in turn, encrypted using a master key.

DocuWare relies on the use of AES with a key length of 256 bits for maximum protection when encrypting. A key length of 4096 bits is used for the encryption of symmetric keys. A

new symmetric key is generated for each document. This increases security, as there would only be a relatively small encrypted data set available for a potential attempt at decryption.

4.3 Access Control for Maintenance Administrators

Specific activities do require full (or comprehensive) administrative rights to the DocuWare Cloud systems. In order to guarantee complete protection of data in these cases as well, maintenance administrators' access procedures are subject to being recorded. The following security mechanisms are installed:

- Each instance of access to DocuWare Cloud systems occurs in an RDP session.
- Each administrator has their own ID. It is therefore possible to determine who logged in to which system at any time.
- To start an RDP session, you must first log on via a VPN. This VPN is secured via certificates only made available to the administrators.
- All administrators are trained and have been especially informed of the sensitive handling of data such as certificates and passwords.

5 Performance

Thanks to DocuWare's multi-client capabilities, DocuWare Cloud is able to make optimum use of its resources. Thus it does not matter whether an organization generates a very high load (such as through many users) or a very low one. Every user always benefits from the full data and storage performance. Moreover, the system makes it possible to react to any weaknesses in short order so that additional capacities can be added to the system.

5.1 Load Balancing

On the DocuWare Cloud system, the load is, in principle, distributed across all available servers. This contributes to a balance in the available servers' workloads and ensures a consistently high performance level of the system overall. If predefined thresholds are exceeded, additional capacities (CPU power or memory) or complete virtual servers can be added. The process for this depends on the part of the DocuWare system which is affected.

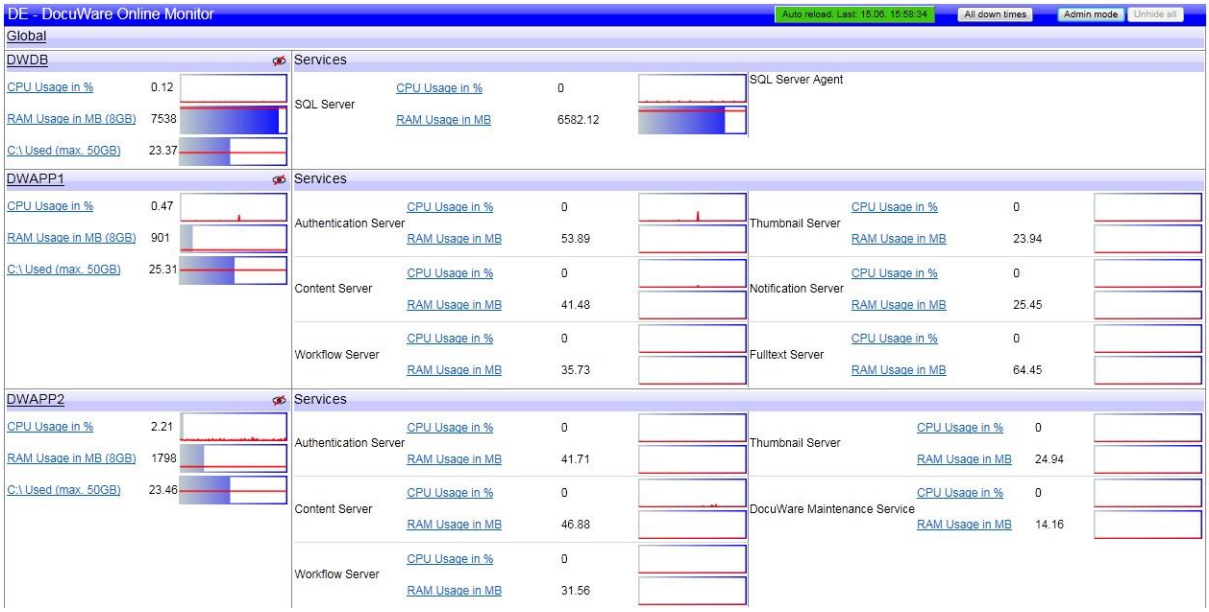
5.2 Dynamic Performance Adjustment

Our support team has access to a variety of options to help us react quickly and flexibly to fluctuating loads:

- Extending the existing virtual server by adding additional processing cores or additional storage space. This is performed within seconds and takes effect immediately after the virtual machine is restarted. Thanks to the entire system's failsafe structure, this step can be carried out during operation without any interruptions.
- Adding entire virtual servers, either by booting up extra servers from standby as needed, or by supplying entirely new virtual servers based on a preconfigured installation package.

6 DocuWare Cloud Monitor: Performance Controls

All DocuWare servers and services are automatically monitored and report any system failures or performance bottlenecks immediately. Microsoft Azure offers Application Insights, a service that monitors all of the DocuWare Cloud system's important parameters. In addition, complete functional tests are regularly carried out to test the login procedure, storage, search, and other important features of DocuWare. If an error occurs or the tests cannot be completed in the specified time, the DocuWare Cloud support team will be notified immediately. This notification is sent either by email or SMS, depending on how urgent it is. If it is extremely urgent, the error will be immediately reported and rectified by our 24/7 on-call team.



The Azure Service Application Insights monitors the Cloud system's important parameters.

7 Logging Users and Processes

DocuWare offers comprehensive logging options to help DocuWare organizations keep constant track of all their internal processes. This makes it possible at any time to determine who within your organization has deleted or modified a particular document. To this end, a Logging Agent must be defined and enabled in DocuWare Administration. The types of information to be logged can be specified during the configuration of logging agents:

- Actions such as sending documents
- File cabinets such as the Accounting file cabinet
- Users or user groups, such as Administrators
- A combination of parameters

8 Information for Administrators

DocuWare Cloud offers additional support for live operation by backing up documents and providing easy upgrades and support.

8.1 DocuWare Request

With DocuWare Request, you have the ability to make a copy of your data or of certain documents, either once or at regular intervals. The customer can freely define the extent of the backup. This means they can request an incremental backup of a file cabinet twice a year, for example. Data created in this manner can be imported into a DocuWare organization at any time, and can be searched and displayed using the query program included in delivery independently of a DocuWare system.

8.2 Hotfixes and Upgrades of the DocuWare Cloud System

The DocuWare Cloud system is always operated with the latest version of DocuWare. Therefore, the current version of DocuWare is installed approximately every six months. We recommend also keeping the locally installed components up to date. Users can upgrade themselves without any problems as long as they are authorized to install software locally. If this is not the case, the IT administrator generally undertakes the update with a Software Management Solution. A silent install for the DocuWare components has been created to quickly upgrade many PCs in a company. See also the Support FAQs https://www.docuware.com/support_faq/index.php?solution_id=3838

Customers are notified of the new versions and updates around four weeks in advance.

8.3 Support

DocuWare Cloud is supported around the clock by an experienced support team. As soon as you become a DocuWare Cloud customer, you can register with the Support Forum https://www.docuware.com/forum/english-forums/docuware-announcements/docuware-cloud-emea-status-information

All scheduled and unscheduled downtimes are openly communicated here. You can also request to immediately receive email notifications for each new message.

9 Data Handover upon Termination of the Contract

If, upon termination of the contract, you wish to download your documents from the DocuWare Cloud system and/or migrate them to another system, we can help you do this. The following options are available for this:

1. Smaller amounts of data with documents that do not need to be processed promptly, if at all, can be received in the form of a DocuWare Request (see chapter "DocuWare Request").

2. For larger amounts of data as well as documents integrated in current processes, we recommend you consider using our DocuWare Professional Service for a fee. This provides you with the following benefits:

- Following consultation and approval by the customer, the Professional Service (PS) is able to access the customer's documents in the data center and therefore also transfer large amounts of data without delay.
- Documents that are in the middle of a workflow process should retain their workflow states and statuses. Thanks to the Professional Service's special know-how, these documents can be migrated promptly into a new system's workflow process.
- The Professional Service's experienced employees can develop customer-specific solutions which are adapted specifically to the company's workflows and document types used.

Following termination of the contract, we will securely and irrecoverably delete all data. A restore from this point will no longer be possible.

10 Compliance & Certifications

Your data is safe with DocuWare Cloud. In addition to industry-leading best practices in security DocuWare Cloud provides your organization cloud-based document management with independently verified processes and infrastructure.

ISO 27001

Information security is critical to you, and ISO 27001 is the best-known standard for an information security management system. DocuWare implements a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.

HGB/AO, GoBS, and GDPdU

The document management system supports the requirements for archiving documents that are subject to mandatory retention according to the rules of orderly bookkeeping, and guarantees audit-compliant, long-term archiving according to HGB/AO, GoBS, and GDPdU, according to the auditing standard PS 880 of the German Institute of Auditors (IDW).

ISO 9001

Quality is at the heart of all that we do. DocuWare utilizes an ISO 9001 certified quality management system. This standard is based on a number of quality management principles including a strong customer focus.

SOC 1/SSAE 16/USAE 3402 and SOC 2 Attestations (formerly SAS 70)

You should be diligent when putting your organization's information in the cloud, have assurance that your data is safe as you choose DocuWare as your service organization. Our hosting provider performs audits in accordance with the Statement on Standards for Attestation Engagements (SSAE) No. 16 put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) and International Standard on Assurance Engagements (ISAE) 3402 put forth by the International Auditing and Assurance Standards Board (IAASB). In addition, the SOC 2 Type 2 audit included an examination of the Cloud Controls Matrix (CCM) from the Cloud Security Alliance (CSA). These audits can be provided to you at your request.

Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

If you are looking to assess the overall security risk of a cloud provider, the Cloud Control Matrix (CCM) is one of the best tools in the industry to help you make an informed decision. The CCM is designed to provide fundamental security principles to guide cloud vendors. Our hosting provider provides detailed information about how our hosting fulfills the security, privacy, compliance, and risk management requirements defined in the CCM version 1.2. This report is filed in the CSA's Security Trust and Assurance Registry (STAR) and can be provided to you at your request.