
White Paper DocuWare Cloud

2.1

Oktober 2016

Impressum:

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

© Copyright 2016 DocuWare GmbH, alle Rechte vorbehalten.

Inhalt

1	Zielsetzung des White Papers	5
2	Einführung	5
3	Überblick Architektur	6
	3.1 Hosting.....	6
	3.1.1 Rechtlicher Hinweis	7
	3.2 DocuWare-System	8
4	Sicherheitskonzept	11
	4.1 Verschlüsselung der Kommunikation	11
	4.2 Verschlüsselung der Dokumente.....	12
	4.3 Zugriffskontrolle Wartungs-Administratoren	12
5	Performance	13
	5.1 Load Balancing	13
	5.2 Dynamische Performance-Anpassung.....	13
6	DocuWare-Cloud-Monitor: Performance-Kontrolle	14
7	Protokollierung von Benutzern und Vorgängen	15
8	Hinweise für Administratoren	16
	8.1 DocuWare Request	16
	8.2 Hotfixes und Upgrade des DocuWare Cloud-Systems.....	16
	8.3 Support	16
9	Datenübergabe bei Beendigung des Vertragsverhältnisses	17
10	Qualitätsgarantie	18

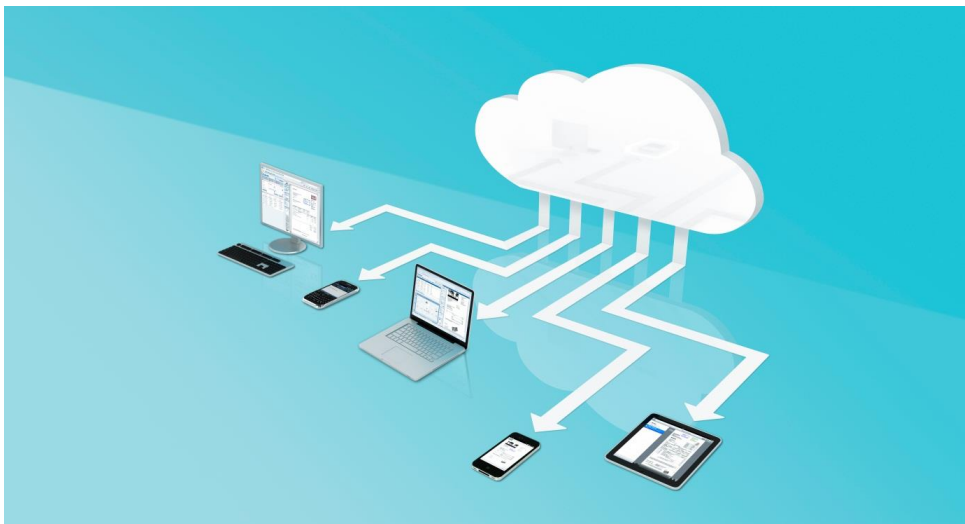
1 Zielsetzung des White Papers

Ihre Informationen sind Ihr Kapital! Mit unserer Dokumentenmanagement-Lösung DocuWare Cloud bieten wir Ihnen eine perfekte Verfügbarkeit und Sicherheit Ihrer Dokumente. Datensicherheit und Performance sind dabei das oberste Ziel der DocuWare GmbH und stehen immer an erster Stelle.

Dieses White Paper stellt die zur Daten- und Ausfallsicherheit getroffenen Maßnahmen dar. Es umfasst sämtliche Vorkehrungen gegen versehentliche oder vorsätzliche Manipulation der verwalteten Inhalte und gegen Datenverlust. Weiterhin gehören zu den Sicherheitsfunktionen Maßnahmen, die dazu dienen, den Datenschutz zu gewährleisten und durch DocuWare vollzogene Änderungen im System nachvollziehbar machen. Der Leser kann sich damit ein technisch fundiertes Urteil über Sicherheit und Aufbau des DocuWare Cloud-Systems bilden. Die technischen Mitarbeiter bei Kunden, Beratungsunternehmen, Fachzeitschriften und Vertriebspartnern werden gleichermaßen angesprochen. Vorausgesetzt wird lediglich ein technisches Grundlagenwissen über den Aufbau moderner Software-Anwendungen, idealerweise von Dokumentenmanagement-Systemen. Detaillierte Kenntnisse aktueller oder früherer Versionen von DocuWare sind nicht nötig.

2 Einführung

Cloud Computing ist eine alternative Form der Softwarenutzung: Via Internet und ohne klassische Software-Installation auf Ihrem lokalen Rechner können Sie mit DocuWare Cloud Dokumente ablegen, suchen, anzeigen, downloaden, bearbeiten und in Ihre Geschäftsprozesse einbinden. Ihre Dokumente sind dabei sicher in der Cloud gespeichert. Sie finden sich nach Eingabe Ihrer Benutzerkennung in Ihrer gewohnten Arbeitsumgebung und haben Zugriff auf alle Dokumente sowie Vorgänge jederzeit und an jedem Ort.



3 Überblick Architektur

Der Aufbau von DocuWare Cloud lässt sich in zwei große Bereiche gliedern:

- Hosting (Infrastruktur)
- DocuWare-System

Um eine größtmögliche Sicherheit und Performance zu bieten, arbeitet die DocuWare GmbH mit einem professionellen Hosters zusammen. Der Hosters übernimmt dabei den Betrieb der gesamten Infrastruktur von DocuWare Cloud in seinem Rechenzentrum.

3.1 Hosting

Nach sorgfältiger Überprüfung sowie ausgiebigen Tests wurde Microsoft Azure als Plattform für DocuWare Cloud gewählt. Diese Plattform bietet verschiedene Dienste, die es DocuWare Cloud ermöglicht, die Geschäftskontinuität für die Kunden zu sichern.

Mit modernster Virtualisierungstechnik wird die Hardware von der Software entkoppelt und dem Kunden über stabile virtualisierte Server-Ressourcen und Cloud-Services als Infrastruktur-Service zur Verfügung gestellt. Im Gegensatz zur realen Hardware lässt sich diese virtuelle Infrastruktur jederzeit flexibel und schnell an die aktuellen Bedürfnisse der Kunden anpassen. Somit ist das System darauf ausgerichtet, ideale Performance zu optimierten Kosten zu gewährleisten; unabhängig davon, wie viele Kunden sich aktuell auf unserem System befinden.

Allgemein

Die ständige Verfügbarkeit der Infrastruktur ist für einen Cloud-Service unerlässlich. Um dies zu gewährleisten, sind in allen Bereichen Maßnahmen getroffen, die einen Single-Point of Failure ausschließen und an vielen Stellen sogar eine drei- oder vierfache Absicherung kritischer Komponenten bieten.

Server

Alle Application Server laufen auf virtuellen Maschinen. Die Leistungsparameter dieser Maschinen können je nach Leistungsbedarf angepasst werden. Wir kümmern uns darum, dass die bei Microsoft Azure angeforderte Leistung auch tatsächlich zur Verfügung steht.

- Die einer virtuellen Maschine zugeordneten Ressourcen (CPU, Speicher etc.) stehen ausschließlich dieser Maschine zur Verfügung. Es erfolgt keine Mehrfachnutzung der Ressourcen durch verschiedene Kunden.
- Eine Anpassung der Anzahl an CPU-Kernen oder des Speicherausbaus kann jederzeit über eine grafische Oberfläche durchgeführt werden und steht nach einem Neustart der virtuellen Maschine sofort zur Verfügung.

Storage

Alle Dokumente werden auf dem Azure Files Service abgelegt. Dort abgelegte Dateien werden dreifach redundant gehalten. Die Dateien werden auf einen zweiten Standort mehrere hundert Kilometer entfernt gespiegelt und dort ebenfalls dreifach redundant gehalten. Auch die gespiegelten Daten bleiben hierbei im gleichen Wirtschaftsraum, das heißt Dokumente, die in der EU abgelegt wurden, verlassen die EU nicht und Daten, die in den USA abgelegt werden, verlassen die USA nicht.

Zusätzlich werden von uns die Dateien einmal wöchentlich zu Azure Blobs kopiert. Einmal kopierte Dokumente werden nicht gelöscht. Durch diese Kopien sind die Dokumente vor versehentlichem Löschen geschützt.

Weitere Informationen zu den verwendeten Diensten Azure Files und Azure Blobs finden sich unter <http://azure.microsoft.com/de-de/services/storage/>.

Netzwerk

Die Netzwerkinfrastruktur ist ebenfalls virtualisiert. Das virtuelle Netzwerk ist nach außen abgeschottet, so dass der gesamte Datenverkehr von außerhalb des Netzwerkes nicht eingesehen werden kann.

Die virtuellen Maschinen innerhalb eines virtuellen Netzwerks befinden sich innerhalb einer Windows-Domäne. Das erleichtert dem DocuWare Cloud Team die Administration des Systems, wenn zum Beispiel ein neuer Application Server hinzugeschaltet wird.

Datenspeicherung / Datensicherheit

Um den lokalen Gegebenheiten Rechnung zu tragen, werden Dokumente und Daten jeweils in der Region des Kunden gespeichert. Damit unterliegen der Betrieb des Systems und die Daten den jeweils lokalen Datenschutz-Richtlinien:

- Alle Kunden aus der Region EMEA werden in einem Rechenzentrum in der EU (Dublin) gehostet. Die Daten werden nach Amsterdam synchronisiert. Dabei werden die europäischen Datenschutzrichtlinien und das deutsche Bundesdatenschutzgesetz beachtet.
- Alle Kunden aus der Region Nord- und Südamerika werden in unserem Rechenzentrum in Iowa, USA, gehostet. Die Daten werden in das Rechenzentrum in Virginia gesichert. Sie unterliegen damit den US-Datenschutzrichtlinien.

3.1.1 Rechtlicher Hinweis

Für Kunden aus Deutschland weist DocuWare auf Folgendes hin: Soweit mit der Nutzung von DocuWare elektronische Bücher und sonst erforderliche elektronische Aufzeichnungen oder Teile davon außerhalb der Geltungsbereichs der deutschen Abgabenordnung (AO) geführt und aufbewahrt werden, bedarf dies gemäß § 146 Abs. 2a AO einer Bewilligung durch die zuständige Finanzbehörde. Deren schriftliche Beantragung ist Sache des Kunden. Eine unverbindliche Formulierungshilfe können Sie hier <https://www.docuware.com/main.asp?sig=dld&lan=de&loc=de&dwdblan=german&dwdbname=MUSTERANTRAG+DATENSPEICHERUNG+AUSLAND> herunterladen.

3.2 DocuWare-System

DocuWare erschließt Unternehmen die wertschöpfenden Potenziale von Dokumenten und deren Inhalten. Das Dokumentenmanagement-System DocuWare ist eine zertifizierte-Software für professionelles Enterprise Content Management (ECM) und revisionssichere elektronische Archivierung. Bei der Konzeption von DocuWare Cloud standen und stehen das Bestreben für eine optimale Performance sowie für den Schutz vor Sicherheitsmängeln beim Betrieb von DocuWare im Vordergrund.

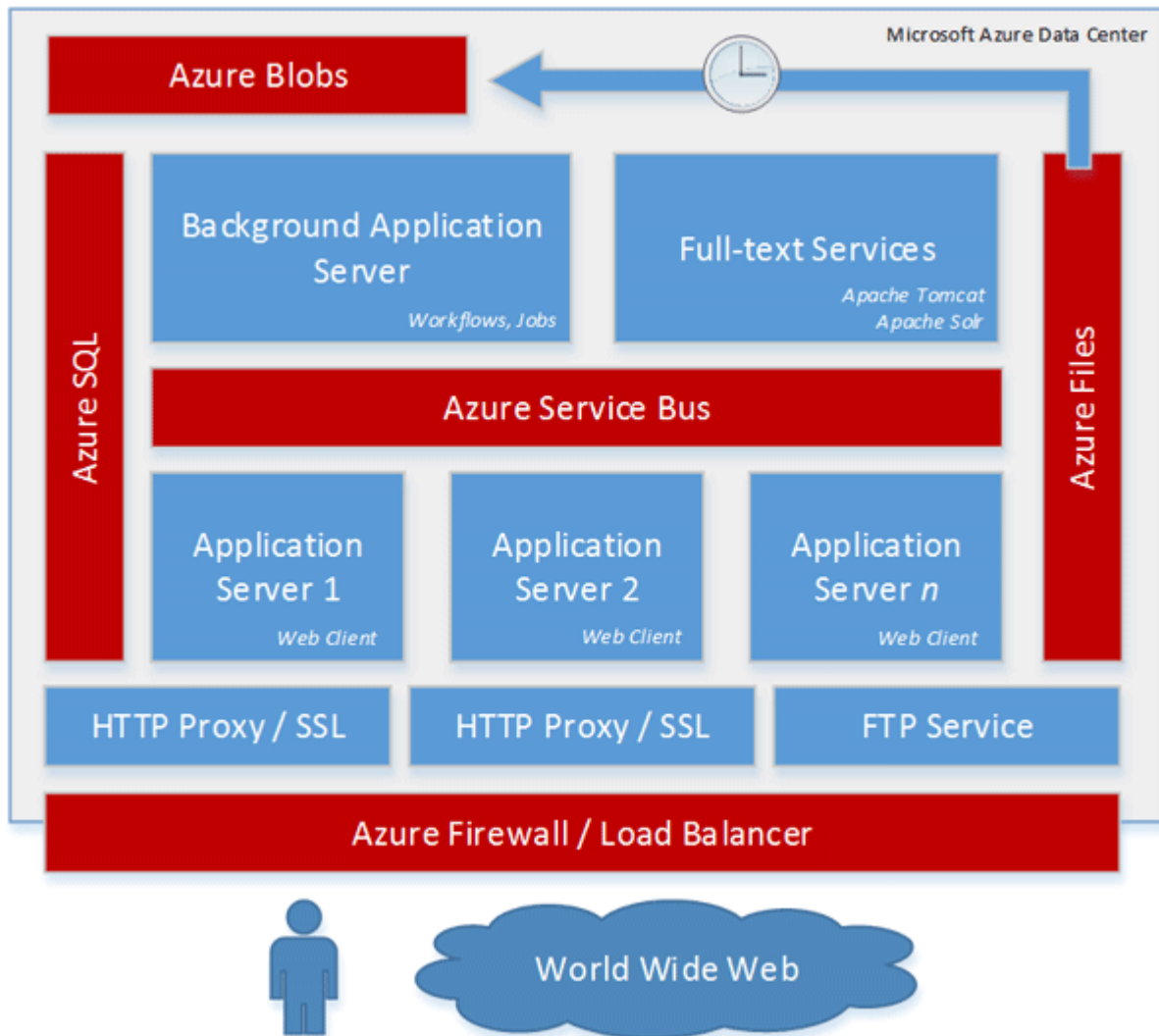
DocuWare Cloud besteht im Wesentlichen aus zwei Komponenten:

- Die **DocuWare-Organisationen** enthalten die verschlüsselten Kundendaten. Dabei besitzt jeder Kunde seine eigene spezifische Organisation, auf die nur er selbst Zugriff hat. Jede Organisation ist über ihre Organisations-ID eindeutig identifizierbar und komplett unabhängig von anderen Organisationen.
- Das **DocuWare-System** beinhaltet alle Server und Dienste zum Betrieb von DocuWare. Um auch im Fall eines Serverausfalls stets die volle Funktionsfähigkeit von DocuWare Cloud zu gewährleisten, sind alle Server redundant vorhanden. Sollte es zu einem Ausfall kommen, läuft das System auf den mehrfach vorhandenen Servern ohne Unterbrechung weiter.

Das **DocuWare-System** besteht aus den folgenden Komponenten:

Firewall mit Round-Robin-Lastverteilung. Die Firewall nimmt alle eingehenden Anforderungen entgegen und leitet sie an die passenden Application Server oder HTTP-Proxy weiter.

HTTP Proxy / SSL. Alle eingehenden HTTPS-Anfragen gelangen auf einen dieser Server. Dort wird die SSL-Entschlüsselung durchgeführt. Danach werden die entschlüsselten Anfragen an einen passenden Application Server delegiert. Wenn der Application Server die Anfrage bearbeitet hat, wird die Antwort per SSL verschlüsselt an den Nutzer ausgeliefert. Auch wenn die Last auf diesen Servern gering ist, gibt es mehrere Instanzen, um Ausfallsicherheit zu gewährleisten.



DocuWare Cloud baut auf die Azure Platform auf. Die roten Komponenten gehören zu Azure Platform, die blauen Komponenten zu DocuWare Cloud.

Application-Server. Diese Server arbeiten alle Anfragen an den WebClient oder die DocuWare Einstellungen ab.

Background Application Server. Dies ist ein spezieller Application Server, der Dienste für Hintergrundaufgaben (wie Workflow oder Autoindex) enthält.

FTP Service. Für den ScanToFTP-Dienst wird ein spezieller Server zur Verfügung gestellt.

Full-text Services. Diese Maschine verwaltet den Volltext für alle Nutzer. DocuWare verwendet dafür Apache Solr. Im Moment reicht ein einziger Server aus, da der Volltext nicht sehr häufig verwendet wird. Dennoch ist diese Lösung leicht skalierbar: Sollte sich eine größere Last abzeichnen, werden wir Solr Cloud verwenden.

Azure Files / Azure Blobs. Dort werden die Dokumente aller Nutzer verschlüsselt gespeichert. Azure Files hält bereits sechs redundante Kopien der Daten, zusätzlich kopiert das DocuWare-Team einmal pro Woche alle neuen Dateien zu Azure Blobs. Dort liegen die Daten ebenfalls verschlüsselt vor. Dadurch werden die Dateien vor versehentlichem Löschen geschützt.

Azure SQL ist eine skalierbare, "managed" SQL-Datenbank, die Microsoft Azure zur Verfügung stellt. Jeder Kunde hat seine eigene Datenbank. Sollte ein Kunde Datenbank-Operationen, wie etwa komplexe Suchen, durchführen, sind Datenbank-Operationen anderer Kunden davon nicht betroffen.

4 Sicherheitskonzept

Die Architektur des DocuWare Cloud-Systems wurde unter den Hauptgesichtspunkten **Datensicherheit** und **Nachvollziehbarkeit der administrativen Vorgänge** entworfen. Diese Maßnahmen beabsichtigen sicherzustellen, dass Dokumente nur von den entsprechend autorisierten Personen aufgerufen und verarbeitet werden können. Dies gilt für die Benutzer innerhalb eines Kundensystems sowie für das Gesamtsystem. Grundsätzlich erfolgt eine strikte Trennung zwischen

- **Kundendaten** (DocuWare-Organisationen)

und

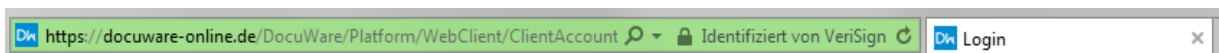
- **Systemdaten** (DocuWare-System)

Die Administratoren erhalten lediglich Zugriff auf die für den Betrieb von DocuWare Cloud nötigen Daten. Ein Zugriff auf Kundendaten ist jederzeit ausgeschlossen. Durch Auditing Services ist der Zugriff auf das DocuWare Cloud-System zu jeder Zeit nachvollziehbar.

4.1 Verschlüsselung der Kommunikation

Innerhalb des Datacenters sind die Daten über ein VPN abgesichert. Somit besteht keine Möglichkeit, Daten oder Informationen unverschlüsselt außerhalb oder innerhalb des Systems abzufangen. Siehe hierzu auch <https://msdn.microsoft.com/library/azure/jj156007.aspx>.

Für die Verschlüsselung des Datenverkehrs zwischen den Nutzern und dem Datacenter wird SSL verwendet. Das gilt sowohl für den HTTP-Verkehr als auch für den Remoting-basierten Verkehr. Durch Verwendung der Extended-Validation-Technologie wird dem Nutzer im Browser sofort durch eine Grünfärbung der Adressleiste eine gesicherte und validierte Verbindung angezeigt:



4.2 Verschlüsselung der Dokumente

Alle in Archiven gespeicherten Dokumente werden automatisch mit Hilfe des Krypto-Verfahrens AES (Advanced Encryption Standard) verschlüsselt. Bei AES handelt es sich um den Nachfolger von DES (Data Encryption Standard). AES ist eines der derzeit sichersten symmetrischen Verschlüsselungsverfahren. Es ist als US-Verschlüsselungsstandard von der US-Regierung für Dokumente mit der höchsten Geheimhaltungsstufe (Top Secret) zugelassen und erfüllt höchste Sicherheitsanforderungen.

Dabei wird für jedes Archiv ein asymmetrisches Schlüsselpaar generiert. Der private Schlüssel wird dazu verwendet, die symmetrischen Schlüssel zu verschlüsseln, die im Rahmen der Verschlüsselung der Dokumente eines Archivs entstehen. Der private Schlüssel des Archivs wird wiederum mit einem Master Key verschlüsselt.

Für einen maximalen Schutz setzt DocuWare bei der Verschlüsselung auf AES mit einer Schlüssellänge von 256 Bit. Für die Verschlüsselung der symmetrischen Schlüssel wird eine Schlüssellänge von 4096 Bits verwendet. Für jedes Dokument wird ein neuer symmetrischer Schlüssel generiert. Dies erhöht die Sicherheit, da für eine Krypto-Analyse nur relativ wenige verschlüsselte Daten zur Verfügung stehen.

4.3 Zugriffskontrolle Wartungs-Administratoren

Für bestimmte Tätigkeiten sind volle (oder umfangreiche) Administrationsrechte an den DocuWare Cloud-Systemen notwendig. Um auch in diesem Fall ein höheres Maß an Datensicherheit zu erreichen, unterliegen Zugriffe für Wartungs-Administratoren einer Protokollierung. Folgende Sicherheitsmechanismen sind installiert:

- Alle Zugriffe auf DocuWare Cloud-Systeme erfolgen per RDP-Sitzung.
- Jeder Administrator hat seine eigene Kennung. So kann jederzeit nachvollzogen werden, wer sich an welchem System angemeldet hat.
- Um eine RDP-Sitzung starten zu können, muss man sich in ein VPN einwählen. Dieses VPN ist über Zertifikate abgesichert, die nur den Administratoren zur Verfügung stehen.
- Alle Administratoren sind geschult und wurden insbesondere auf sensiblen Umgang mit Daten wie Zertifikate und Passwörter hingewiesen.

5 Performance

Aufgrund der Mehrmandanten-Fähigkeit von DocuWare Cloud ist DocuWare Cloud in der Lage, die vorhandenen Ressourcen optimal zu nutzen. Dabei spielt es keine Rolle, ob eine Organisation sehr große Last erzeugt (z.B. durch viele Benutzer) oder nur sehr geringe Last. Allen Benutzern stehen immer die komplette Rechen- und Storage-Performance zur Verfügung. Zudem kann in kürzester Zeit auf Schwankungen reagiert werden und es können zusätzliche Kapazitäten zum System hinzugefügt werden.

5.1 Load Balancing

Die Last auf dem DocuWare Cloud-System wird grundsätzlich auf alle verfügbaren Server verteilt. Dies trägt zu einer ausgeglichenen Nutzung der verfügbaren Server bei und stellt eine gleichbleibend hohe Performance des Gesamtsystems sicher. Werden vordefinierte Grenzwerte überschritten, können in kurzer Zeit zusätzliche Kapazitäten (CPU-Leistung oder Speicher) oder komplette virtuelle Server hinzugefügt werden. Dies geschieht abhängig vom jeweils betroffenen Teil des DocuWare-Systems.

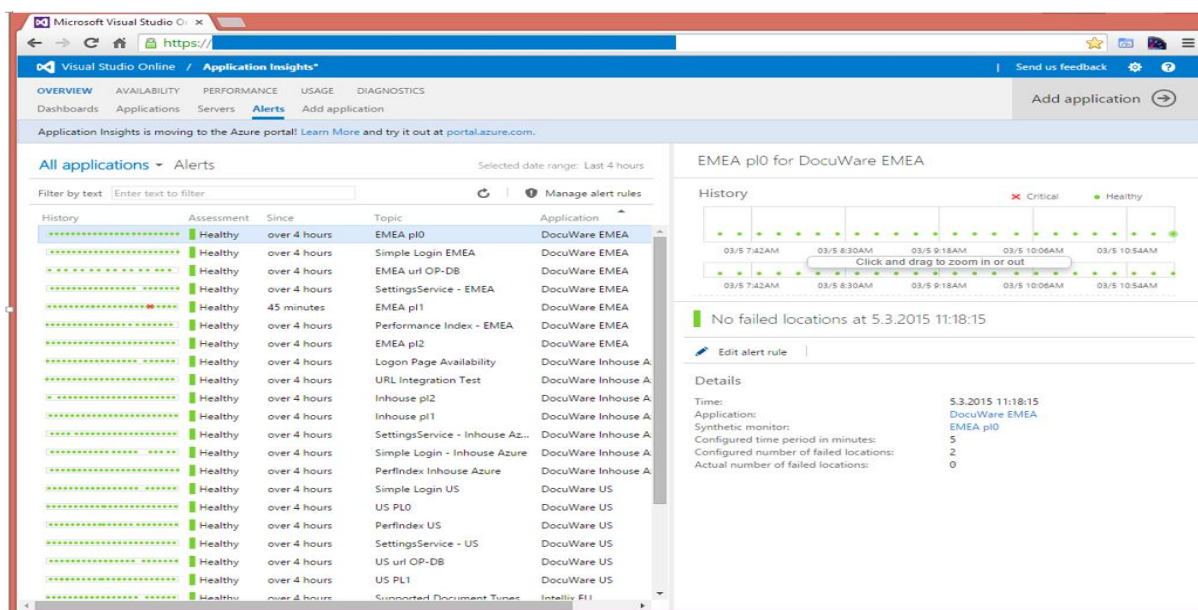
5.2 Dynamische Performance-Anpassung

Um schnell und flexibel auf schwankende Lastzustände reagieren zu können, stehen unserem Support-Team mehrere Möglichkeiten zur Verfügung:

- **Erweiterung der vorhandenen virtuellen Server** durch Hinzufügen von zusätzlichen Prozessorkernen oder zusätzlichem Speicher. Dies geschieht innerhalb von Sekunden und wird nach einem Neustart der virtuellen Maschine sofort wirksam. Durch den ausfallsicheren Aufbau des kompletten Systems kann diese Maßnahme im laufenden Betrieb ohne Unterbrechung durchgeführt werden.
- **Hinzufügen von kompletten virtuellen Servern**, die entweder im Wartezustand geparkt sind und einfach hochgefahren werden, oder durch die Bereitstellung eines neuen virtuellen Servers auf Basis eines vorkonfigurierten Installationspaketes.

6 DocuWare-Cloud-Monitor: Performance-Kontrolle

Alle DocuWare-Server und -Dienste werden automatisch überwacht und melden Ausfälle oder Performance-Engpässe umgehend an DocuWare. Microsoft Azure bietet mit Application Insights einen Dienst, der alle wichtigen Parameter des DocuWare-Cloud-Systems überwacht. Zudem werden in regelmäßigen Abständen komplette Funktionstests durchgeführt, die Login, Ablage, Suche und andere wichtige Funktionen in DocuWare prüfen. Sollte dabei ein Fehler auftreten oder sollten die Tests nicht in der vorgegebenen Zeit abgeschlossen werden können, so wird umgehend das DocuWare-Cloud-Support-Team informiert. Abhängig von der Dringlichkeit geschieht dies entweder per E-Mail oder per SMS. Bei höchster Dringlichkeitsstufe wird der Fehler sofort gemeldet und durch das 24x7-Bereitschaftsteam behoben.



Der Azure-Dienst Application Insights überwacht die wichtigen Parameter des Cloud-Systems.

7 Protokollierung von Benutzern und Vorgängen

Um stets alle Vorgänge innerhalb einer DocuWare-Organisation nachvollziehen zu können, bietet DocuWare umfangreiche Protokollierungsmöglichkeiten. So kann jederzeit problemlos nachvollzogen werden, wer innerhalb Ihrer Organisation ein Dokument gelöscht oder verändert hat. Hierfür muss in der DocuWare Administration ein Logging-Agent definiert und aktiviert werden. Bei der Konfiguration der Logging-Agenten lässt sich genau festlegen, welche Informationen protokolliert werden sollen:

- Aktionen, z.B. Versenden von Dokumenten
- Archive, z.B. das Buchführungsarchiv
- Benutzer oder Benutzergruppen, z.B. Administratoren
- Eine Kombination von Parametern

8 Hinweise für Administratoren

DocuWare Cloud bietet zusätzliche Unterstützung für den laufenden Betrieb, etwa durch Backups von Dokumenten, durch ein bequemes Upgrade und Support.

8.1 DocuWare Request

Mit DocuWare Request haben Sie die Möglichkeit, einmalig oder in regelmäßigen Abständen eine Kopie Ihrer Daten oder von bestimmten Dokumenten zu erhalten. Der Umfang des Backups ist dabei vom Kunden frei definierbar. So kann beispielsweise halbjährlich eine inkrementelle Sicherung eines Archivs angefordert werden. Die so erzeugten Daten können jederzeit in eine DocuWare-Organisation eingespielt oder unabhängig von einem DocuWare-System über das mitgelieferte Abfrageprogramm recherchiert und angezeigt werden.

8.2 Hotfixes und Upgrade des DocuWare Cloud-Systems

Das DocuWare Cloud System wird immer mit der neuesten DocuWare Version betrieben. Deshalb wird etwa alle sechs Monate die aktuelle DocuWare Version eingespielt. Wir empfehlen, auch die lokal installierten Komponenten auf dem neuesten Stand zu halten. Anwender können das Update problemlos selber ausführen, sofern sie zur lokalen Installation von Software berechtigt sind. Ist dies nicht der Fall, übernimmt das Update der IT-Administrator in der Regel mit einer Software Management Solution. Damit das Upgrade auf zahlreichen PCs in einem Unternehmen schnell von statten geht, lässt sich eine unbeaufsichtigte Installation ("silent install") der DocuWare-Komponenten einrichten, siehe dazu auch die Support FAQs
https://www.docuware.com/support_faq/index.php?solution_id=3838.

Kunden werden zu neuen Versionen und Updates etwa vier Wochen im Voraus benachrichtigt.

8.3 Support

DocuWare Cloud wird von einem erfahrenen Support-Team rund um die Uhr betreut. Sobald Sie Kunde von DocuWare Cloud sind, können Sie sich auch im Support Forum <https://www.docuware.com/forum/english-forums/docuware-announcements/docuware-cloud-emea-status-information> registrieren. Hier werden alle geplanten und ungeplanten Ausfallzeiten offen kommuniziert. Auf Wunsch erhalten Sie bei jeder neuen Meldung sofort eine E-Mail-Benachrichtigung.

9 Datenübergabe bei Beendigung des Vertragsverhältnisses

Sollten Sie sich zur Beendigung des Vertragsverhältnisses entschließen, unterstützen wir Sie auf Wunsch dabei, Ihre Dokumente vom DocuWare Cloud-System zu laden und/oder in ein anderes System zu migrieren. Dafür gibt es folgende Möglichkeiten:

1. Kleinere Datenmengen mit Dokumenten, die nicht zeitnah oder gar nicht mehr bearbeitet werden müssen, können Sie in Form eines DocuWare Request (siehe das Kapitel "DocuWare Request") erhalten.

2. Für größere Datenmengen sowie für Dokumente, die in aktuelle Prozesse eingebunden sind, empfehlen wir, den kostenpflichtigen DocuWare Professional Service in Anspruch zu nehmen. Dies bringt Ihnen folgende Vorteile:

- Der Professional Service PS kann nach Absprache und Freigabe durch den Kunden auf die Dokumente des Kunden im Datacenter zugreifen und deshalb auch große Datenmengen ohne lange Verzögerung übergeben.
- Manche Dokumententypen sind in aktuelle Prozesse eingebunden und müssen zeitnah bearbeitet werden. Wenn der Arbeitsablauf länger ins Stocken gerät, kann sich dies negativ auf den Umsatz auswirken. Mit dem speziellen Know-How des Professional Service können Sie dies vermeiden und lebende Dokumente zeitnah in die Prozesse eines neuen Systemes migrieren.
- Die erfahrenen Mitarbeiter vom Professional Service können kundenspezifische Lösungen entwickeln, die speziell auf die Arbeitsabläufe und die verwendeten Dokumententypen im Unternehmen zugeschnitten sind.

Im Anschluss an die Beendigung des Vertragsverhältnisses werden alle Daten von uns sicher und unwiderruflich gelöscht. Ein Restore ist ab diesem Zeitpunkt nicht mehr möglich.

10 Qualitätsgarantie

In der DocuWare Cloud werden Ihre Daten durch international führende Best Practices zum Thema Sicherheit geschützt. Ihre Daten sind in der DocuWare Cloud also sicher. Zudem sind die Verfahren und die Infrastruktur, auf denen das cloudbasierte Dokumentenmanagement Ihres Unternehmens beruht, von unabhängiger Seite geprüft und zertifiziert:

ISO 27001



Informationssicherheit ist für Sie entscheidend und ISO 27001 ist der anerkannte Standard für ein dokumentiertes Managementsystem für Informationssicherheit (ISMS). DocuWare bietet eine systematische und klar strukturierte Methode für die Verwaltung von sensiblen Unternehmensdaten, so dass sie zuverlässig geschützt sind. Sowohl das Personal als auch die Prozesse und das IT-System Ihres Unternehmens werden im zugrundeliegenden Risikomanagement-Prozess berücksichtigt.

HGB/AO, GoBS und GDPdU



Das Dokumentenmanagementsystem unterstützt die Anforderungen an die Archivierung aufbewahrungspflichtiger Dokumente nach den Grundsätzen einer ordnungsgemäßen Buchführung und gewährleistet die revisionssichere Langzeitarchivierung nach HGB/AO, GoBS und GDPdU gemäß dem Prüfungsstandard PS 880 des Instituts der Wirtschaftsprüfer (IDW).

ISO 9001



Qualität ist unser größtes Anliegen. Das Qualitätsmanagementsystem, das DocuWare verwendet, ist nach ISO 9001 zertifiziert. Die Norm basiert auf mehreren Richtlinien für Qualitätsmanagement mit Schwerpunkt auf dem Kunden.

SOC 2 Attestations (früher SAS 70)



Überprüfen Sie sorgfältig, wem Sie die Informationen Ihres Unternehmens in der Cloud anvertrauen. Mit DocuWare als Servicenbieter können Sie sich darauf verlassen, dass Ihre Daten sicher sind. DocuWare Cloud erfüllt die strikten Standards, welche vom renommierten American Institute of Certified Public Accountants (AICPA) vorgegeben werden – und zwar nicht nur mit seiner Software, sondern auch mit der Infrastruktur, der verschiedensten Verfahren im Umgang mit Daten und im Personalwesen.

Die SOC - oder Service Organization Controls - umfassen eine Reihe von Kriterien zu Kontrollen bezüglich Sicherheit, Verfügbarkeit, Prozessintegration, Vertraulichkeit und/oder Datenschutz für Service-Dienstleister. In der Vergangenheit haben viele Dienstleister die SAS 70 Berichte genutzt, um eine Konformität mit den Best Practices im Handling von Finanzberichten zu sichern. SOC ersetzt nun den SAS 70 Standard. Die SOC 2-Berichte sind fokussiert auf Service-Dienstleister, wie Anbieter von Cloud Software (SaaS).

Hinweis: Beachten Sie bitte die Informationen [in diesem FAQ-Artikel](#), um sicherzustellen, dass Ihre Organisation in der DocuWare Cloud SOC 2-konform ist.

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



Um das Risikomanagement eines Cloudanbieters einschätzen zu können, ist die Cloud Controls Matrix (CCM) eines der besten Werkzeuge, die die Industrie zu bieten hat. Die CCM beinhaltet grundlegende Sicherheitsprinzipien für Cloudanbieter. Unser Hosting Provider hält genaue Informationen darüber vor, wie mit dem Hosting die Anforderungen an Sicherheit, Datenschutz, Richtlinienkonformität und Risikomanagement erfüllt werden - diese Anforderungen sind in der CCM Version 1.2 festgelegt. Der Report wird im Security Trust der CSA und im Assurance Registry (STAR) aufgeführt und kann Ihnen auf Wunsch zur Verfügung gestellt werden.

ISO/IEC 27017:2015

Der Hostservice Microsoft Azure ist konform mit der Norm ISO/IEC 27017:2015, die Richtlinien für Kontrollen zur Informationssicherheit zur Verfügung stellt. Diese Richtlinien ergänzen Kontrollen, wie sie in der ISO /IEC 27002 spezifiziert sind und beziehen sich besonders auf Cloudservices. Von der zertifizierten Informationssicherheit profitieren wir als Cloudservice, der von Microsoft Azure gehostet wird, wie auch Sie als unsere Kunden.