White Paper
DocuWare Online

Version 1.0

December 2013

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 Online. Essentially, this white paper sets out to describe the basic technical structure and security concept for DocuWare Online. There may be small or temporary differences, but only with respect to individual functions in a particular version.

Contents

1 Objectives of This White Paper 5

1.1 Introduction 5

2 Architecture – Overview 6

2.1 Hosting 6

2.2 DocuWare System 9

3 Security Concept 12

3.1 Encrypting Communication 12

3.2 Document Encryption 12

3.3 Access Control for Maintenance Users 13

3.4 Access Control for Maintenance Administrators 13

4 Fail-Safety 14

4.1 24/7 Support 14

4.2 Snapshot Backup 14

4.3 Logical Distribution of the Virtual Servers 14

5 Performance 15

5.1 Load Balancing 15

5.2 Dynamic Performance Adjustment 15

6 DocuWare Online Monitor – Performance Controls 16

7 Logging Users and Processes 17

8 Backup/Restore 18

8.1 DocuWare Request 18

8.2 Backup System 18

9	Data Handover upon Termination of the Contract	19
10	Quality Guarantee	20
11	Index	21

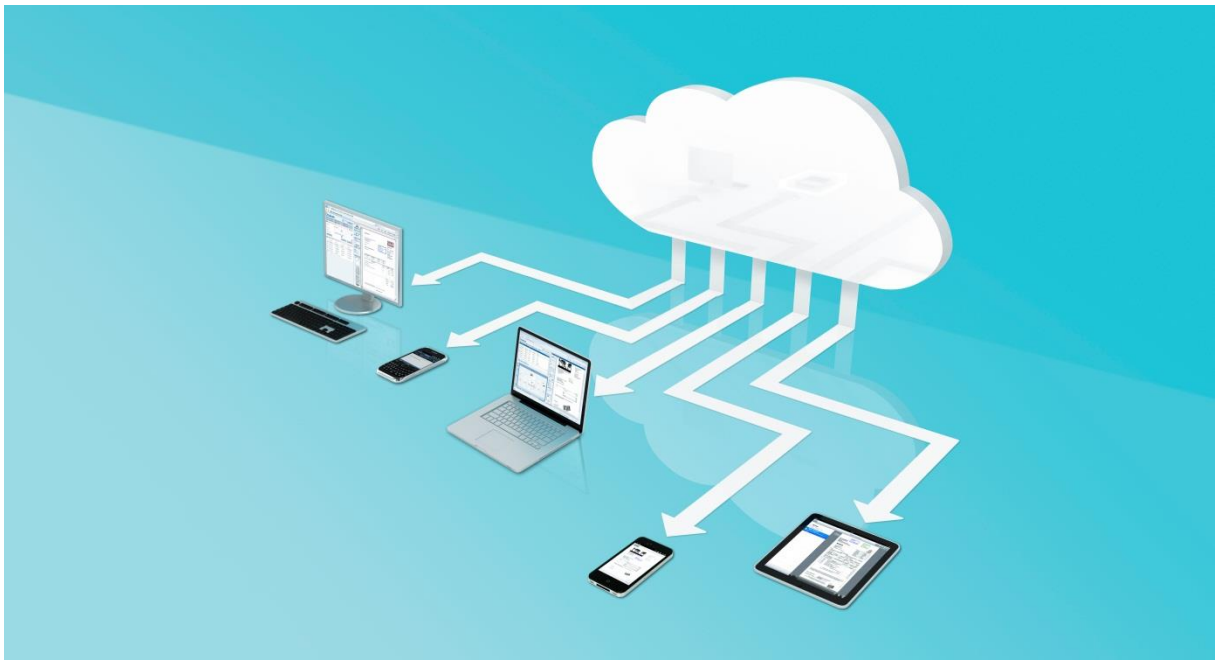
1 Objectives of This White Paper

Your information is your asset! With our new cloud-based document management solution, DocuWare Online, we are offering you even greater availability and security for your documents. Data security and performance are and always have been DocuWare'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 Online 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.

1.1 Introduction

Cloud computing is a new way to use software: You can use DocuWare Online 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.



2 Architecture – Overview

The structure of DocuWare Online 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 decided to work in partnership with a professional host. The host will take over the operation of the entire DocuWare Online infrastructure at its data center.

2.1 Hosting

A next-generation IaaS ("Infrastructure as a Service") provider was chosen to be the host. Using the latest cloud technologies, the provider offers the best operating conditions for DocuWare Online. 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. 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.

- Every system operates with a RAID-60 storage system and is equipped with ample reserve capacity. This guarantees maximum protection of the data and smooth, uninterrupted server operation even if there is an error. In the unlikely event that a server outage occurs despite these measures, the virtual systems running on the server automatically migrate elsewhere and are soon operational again.
- Data storage locations are unquestionably protected from outages, as they are physically separated from the host servers and exist in multiple parallel copies on a high-availability system (see “Storage”).
- The network connection for all the servers is always redundant. Each physical server is connected to several LAN segments in the data center and the data center has several separate Internet connections.
- The virtual servers are kept in different fire zones (high-availability zones). This geographical separation of the hardware makes it almost impossible for virtual servers to fail due to external influences.

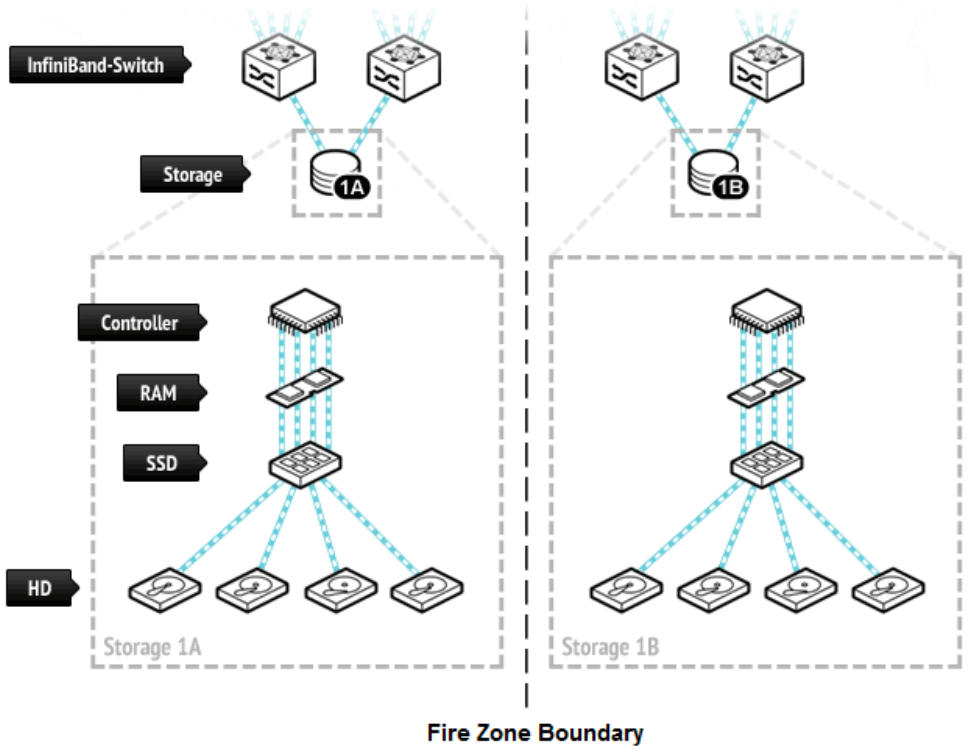
Servers

Every virtual system runs on a specially optimized hardware platform. Moreover, the virtualization solution used in many areas has been optimized for the hardware present, offering optimum protection from outages and a consistently good performance:

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

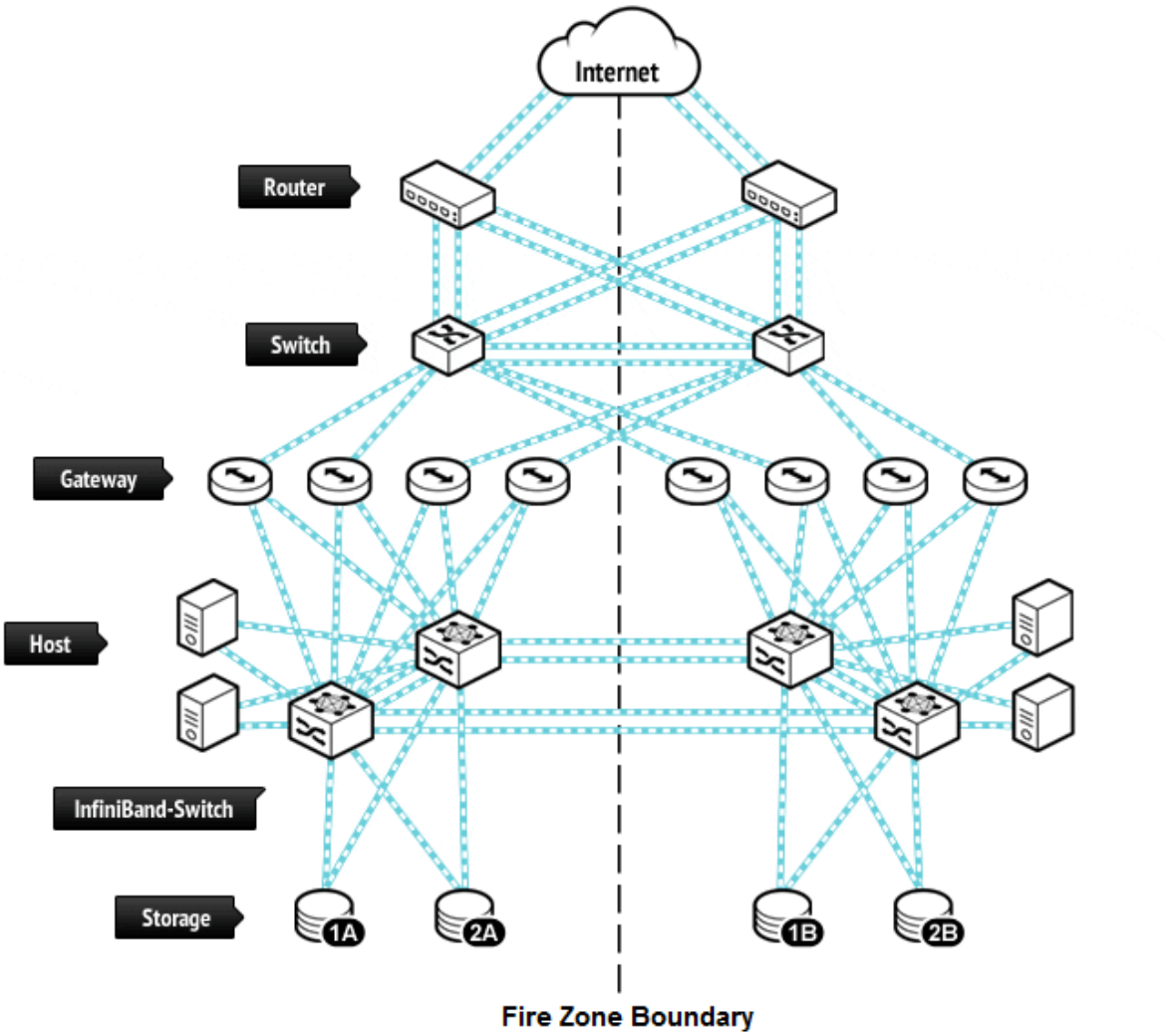
Storage

As with the host machines, all storage uses RAID 60 hard disks exclusively. Although storage with RAID 60 technology can already compensate for the failure of several hard drives, storage server systems are also redundantly hosted to ensure that your data is optimally protected. Each storage unit is made up of two subunits, which are always kept in different fire zones in the relevant data center. Both subunits work synchronously and each contains the entire database. Each subunit also stores the data redundantly again within the unit. Each subunit also has a set of SSD hard drives (hard drives without mechanics on RAM basis) as a cache in order to optimize the speed of the unit.



Networks

The connection between the host systems and the Internet is a large factor in determining the overall system's speed. Beyond that, the connections among the various systems and to the storage servers play an even greater role. That is why our data center employs the latest high-performance data transfer technologies. Instead of 10 GBit Ethernet (10 GbE), only 4x QDR InfiniBand technology that supports maximum transfer rates of up to 4 x 10 GBit/s with a switch latency of 200 ns is used. Our data center thus offers transfer rates 4 times faster and latency periods 10 times shorter than comparable 10 GBit Ethernet technology. InfiniBand is also less susceptible to failure than 10 GBit Ethernet and allows the infrastructure to be scaled more quickly without any loss of performance or efficiency.



Schematic Representation of the Network Connections in the Entire System

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:

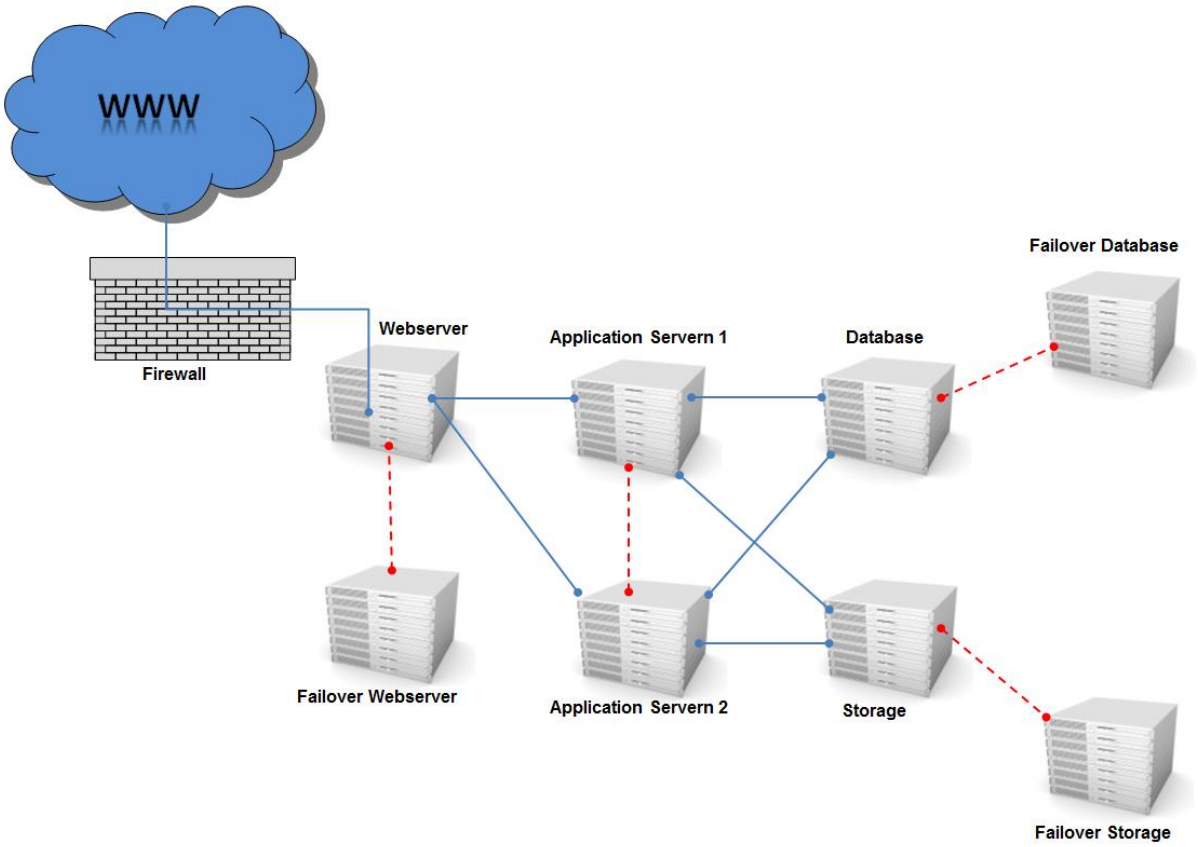
- All customers from the EMEA region are hosted by a data center in the EU. They are therefore subject to European data protection standards and the German Federal Data Protection Act.
- All customers in the North and South America region are hosted in our United States data center. They are therefore subject to US data protection guidelines (including the US Patriot Act).

2.2 DocuWare System

DocuWare allows companies to tap into the value-adding potential of documents and their contents. The DocuWare 5 document management system is the state-of-the-art software for professional enterprise content management (ECM) and tamper-proof electronic archiving. In designing DocuWare Online, 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 5.

DocuWare Online 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 5. All servers are redundantly available to ensure the full functionality of DocuWare Online at all times, even in the event of server failure. If a failure does occur, the system continues running uninterrupted on the twin or other available server.


WWW
Firewall
Webserver
Application Servern 1
Database
Failover Database
Failover Webserver
Application Servern 2
Storage
Failover Storage

The DocuWare system consists of the following components:

1 Two application servers (1 & 2) contain all the important DocuWare services, which are needed for the operation of the DocuWare system, such as: :
- Authentication Server
- Content Server
- Workflow Server
- Fulltext Server
- Notification Server
- Thumbnail Server
- Job Processor

2 Two Web servers (the Web server & failover Web server) are home to the IIS (Internet Information Service) and are responsible for generating web instances for DocuWare organizations.

3 Both customer databases and system databases are, completely redundantly, saved on two database servers (the database & failover database).

4 The encrypted customer data is, completely redundantly, saved on two storage servers (storage & failover storage).

5 In order to protect DocuWare Online against attacks over the Internet, a professional firewall solution is deployed to guarantee the comprehensive protection for the systems. It includes the following components, among others:

Anti-malware technologies, which use generic signatures and heuristic technologies to catch even malware variants which do not match a specific signature.

Intrusion prevention technologies protect the system from vulnerabilities which can be caused by plug-ins.

URL filtering efficiently blocks malicious websites by using several URL filters, and anti-phishing and anti-malware technologies.

Reputation services, which ward off spy and malware attacks at an early stage even before signatures are available for them.

3 Security Concept

The DocuWare Online 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 Online. They are never capable of accessing customer data, as the system automatically prevents it. Furthermore, a system has been implemented to enable monitoring and permanent recording of instances of administrator access. This means that all changes to the DocuWare Online system are traceable accountable at all times.

3.1 Encrypting Communication

All of DocuWare Online's data traffic is encrypted as a rule. That applies to the connection between the client and the online system as well as to communication among servers. Thus there is no way for data or information to be intercepted inside or outside of the system.

A Secure Site SSL Certificate (from VeriSign) with an encryption rate of up to 256 bits is used for the encryption. Extended validation technology instantly assures the user that the connection is secure and validated by coloring the address bar green.

3.2 Document Encryption

All documents saved in DocuWare Online 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-256 with the maximum key length of 256 bit 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.

3.3 Access Control for Maintenance Users

In our approach to DocuWare Online's maintenance, we have put in place a strict division between maintenance users and maintenance administrators. Maintenance users have a very limited spectrum of rights and can only perform actions on the system that help ensure the system's smooth functioning. These are, more specifically:

- Restarting DocuWare services
- Access to server event logs
- Access to system databases
- Access to local IIS instances

This enables maintenance users to analyze potential problems and rectify them using targeted measures. This security access level applies to all initial analyses and "normal" maintenance activities.

Under no circumstances do maintenance users receive access to customer data or to directories in which customer data is stored.

3.4 Access Control for Maintenance Administrators

Specific activities do require full (or comprehensive) administrative rights to the DocuWare Online systems. In order to guarantee 100 percent protection of data in these cases as well, maintenance administrators' access procedures are strictly defined and are also completely recorded and supervised.

- Each instance of access to DocuWare Online systems occurs in an RDP session.
- Following a separation of duties approach, the passwords are stored in preconfigured RDP shortcuts and are thus never disclosed to the administrators. The only way to launch a session is by clicking on the RDP shortcut. Part of the password is determined by a member of DocuWare management.
- Every RDP session is logged using special software and saved in a secured DocuWare file cabinet. The Vice President of Online Operations is automatically informed of every log, and holds responsibility for supervising and approving the session. This ensures that all administrative activities are supervised and completely documented.
- The maintenance administrators' passwords are kept with a security server and transmitted in two separate parts. In exceptional cases, the password may be requested via a 24/7 hotline. Password requests are automatically forwarded to the Vice President of Online Operations. The password must then be reset and transmitted on the following workday.

4 Fail-Safety

Constant system availability is a basic precondition for a Cloud service's success. Point 3, "Architecture – Overview," already documents a wide range of comprehensive measures to guarantee this. Beyond those mentioned here, even more organizational measures have been made to boost the level of fail-safety further still.

4.1 24/7 Support

DocuWare Online is supported around the clock by an experienced support team. Any unexpected issues are reported and resolved on an ongoing basis (see point 7, "DocuWare Online Monitor – Performance Check"). Employees are warned about such instances via a multilevel system of email, monitor alerts, or text messages, depending on urgency, and are prepared to react appropriately.

4.2 Snapshot Backup

Together with the measures described in section 3.1, snapshots of the virtual machines in use are also created at regular intervals. This ensures that a server can be completely restored if there are any unexpected problems. The strict separation of data and functionality ensures that this measure is never applied to customer data or documents.

4.3 Logical Distribution of the Virtual Servers

For the best possible protection against hardware failures, the virtual DocuWare servers are operated on multiple host systems. This ensures that a failure of a physical hosting system would not effect more than one redundant component of the DocuWare system.

5 Performance

Thanks to DocuWare's multi-client capabilities, DocuWare Online 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 Online 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.

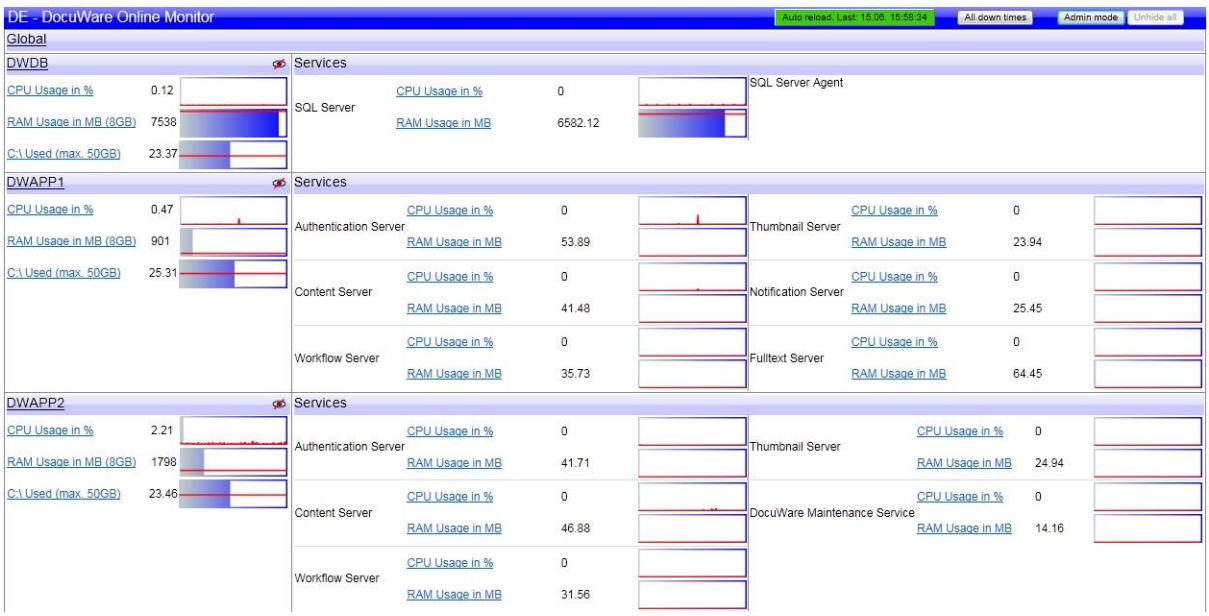
5.2 Dynamic Performance Adjustment

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. With the upcoming versions of Windows Server Datacenter Edition, it will be possible even without restarting.
- 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 Online Monitor – Performance Controls

All DocuWare servers and services are automatically monitored and report any system failures or performance bottlenecks immediately. A special service has been developed for this, which specifically monitors all the important parameters for our online system. These include the CPU load, working storage utilization, free hard disk space, and the accessibility of DocuWare services, among other things. 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 Online 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 at any time of day.



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 login agent must be defined and enabled in DocuWare Administration. The types of information to be logged can be specified during the configuration of login 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 Backup/Restore

DocuWare Online's existing standards already guarantee you optimum data security and availability. We can offer additional options for customers with special or unusually high requirements.

8.1 DocuWare Request

With DocuWare Request, you have the ability to make a copy of your data on an external storage medium, 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. To set up a DocuWare Request backup, please contact technical support.

8.2 Backup System

All web customers have the option of signing up for a complete backup system for their organizations. With this service, the backup system is updated with all changes to documents in the main system on a regular schedule. The documents can be restored from the backups at any time or are available for read access in a worst-case scenario. Primary and backup systems are always geographically separated on separate continents. Up to five users have access to their documents via Web Client as usual. To set this up, please contact our technical support.

9 Data Handover upon Termination of the Contract

If, upon termination of the contract, you wish to have a copy of all of your data in the form of a DocuWare Request (see "9.1 DocuWare Request"), this will of course be provided. Following termination of the contract, we will securely and irrecoverably delete all data.

10 Quality Guarantee

DocuWare regulary has its product and the company tested and certified by independent institutions: Three certifications prove, that also DocuWare Online meets the very highest of requirements as document management system.

DocuWare Online is certified as DMS

DocuWare is certified according to ISO 27001:2005. This standard specifies the requirements for the production, introduction, operation, monitoring, maintenance, and improvement of a document information security management system (ISMS). The focus of the certification is DocuWare Online.

DocuWare guarantees audit-compliant archiving

AO
GDPdU
Testiert

The DMS 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). This certification is especially important in Germany.

Quality management meets international standard

ISO 9001 www.isocert.de zertifiziert

As a DMS manufacturer, DocuWare meets the international standard DIN EN ISO 9001:2008, which acknowledges DocuWare a "good quality management system" in respect of "the development and sales of a standard software for document management.

11 Index

2

24/7 Support • 15

A

Access Control for Maintenance Administrators • 14
Access Control for Maintenance Users • 14
Architecture – Overview • 7

B

Backup System • 19
Backup/Restore • 19

D

Data Handover upon Termination of the Contract • 20
Document Encryption • 13
DocuWare Online Monitor – Performance Controls • 17
DocuWare Request • 19
DocuWare System • 10
Dynamic Performance Adjustment • 16

E

Encrypting Communication • 13

F

Fail-Safety • 15

H

Hosting • 7

I

Introduction • 5

L

Load Balancing • 16
Logging Users and Processes • 18
Logical Distribution of the Virtual Servers • 15

O

Objectives of This White Paper • 5

P

Performance • 16

Q

Quality Guarantee • 21

S

Security Concept • 13
Snapshot Backup • 15