White Paper Sicherheit

Version 2.0

DocuWare

Inhalt

Dieses Dokument wurde erstellt mit AuthorIT™, Total Document Creation (http://www.author-it.com).

Disclaimer

Dieses Dokument wurde mit größter Sorgfalt zusammengestellt und die Informationen darin sind Quellen entnommen, die als zuverlässig gelten. Dennoch kann keine Haftung übernommen werden für die Richtigkeit, Vollständigkeit und Aktualität der Informationen. Aus den in diesem Dokument aufgenommenen Informationen können keine Ansprüche hergeleitet werden. Die DocuWare GmbH behält sich das Recht vor, jegliche Informationen, die in diesem Dokument enthalten sind, ohne vorherige Ankündigung zu verändern.

DocuWare GmbH
Therese-Giehse-Platz 2
82110 Germering
www.docuware.com (http://www.docuware.com)

1 Einführung

Dieses White Paper stellt die Sicherheitsmaßnahmen innerhalb der DocuWare-Software dar. Schwerpunkte sind Zugangs- und Zugrifssicherheit, die Vermeidung von Serverausfällen und Datenverlust sowie der Schutz der Dokumente vor Missbrauch und Manipulation. Auch werden die Verifizierung des Dokumenturhebers anhand einer elektronischen Signatur und die Nachprüfbarkeit von Dokumentänderungen beschrieben. Es werden die zugrunde liegenden Technologien behandelt sowie ihre Anwendung im DocuWare-System.

Angesprochen sind die technischen Mitarbeiter bei Kunden, Beratungsunternehmen, Fachzeitschriften und Vertriebspartnern gleichermaßen. Vorausgesetzt wird lediglich technisches Grundlagenwissen über den Aufbau von Software-Applikationen, idealerweise von Dokumenten-Management-Systemen sowie Kenntnisse der DocuWare-Architektur und Komponenten.

Informationen zum Aufbau des DocuWare-Systems entnehmen Sie bitte dem White Paper Systemarchitektur. (http://help.docuware.com/de/#t54927) Hier werden auch die einzelnen Komponenten ausführlich beschrieben. Die wichtigsten DocuWare-spezifische Begriffe sind im Glossar (auf Seite 39) erklärt.

2 Zugangssicherheit

Das DocuWare-System ist vor missbräuchlichen Zugriff durch einen sicheren Datenaustausch der Komponenten untereinander sowie durch ein komplexes Loginverfahren geschützt.

2.1 Kommunikation absichern

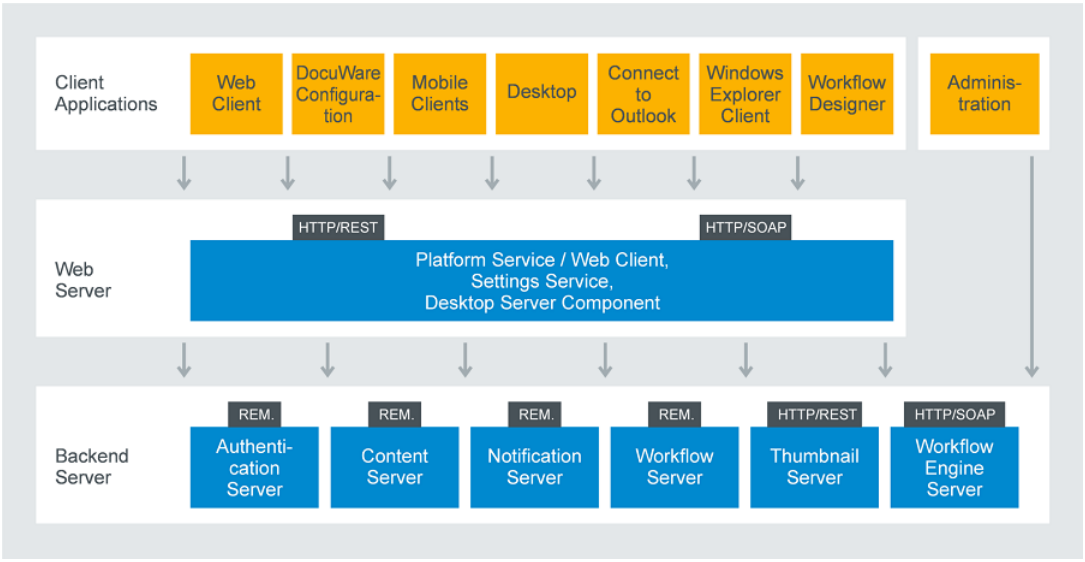
DocuWare nutzt für die Kommunikation der einzelnen Software-Komponenten untereinander die folgenden TCP-basierten Protokolle.

Standardmäßig ist die Verschlüsselung der Protokolle deaktiviert. Der System-Administrator kann die Sicherheitsprotokolle jedoch für jede ein- und ausgehende Serververbindung aktivieren.

- **HTTP/HTTPS (Übertragung von HTML oder Binärdaten)**
  Standardmäßig ist HTTP unverschlüsselt. Um mit diesem Protokoll sicher über Internet zu kommunizieren, sollten Sie es mit SSL verschlüsseln (HTTPS). Dafür ist ein Zertifikat auf dem Server mit den IIS (Internet Information Services) erforderlich.

- **HTTP/HTTPS mit REST (Representional State Transfer)**
  Vor allem der DocuWare Platform Service läuft vollständig REST-basiert.

- **HTTP/HTTPS mit SOAP (Simple Object Access Protocol)**
  SOAP dient dem Austausch von Nachrichten, die auf dem XML Information Set beruhen. Im DocuWare-System wird SOAP von verschiedenen Web Servern in der Kommunikation mit den Client-Anwendungen eingesetzt.



Die Kommunikation zwischen den Schichten Client-Anwendungen, Web Server und Backend Server

Mehr Informationen zu den Kommunikationstechnologien von DocuWare finden Sie im White Paper Systemarchitektur http://help.docuware.com/de/#t61140.

2.1.1 TCP Verschlüsselung

Die Einstellungen für TCP-basierte Kommunikation können in der DocuWare Administration geändert werden. Für jeden Kommunikationskanal eines Servers lässt sich „SSL", oder „Windows-Sicherheitseinstellungen" wählen. Werksseitig ist zunächst „Keine Sicherheitseinstellungen" aktiviert.

Mit der Funktion „Windows-Sicherheitseinstellungen" stehen Microsoft NTLM und Kerberos als unterstützte Protokolle zur Verfügung. Wegen der höheren Sicherheit empfehlen wir Kerberos. Lediglich, wenn das Partner-System dies nicht unterstützt wird, beispielsweise bei älteren Windows-Versionen, sollte NTLM vergewendet werden.

Bei Kerberos handelt es sich um ein sogenanntes „Ticket Granting Protocol" (siehe auch Kapitel Login über TCP Verbindungen (auf Seite 8)). Es wurde am MIT in Boston entwickelt, ist ein IETF-Standard und wird weithin unterstützt.

Mehr Information zur Konfiguration zu Kerberos (http://www.docuware.com/support_faq/index.php?action=artikel&cat=7&id=1319&artlang=de&highlight=kerberos) erhalten Sie beim DocuWare Support.

Der Zugriff von Clients aus dem Internet oder Intranet auf die DocuWare-Server erfolgt nach einer Verifikation der Identität der Kommunikationspartner immer über verschlüsselte Kommunikationskanäle. Für die Kommunikation außerhalb von Domänen und über öffentliche Zugangskanäle wird die SSL-Verschlüsselung empfohlen.

Für die SSL-Kommunikation müssen die Server über ein entsprechendes Zertifikat verfügen, das im Windows-Zertifikatsspeicher des jeweiligen Computers abgelegt ist.

2.1.2 HTTP Verschlüsselung

Um mit HTTP sicher über Internet zu kommunizieren, sollten Sie es mit SSL verschlüsseln (HTTPs). Dafür ist ein Zertifikat auf dem Internet Information Server erforderlich. Bestimmte Systemkomponenten müssen dann neu in der Konfiguration angepasst werden.

Mehr Informationen auch dazu gibt es beim DocuWare Support (http://www.docuware.com/support_faq/?action=search&search=ssl+zertifikat&submit.x=0&submit.y=0).

2.2 Authentication Server: Zentrale für Zugangssicherheit

Der Authentication Server verwaltet sämtliche Benutzer, Lizenzen und Rechte des Systems. Die Nutzung des Systems erfordert zunächst immer eine Anmeldung am Authentication Server. Er ist somit zuständig für die Zugangssicherheit, d.h.

- das Login der Benutzer,
- die Lizenzverwaltung,
- die Verwaltung der benutzerspezifischen Einstellungen.

Da DocuWare mandantenfähig ist, sind Benutzer „Organisationen" zugeordnet, die über den Authentication Server verwaltet werden. Eine Organisation ist eine logische Struktur, sie umfasst:

- Benutzer und Benutzergruppen
- Logische Archive, inklusiv zugehöriger Platten
- Prozesse
- Templates für Stempel, Erkennungsschemata, Auswahllisten

Pro DocuWare-System existieren ein oder mehrere Authentication Server, die organisationsübergreifend agieren. Um Ausfällen vorzubeugen, kann der Authentication Server redundant installiert sein, mehr dazu im Kapitel Ausfallsicherheit (auf Seite 26).

Benutzt wird der Authentication Server von

- einer oder mehrere Organisationen mit jeweils
- mindestens einem oder Hunderten von Benutzern.

DocuWare arbeitet mit internen User-IDs statt mit dem Benutzernamen des Logins. Nur diese User-IDs dienen als Datenbank-Schlüssel. Somit können Benutzer jederzeit umbenannt werden, ohne die zugeordneten Einstellungen ändern zu müssen.

Bei der Anmeldung eines Benutzers überprüft der Authentication Server auch die Lizenzen pro Organisation und Benutzer. Es werden sowohl „Concurrent Licenses" als auch „Named Licenses" unterstützt.

2.3 Login

2.3.1 Login-Verfahren

Das Login in DocuWare erfolgt immer über den Authentication Server. Das Login-Verfahren enthält gleichzeitig die Prüfung der für den Nutzer verfügbaren Lizenzen. Authentication Server unterstützt die folgenden Authentifizierungsmethoden:

- **DocuWare-Login**
  Der Benutzer muss sich über Namen und Kennwort, wie in DocuWare hinterlegt, als berechtigt ausweisen.
- **Trusted Login (Single-Sign-On)**
  Der Client identifiziert sich ohne weitere Benutzereingabe über den Login-Namen des Windows-Betriebssystems. Der Authentication Server prüft den Login mittels der Benutzerverwaltung von Windows.
  Damit dieses Verfahren verwendet werden kann, müssen sich Client und Server im selben Windows Domain Netzwerk befinden. Da immer häufiger mobile Lösungen und zentral gehostete Lösungen verwendet werden, wird dieser Logintyp vermutlich seltener zum Einsatz kommen. Trusted Login ist auch nicht bei DocuWare online verfügbar.
- **Login Token**
  Login Tokens werden in der Regel nur für Single-Sign-ons zwischen DocuWare-Komponenten verwendet. Damit muss sich der Benutzer nur einmal bei DocuWare anmelden, auch wenn er beispielsweise zuerst den Web Client und dann die Web Client Einstellungen aufruft. Authentication Server stellt dazu ein Login Token für einen Benutzer aus, wenn dieser sich für Anwendung A hinreichend authentifiziert hat, und übermittelt dieses verschlüsselt zur Anwendung B.

2.3.2 Login über TCP Verbindungen

Um bei Komponenten, die über TCP miteinander kommunizieren, sicheren Zugriff zu gewährleisten, arbeitet DocuWare mit einem „Ticket-Granting-Ticket" (TGT). Der Benutzer beziehungsweise Client identifiziert sich am Authentication Server und fordert einen Service an. Er erhält dafür ein „Ticket" und kann mit diesem Ticket den Service eines anderen Servers, z.B. eines Content Server, nutzen.

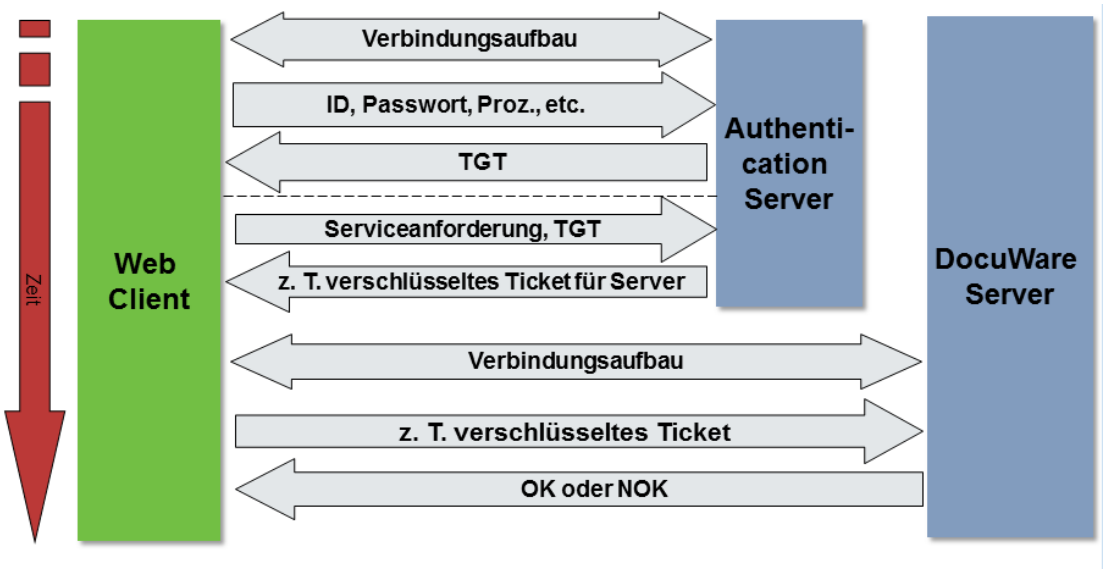


Abbildung 6: Mit dem Ticket-Granting-Verfahren beim Login wird Zugriffssicherheit gewährleistet.

Der Ablauf der Authentifizierung wird im Folgenden skizziert. Die einzelnen Schritte laufen nacheinander ab, wie oben in der Grafik dargestellt.

2.3.2.1 Schritt 1: Client-Anmeldung beim Authentication Server

Genereller Ablauf der Anmeldung beim Authentication Server:

1 Client etabliert eine sichere, das heißt verschlüsselte Kommunikationsverbindung mit dem Authentication Server.

2 Nur DocuWare-Login: Der Client fragt beim Benutzer Benutzerkennung und Passwort ab.

3 Client identifiziert sich gegenüber Authentication Server durch Kennung und Passwort beziehungsweise durch das Ticket, das er von der Windows-Verwaltung erhalten hat.

4 Der Authentication Server prüft die Informationen, erstellt ein „Ticket-Granting-Ticket (TGT)" und sendet es an den Client. Außerdem wird die Lizenznutzung vermerkt. Das heißt, dass eine Lizenz bis zum Logout (oder Timeout) blockiert wird.

2.3.2.2 Schritt 2: Client-Serviceanforderung bei Authentication Server

Nach der Anmeldung kann der Client bei dem Authentication Server die Nutzung von Services nach folgendem Verfahren beantragen:

1 Client übergibt folgende Informationen an den Authentication Server:
a. Gewünschter Backend-Server (Content Server, Workflow Server, oder andere)
b. Zusätzlich benötigte Parameter, zum Beispiel Identifikation des logischen Archivs
c. Das oben erhaltene TGT

2 Authentication Server bestimmt den zu nutzenden Server, je nach der konfigurierten Lastenverteilung.

3 Schließlich sendet der Authentication Server dem Client ein zeitlich limitiertes Ticket für diesen Server. Das Ticket enthält unter anderem einen Session Key für die Kommunikation zwischen Client und Server.

2.3.2.3 Schritt 3: Client-Anmeldung bei zugewiesenem Server

Mit diesem Ticket wendet sich der Client nun an den vom Authentication Server zugewiesenen Server. Er folgt dabei folgendem Verfahren:

1 Client baut eine sichere Verbindung mit dem zu nutzenden Server auf und übergibt das vom Authentication Server erhaltene Ticket.

2 Server wertet die enthaltenen Informationen des Tickets aus und überwacht die Gültigkeit des Tickets.

3 Server sendet eine Bestätigung an den Client und ist nun bereit, Anforderungen entgegenzunehmen.

Ist das Ticket abgelaufen, ist es Aufgabe des Clients eine Verlängerung des Tickets bei dem Authentication Server einzufordern. Der Ablauf ähnelt dem Verfahren zum Erhalt eines neuen Tickets. Da aber der gleiche Session Key benutzt wird, kann die Session ohne Verlust fortgesetzt werden.

2.3.2.4 Schritt 4: Client-Logout bei Authentication Server

Am Ende einer Session muss sich der Client ordnungsmäßig bei dem Authentication Server abmelden. Dazu baut der Client eine sichere Verbindung zum Authentication Server auf und übergibt sein Ticket-Granting-Ticket. Daraufhin gibt der Authentication Server die Lizenz wieder frei.

Lizenzen können immer nur für eine vorgegebene Zeit belegt werden. Fällt der Client aus, wird die Lizenz über ein Timeout wieder frei. Nach einem Ausfall und Neustart des Authentication Server werden ebenfalls blockierte Lizenzen wieder freigegeben.

2.3.3 Login via HTTP

Die Anmeldung bei mit HTTP kommunizierenden Komponenten basiert auf Cookies. Einmal verifizierte Anmeldedaten werden verschlüsselt in einer kleinen Textdatei gespeichert. Dieses Cookie wird beispielsweise genutzt, um den Benutzer bei einem erneuten Öffnen des Browsers automatisch zu verifizieren.

Authentication Server lässt sich jedoch nicht direkt über HTTP ansprechen. Deshalb adressieren HTTP-basierte Anwendungen zunächst Web Client Server oder die Platform Services. Diese mittlere Serverschicht leitet die Anmeldedaten dann zum Authentication Server weiter. Nach der erfolgreichen Authentifizierung wird das Cookie für den Client bereitgestellt.

Proxy Server und Firewalls können zwischengeschaltet werden, obwohl sie keinen Einfluss auf diese Anmeldeprozedur nehmen. Vorausgesetzt, dass die Clients über HTTPs kommunizieren, können die Logindaten nicht abgefangen werden.

2.3.4 Passwörter

Benutzernamen und Passwörter werden in DocuWare generell verschlüsselt beziehungsweise als Hash-Wert abgespeichert. Dies gilt auch für Systemeinstellungen, wie zum Beispiel das Login beim Datenbank-Server.

Konkret wird das sogenannte „salted" Hash-Verfahren verwendet, bei dem durch Kombination mit einem Zufallswert auch bei zwei identischen Passwörtern nicht der gleiche Hash-Wert entsteht. Passwörter sind damit weder lesbar, noch reproduzierbar.

Hat der Benutzer sein Passwort vergessen, kann er über den Anmeldedialog des Web Client ein automatisch generiertes Passwort anfordern. Damit ist es möglich, sich im Web Client einzuloggen und ein neues persönliches Passwort einzugeben.

Alternativ dazu kann auch der Organisationsadministrator das Passwort zurücksetzen. Dies ist für Benutzer mit der Sicherheitsstufe „Hoch" allerdings nicht möglich, siehe auch Kapitel DocuWare als Hochsicherheitssystem (auf Seite 19). Benutzer mit hoher Sicherheitsstufe können ihre Passwörter nur selber erneuern.

In der DocuWare Administration lässt sich zudem festlegen, wie komplex Passwörter zu sein haben, beispielsweise ob ein Groß- oder Kleinbuchstabe, eine Ziffer oder ein Sonderzeichen in der Zeichenfolge enthalten sein müssen. Auch lässt sich die minimale Zeichenzahl eines Passworts festlegen, wie lange es gültig bleibt und ab wie vielen falschen Passworteingaben der Zugang gesperrt wird. Der Organisationsadministrator kann zudem das Passwort-Zeitlimit für bestimmte Benutzer wieder deaktivieren. Dies ist beispielsweise dann nützlich, wenn sich Workflows als Benutzer bei einem Server anmelden müssen.

2.3.5 Anmeldedaten für andere Systeme

Alle sensiblen Daten wie Logindaten für andere Systeme, das Datenbankserver-Passwort, das Passwort für den Mail-Server oder LDAP-Passwörter werden verschlüsselt gespeichert, so dass nur die Serverkomponenten diese entschlüsseln können. Damit sind diese Daten sicher, auch wenn bestimmte Benutzer auf diese Datenbanken zugreifen können, etwa für Backup-Zwecke.

3 Rechteverwaltung

Mitarbeiter in großen Organisationen haben mit komplexen Abläufen zu tun und unterliegen vielen Regularien. Um ihre Aufgaben erfüllen zu können, benötigen sie Berechtigungen zur Benutzung vorhandener Ressourcen, z.B. Dokumenten- und IT-Funktionen. Dabei sind auch Beschränkungen erforderlich, um nur berechtigten Personen bestimmte Befugnisse erteilen zu können und um die Übersichtlichkeit für alle Beteiligten zu erhalten.

DocuWare bietet ein Rechtekonzept, das auch solch komplexe Szenarien abbilden kann. Für jeden Anwender lässt sich der Handlungsspielraum detailliert definieren.

3.1 Definition der Begriffe

3.1.1 Rechte

Grundlegend für die Rechteverwaltung in DocuWare ist die Unterscheidung in funktionale Rechte und Archivrechte. Zusätzlich können für bestimmte Objekte Benutzer- und Administratorrechte definiert werden.

- **Funktionale Rechte**
  Einem Benutzer können verschiedene funktionale Rechte eingeräumt werden. Dazu gehören beispielsweise die Rechte, den Web Client sowie dessen Dialoge und Briefkörbe zu verwalten, E-Mail-Benachrichtigungen in der DocuWare Konfiguration zu konfigurieren und vieles mehr.
- **Archivrechte**
  Über die Archivrechte ist festgelegt, welche Zugriffsmöglichkeiten einem Benutzer hinsichtlich der archivierten Dokumente und Indexdaten zur Verfügung stehen. Die Rechte umfassen das Ablegen und Suchen von Dokumenten, das Ändern von Indexeinträgen oder den Export von archivierten Dokumenten in das Dateiverzeichnis. Für einen Benutzer können pro Archiv verschiedene Archivrechte vergeben werden.

Benutzer- und Administratorrechte
Einige Objekte können Benutzern und Rollen als Administrator oder Benutzer zugeordnet werden. Dies umfasst beispielsweise Briefkörbe, OCR-Einstellungen, Importkonfigurationen und viele andere. Mit dem Benutzerrecht lässt sich das Objekt verwenden, das Administratorrecht enthält das Recht, das Objekt beziehungsweise die zugehörige Konfiguration zu ändern.

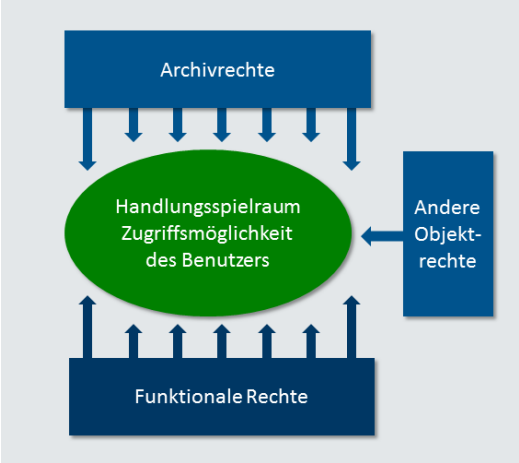


Abbildung 7: Mit der komplexen Rechtestruktur vom DocuWare-System lässt sich der Handlungsspielraum eines Benutzers präzise festlegen.

3.1.2 Profile und Rollen

Über Profile und Rollen ist es möglich, anstelle von vielen Einzelrechten in "Containern" zusammengefasste Rechte zu vergeben. Die Vergabe von Rechten über Profile und Rollen hat zwei Vorteile:

Erstens können detailliert zusammengestellte Rechte auf Knopfdruck an beliebig viele Benutzer vergeben werden, ohne dass ein Administrator pro Benutzer per Hand die komplexe Rechtestruktur anpassen muss.

Zweitens können Zusammenstellungen von Rechten auch ohne Benutzer existieren. Falls ein Mitarbeiter die Firma verlässt, kann ein Nachfolger - ohne großen Aufwand - die gleichen Rechte zugewiesen bekommen, unabhängig davon wie detailliert die Rechtezuweisung im Einzelnen ist.

- **Profile**
  Rechte können zu funktionalen oder Archivprofilen zusammengefasst werden. Sie lassen sich einzelnen Benutzern und Rollen zuteilen.
- **Rollen**
  Mehrere Profile lassen sich zu einer Rolle zusammenfassen. Eine Rolle kann sowohl Profile mit funktionalen Rechten als auch Profile mit Archivrechten umfassen. Rollen können Gruppen und einzelnen Benutzern zugewiesen werden.

3.1.3 Benutzer und Gruppen

Die einzelnen DocuWare-Benutzer können zu verschiedenen Gruppen zusammengefasst werden. Dabei ist es auch möglich, dass ein Benutzer Mitglied mehrerer Gruppen ist.

- **Benutzer**
  Für jeden Mitarbeiter, der DocuWare verwenden soll, wird mindestens ein Benutzer angelegt. Das Rechtespektrum erhalten Benutzer über die Zuweisung einzelner Rechte oder Rechtebündelungen in Form von Profilen und Rollen.
  Benutzer können Gruppen angehören.
- **Gruppen**
  Benutzer, die über die gleichen Funktionalitäten verfügen und die gleichen Archivrechte besitzen sollen, lassen sich zu Gruppen zusammenfassen. Entsprechende Rechte erhält

der einzelne Benutzer über die Zugehörigkeit zu der Gruppe, der die entsprechende Rolle zugewiesen ist.

3.1.4 Ererbte und explizite Rechte

Bei der Zuweisung von Rechten zu Benutzern unterscheidet DocuWare zwischen ererbten und expliziten Rechten.

- **Ererbtes Recht**
  Rechte, die ein Benutzer über die Zugehörigkeit zu einer Gruppe oder über eine Rolle bzw. ein Profil erhalten hat, sind ererbte Rechte.
- **Explizites Recht**
  Rechte, die ein Benutzer direkt erhält und nicht über Rolle, Profil oder Gruppe, sind explizite Rechte. Es können nur funktionale Rechte als explizite Rechte vergeben werden.

Rechte sind immer additiv. Das heißt, die Summe der ererbten Rechte und der expliziten Rechte eines DocuWare-Benutzers bilden den Handlungsspielraum dieses Benutzers.

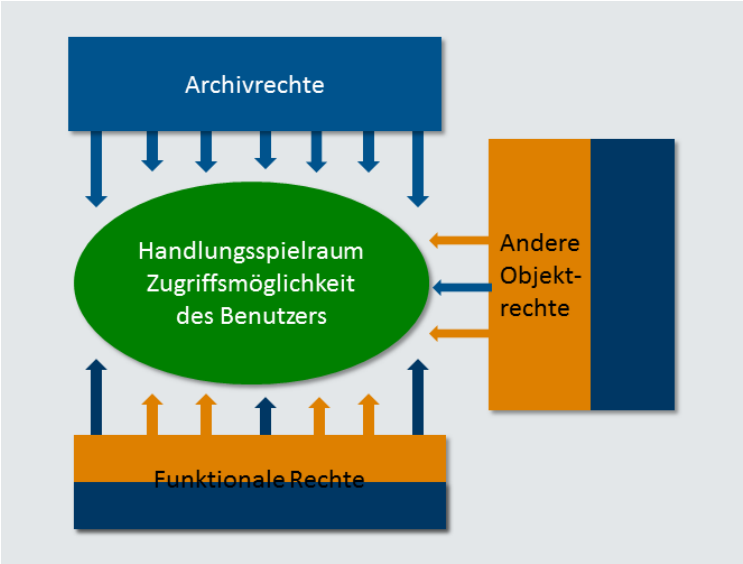


Abbildung 8: Explizite Rechte, hier orange markiert, werden direkt zu Benutzern zugeordnet. Oder der Benutzer erbt ein Recht von einer Rolle oder einer Gruppe (blau).

3.2 Zuweisung der Rechte

Mit den im vorigen Kapitel beschriebenen Möglichkeiten lassen sich die Rechte flexibel an die jeweilige Organisation anpassen. Gruppen – als Zusammenfassung von Benutzern – und Rollen – als Zusammenfassung von Rechten – sind dabei verschiedene Sichtweisen auf dieselbe Sache. Einmal sind die Mitarbeiter und entsprechend die Benutzer der Ausgangspunkt, das andere Mal die Arbeitsabläufe beziehungsweise die Funktionen im DocuWare-System.

3.2.1 Vergabe der Funktionsrechte

Durch die funktionalen Rechte wird festgelegt, welche Funktionen einem DocuWare-Benutzer im Web Client, in der DocuWare Konfiguration oder anderen Modulen zur Verfügung stehen. Des Weiteren wird ein Teil seines Handlungsrahmens in der DocuWare-Administration bestimmt.

Durch die Zuweisung der einzelnen Menüfunktionen als Rechte lässt sich genau festlegen, welche Funktionalitäten einem Benutzer im DocuWare-System zur Verfügung stehen. Wenn ein Benutzer beispielsweise nicht das Recht hat, Briefkörbe zu verwalten, wird das Modul gar nicht angezeigt, wenn der Benutzer die DocuWare Konfiguration aufruft.

3.2.2 Einstellungen auf Archivebene

Archivrechte werden in jedem Fall zu Profilen zusammengefasst. Es ist nicht möglich Archivrechte - direkt einzeln Benutzern zuzuweisen. Nur die Archivprofile können Benutzern bzw. Rollen zugewiesen werden.

Genauso wie die funktionalen Rechte sind auch die Archivprofile additiv. Das heißt, werden einem Benutzer mehrere Archivprofile eines Archivs zugewiesen, erhält er alle Rechte, die diesen Profilen gemeinsam sind. Weiterhin bedeutet dies, dass Rechte nicht eingeschränkt, sondern nur erweitert werden können. Dieses Verhalten wird im Kapitel Zusammenspiel der Rechte (auf Seite 18) näher erläutert.

Archivrechte können in administrative und allgemeine Archivrechte sowie in Feldrechte unterteilt werden.

- **Archivrechte**
  Administrative Archivrechte sind zum Beispiel: Archivrechte für Benutzer ändern, Such- und Ablagemasken sowie Ergebnislisten zu diesem Archiv erstellen und das Archiv migrieren. *Allgemeine Archivrechte* sind zum Beispiel Ablegen, Suchen und Dokument löschen.
  Die Archivrechte beziehen sich immer auf jeweils ein Archiv mit allen darin enthaltenen Dokumenten. Für verschiedene Archive können verschiedene Archivrechte vergeben werden.
- **Feldrechte**
  Zusätzlich zu den allgemeinen Archivrechten können Rechte auf Feldebene vergeben werden. Diese Rechte beziehen sich nur auf das entsprechende Feld, nicht auf alle Felder des Archivs. Zu den Feldrechten gehören unter anderem das Suchrecht, das Recht, Feldinhalte zu ändern, und das Recht, Einträge zu verwenden, die nicht in einer Auswahlliste vorhanden sind.

(Um innerhalb eines Archivs Rechte nach Indexeinträgen vergeben zu können, stehen zudem Indexfilter zur Verfügung. Die Limitierung der Dokumentenzugriffe über Indexdaten bietet sich insbesondere dann an, wenn Dokumente sensiblen Inhalts in einem Archiv zusammengefasst werden. Beispiel: In einem Personalarchiv sind die Dokumente der Mitarbeiter gespeichert. Als Indexeintrag steht unter anderem der Mitarbeitername zur Verfügung. Mitarbeiter der Personalabteilung haben Zugriff auf alle Dokumente, während der einzelne Mitarbeiter nur auf die Dokumente Zugriff hat, die mit seinem Namen in den Indexdaten abgelegt sind.)

3.2.3 Benutzer- und Administratorrecht zuweisen

Damit ein Benutzer für ein Objekt das Benutzer- und Administratorrecht zuweisen kann, muss diesem Benutzer in der DocuWare Administration zunächst das funktionale Recht zugewiesen sein, wie etwa, OCR-Einstellungen zu verwalten. Dann wird das entsprechende Modul in der DocuWare Konfiguration angezeigt, sobald der Benutzer sich anmeldet. Er kann nun eine OCR Einstellung anlegen und wählen, welche Benutzer oder Gruppen diese Konfiguration verwenden und/oder verwalten können sollen.

3.2.4 Vordefinierte Rollen

Nach der Erstinstallation existieren in jedem DocuWare-System vordefinierte Rollen mit vordefinierten Profilen, um die Verwaltungsaufgaben ebenfalls dem Berechtigungskonzept zu unterwerfen. Diese vordefinierten Rollen können verschiedenen Benutzern oder Benutzergruppen zugewiesen werden.

System-Administrator

Der System-Administrator verwaltet das System aus Sicht der generell benötigten Basiskomponenten und der Hardware. Dazu gehören unter anderem die Verwaltung der Datenbankverbindungen, der Kommunikationswege und der Ablagepfade der Dokumente.

Der System-Administrator kann so definiert werden, dass er keinen Zugriff auf einzelne Organisationsinformationen hat und insbesondere nicht in die detaillierte Benutzerverwaltung eingreifen kann. Allerdings kann nur er die Rolle „System-Administrator" anderen Benutzern zuweisen. Dies ist nicht in der Benutzerverwaltung der Organisation möglich.

Nach der DocuWare-Installation übernimmt er gleichzeitig die Rolle des Organisations-Administrators für alle Organisationen. Mit jeder neu erzeugten Organisation übernimmt der System-Administrator zunächst automatisch auch die Rolle des Organisations-Administrators, die dann aber einer anderen Person zugewiesen werden kann.

Aufgaben System-Administrator

- Hardware, Betriebssystem, Datenbank
- Installation DocuWare-Server-Module

Konfiguration systemweiter Einstellungen zu:

- Server wie Authentication Server, Content Server und andere
- Verbindungen für Datenbanken, Dateiverzeichnisse, SAP-Remote-Verbindungen
- Speichersysteme
- Benutzerverzeichnisse
- Protokollierung

Organisations-Administrator

Ein DocuWare-System kann eine oder auch mehrere Organisationen mit jeweils eigenem Organisations-Administrator umfassen. Der Organisations-Administrator verwaltet insbesondere die Rechte, Benutzer und Benutzergruppen seiner Organisation. Die Rolle beinhaltet keine Zugriffsrechte auf Archive und deren Verwaltung.

Zur Übernahme dieser Rolle ist kein technisches Detailwissen der IT-Umgebung erforderlich. Der Organisations-Administrator kann die Rolle auch anderen Benutzern zuordnen oder entziehen. Insbesondere kann die Rolle auch einem System-Administrator entzogen werden.

Aufgaben Organisations-Administrator (je Organisation)

- Lizenzen
- Client-Systeme und Briefkörbe
- Stempel/Signaturen
- Viewer und Fremdapplikationen
- Auswahllisten
- Validierungen
- Benutzer und Gruppen
- Protokollierung
- Workflows

Archiv-Besitzer

Das Recht des Archiv-Besitzers wird vom DocuWare-System automatisch der Person zugeordnet, die das Archiv anlegt. Sie kann dieses Recht sowie auch andere Rechte zur Erledigung von Verwaltungsaufgaben an andere Benutzer weitergeben.

Der Besitzer verwaltet die Archivstruktur, z.B. Index- und Plattenstruktur, und vergibt die Zugriffsrechte auf das Archiv, in dem er Archivprofile erzeugt. Bezogen auf das Archiv macht der Besitzer ebenfalls die Vorgaben für den Organisations-Administrator, damit dieser die Zuordnungen der Archivprofile zu Benutzern bzw. Rollen vornehmen kann.

Aufgaben Archiv-Besitzer (je Archiv)

- *Volltextindexierung*
- *Benutzte Datenbank-Verbindung*
- *Dokumentablage und Plattenkonzept*
- *Indexfelder*
- *Rechte für das Archiv*
- *Dialoge für Ablage, Suchen und Ergebnisliste*
- *Protokollierung*

3.2.5 Objektrechte: Benutzer oder Administrator

Benutzerrecht für die Konfiguration eines Objekts in den Web-Client-Einstellungen beispielsweise eines Briefkorbs bedeutet, dass der entsprechende Benutzer dieses Objekt verwenden, aber nicht die jeweilige Konfiguration ändern darf. Administratorrecht meint, dass der Benutzer das Objekt ändern, aber nicht benutzen darf. Es ist möglich, beide Rechte einem Benutzer zuzuweisen, so dass er die Konfiguration nutzen und ändern darf.

Objekte mit Administrator- oder Benutzerrechten:

- *Briefkörbe*
- *Smart Connect*
- *E-Mail-Benachrichtigungen*
- *MFP-Workflow*
- *OCR Vorlagen,*
- *Connect to Outlook*
- *Import*
- *Printer*
- *Connect to Mail*
- *Request*

3.2.6 Zusammenspiel der Rechte und Berechtigungen

Mitglied mehrerer Gruppen, Besitzer mehrerer Rollen oder Profile

Rechte sind immer additiv. Das heißt, die Summe der zugewiesenen Rechte eines DocuWare-Benutzers bildet den Handlungsspielraum dieses Benutzers.

Ist ein Benutzer Mitglied mehrerer Gruppen, hat er alle Rechte, die über diese Gruppen und ihre Rollenzuteilung verfügbar sind.
Sind einem Benutzer mehrere Rollen oder Profile zugewiesen, hat der Benutzer alle Rechte zusammen, die über diese Rollen beziehungsweise Profile zugeteilt werden.

Beispiele:

- Ein Benutzer hat sein Rechtespektrum über eine Rolle erhalten. Weist man diesem Benutzer eine weitere Rolle mit weniger Rechten zu, ändert sich für den Benutzer nichts, da die Rechte additiv sind. Um ihm die Rechte einzuschränken, muss man ihm die ursprüngliche Rolle entziehen. Entsprechendes gilt auch für Gruppen.

Ein Benutzer ist Mitglied zweier Gruppen und hat über die Rollen dieser Gruppen sein Rechtespektrum erhalten. Entzieht man ihm die Mitgliedschaft einer Gruppe, so verliert er nicht automatisch alle Rechte, die ihm über die Rollen dieser Gruppe zugewiesen sind, sondern nur diejenigen, die über die andere Gruppe nicht zugeteilt werden.

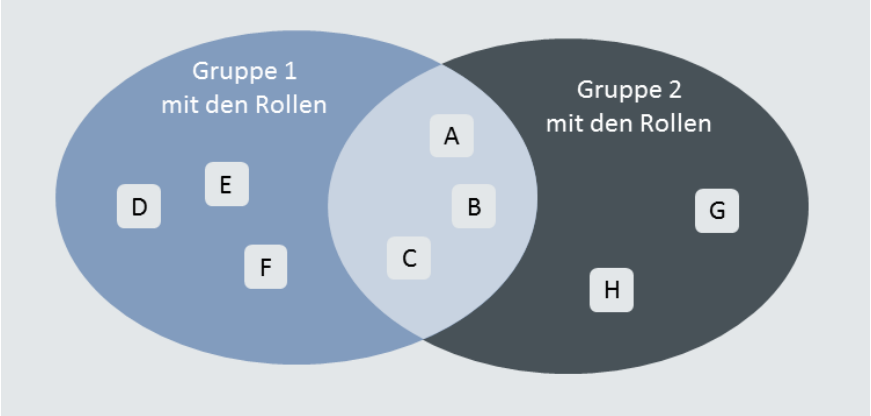


Abbildung 09: Entzieht man einem Benutzer die Mitgliedschaft der Gruppe 2, so verliert er nur die Rollen G und H, da er über die Rollen A, B und C noch über die Gruppe 1 verfügt. Entsprechendes gilt auch für Rollen und Profile, die einem Benutzer zugewiesen sind.

Dialogeinstellungen und Archivrechte

Die Möglichkeiten, die ein Benutzer in einem Archiv hat, resultieren aus den Archivrechten, die ebenfalls die Dialoge umfassen.

- Eine Ergebnisliste enthält in der Werkzeugliste standardmäßig den Button „Als PDF mit Anmerkungen herunterladen". Ein Benutzer hat nun das Archivrecht „Export" und kann diese Option verwenden. Der andere hat das Export-Recht nicht, weshalb der Button zum Herunterladen eines PDF mit Anmerkungen ausgegraut ist. Er kann diese Funktion nicht nutzen.

Feldeinstellungen und Archivrechte

Die Einstellungen zu den einzelnen Archivfeldern und die zugewiesenen Archivrechte überschneiden sich in einigen Bereichen. So ist es möglich, ausgewiesenen Benutzern spezielle Rechte zur Verfügung zu stellen, während „normale" Benutzerrechte über die Feldeinstellungen gesteuert werden. Ein Beispiel:

- Ein Archivfeld im Speicherdialog ist als „Fester Wert" belegt. Ein Benutzer hat wiederum das Recht, Indexeinträge zu ändern. Dieser Benutzer ist demnach berechtigt, den festen Feldeintrag im Speicherdialog oder / oder in der Infobox der Ergebnisliste zu ändern.

Die Archivrechte eines Benutzers haben also Vorrang gegenüber den Feldrechten.

3.3 DocuWare als Hochsicherheitssystem

Wenn ein DocuWare System auf „Hichsicherheitssystem" gesetzt wird, kann der Organisationsadministrator die Eigenschaft „Hochsicherheit" bestimmten Benutzern und Archiven zuteilen. Nur ein Benutzer mit dieser Eigenschaft kann auf ein Hochsicherheits - Archiv zugreifen. Folgende Unterschiede gibt es zu einem System ohne die Eigenschaft „Hochsicherheit":

- Der Organisations-Administrator kann nicht für einen Hochsicherheits-Benutzer das Passwort zurücksetzen. Nur der Benutzer selbst hat dann die Möglichkeit, das Passwort zu ändern.

- Für solche Benutzer ist es auch nicht möglich, sich über ein Trusted Login (siehe Kapitel Login-Verfahren (auf Seite 8)) anzumelden, da beim Trusted Login die Sicherheit nicht über DocuWare gewährleistet wird.
- Es ist nicht möglich für ein Hochsicherheits-Archiv die Archiv-Profile einer Rolle zuzuweisen. Diese Archiv-Profile müssen Benutzern direkt zugewiesen werden und diese Benutzer ebenfalls über die Eigenschaft „Hochsicherheit" verfügen. Somit ist ausgeschlossen, dass für besonders sensible Bereiche ein Zugriff per Zufall über Gruppen- und Rollenzuweisungen erfolgen kann.

4 Sicherheitsmaßnahmen für Archive und Dokumente

Neben dem Authentifizierungssystem und dem Berechtigungskonzept existieren weitere Maßnahmen, um die Ablagen gegen Missbrauch und Dateninkonsistenz zu schützen. Dazu gehören unter anderem die Sperrung von Dokumenten, die überarbeitet werden, die Verschlüsselung von Ablagen und der Einsatz von Stempeln und elektronischen Signaturen.

4.1 Content Server Transaktionen für Datenkonsistenz

Wenn Dokumente gespeichert werden, fallen Aktualisierungen sowohl in der Datenbank als auch im Dateisystem an. Um die Einheitlichkeit des Datenbestandes im Falle eines Serverausfalls zu gewährleisten, wurde der Speichervorgang als Transaktion im Content Server integriert. Wenn Schrittfolgen einer solchen Transaktion nicht abgeschlossen werden können, werden die bereits ausgeführten Änderungen automatisch rückgängig gemacht. Damit sind Datenbank und Dateisystem in jeden Fall auf dem gleichen Stand.

4.2 Dokumenten-Sperrung in Archiven

Um zu verhindern, dass zwei Benutzer gleichzeitig ein Dokument ändern, ist es möglich, ein zu bearbeitendes Dokument für andere Benutzer zu sperren. Diese können das Dokument zwar betrachten, aber nicht mit Anmerkungen oder Stempeln versehen. In der DocuWare Administration lässt sich der Modus festlegen, in welchem sich ein Dokument standardmäßig im Web Client von der Ergebnisliste öffnet. Es sind drei Modi möglich:

- Bearbeiten-Modus: Wenn ein Dokument in diesem Modus geöffnet wird, kann es bearbeitet werden. Es ist dann für andere Benutzer im Archiv gesperrt, sobald es angezeigt wird. Sobald das Dokument wieder geschlossen wird, wird die Sperrung aufgehoben.
- Ad-hoc-Bearbeiten-Modus: Dieser Modus ist standardmäßig eingestellt. Die Dokumente werden zunächst im Read-Only-Modus geöffnet und sind im Archiv nicht gesperrt. Sobald ein Benutzer ein Bearbeitungswerkzeug aktiviert, wird das Dokument für die Bearbeitung freigegeben und im Archiv gesperrt.
- Read-only: Ein Dokument kann angezeigt, aber nicht bearbeitet werden. Es können also keine Kommentare und keine Stempel gesetzt werden.

Sämtliche Sperrdaten werden in der Datenbank vermerkt. Spezielle Mechanismen sorgen dafür, dass Sperren und Freigaben auch nach dem Ausfall des Clients, der Anwendung oder des Servers wieder in einen konsistenten Zustand gebracht werden.

4.3 Versionsmanagement: Nachvollziehen von Änderungen

Wenn Versionsmanagement für ein Archiv aktiviert ist, speichert DocuWare die Änderungen an einem Dokument in einer neuen Dokumentversion. Das Original und die älteren Versionen bleiben im Archiv. Das bearbeitete Dokument wird gesperrt, so dass nicht zwei Benutzer aus Versehen gleichzeitig das selbe Dokument ändern.

Sie können Versionsmanagement manuell oder automatisch einsetzen:

- Manuell: Der Benutzer checkt ein Dokument aus dem Archiv aus, entweder ins Dateiverzeichnis oder in einen Briefkorb. Sobald ein Dokument ausgecheckt wurde, ist es im Archiv gesperrt. Andere Benutzer können es nur betrachten. Wenn das Dokument wieder ins Archiv eingecheckt wird, erhält es eine höhere Versionsnummer. Diese kann der Benutzer bei Bedarf selber eingeben wie auch Anmerkungen zur neuen Version einfügen.
- Automatisches Versionsmanagement ist im Hintergurnd aktiv, ohne dass der Benutzer manuell eingreifen muss. Auch hier wird ein zu bearbeitendes Dokument gesperrt. Die Änderungen werden in einem Dokument mit einer automatischen Versionsnummer gespeichert. Sie können ein Dokument auch von dem Archiv auschecken, aber dann wird automatisch das manuelle Versionsmanagement aktiviert.

Bei beiden Varianten des Versionsmangements werden ältere Versionen und das Original im Archiv vorgehalten und können in der Versionsübersicht samt unter anderem Nummer, Status, Speicherdatum und Kommentar betrachtet werden.

Der Status eines Dokuments macht kenntlich, um welche Dokumentenversion es sich handelt. Dieser kann "Aktuell" für das neuste Dokument sein, "In Bearbeitung" für ein ausgechecktes oder für ein bereits in DocuWare geöffnetes Dokument sowie "Veraltet" für eine Version, die nicht mehr aktuell ist.

Die Indexkriterien ändern sich nicht, wenn eine neue Version erstellt wird, so dass die Versionen zunächst die gleichen Indexkriterien haben. Sie können die Indexkriterien bei der aktuellen Dokumentversion ändern, diese werden jedoch nicht automatisch auf die alten Versionen übertragen.

4.4 Verschlüsselte Archive

Um sicherzustellen, dass selbst Administratoren keine sensiblen Dokumente lesen können, lassen sich in DocuWare Dokumente verschlüsselt speichern. Optional können auch die jeweiligen Header-Dateien verschlüsselt werden.

Volltext-Dateien können nicht durch DocuWare verschlüsselt werden, siehe dazu auch das Kapitel Sensible Daten außerhalb von DocuWare schützen (auf Seite 24). Die Indexdaten in der Datenbank sind ebenfalls nicht verschlüsselt. Enthalten die Indexdaten sehr sensible Informationen, ist auf die Sicherungsmöglichkeiten des Datenbank-Anbieters zurückzugreifen.

Es ist zu beachten, dass verschlüsselte Ablagen für autorisierte Nutzer nur bei Verfügbarkeit des entsprechenden Schlüssels nutzbar sind. Dabei sind die Schlüssel für die Entschlüsselung der Dokumente im Dokument-Header gespeichert. Die Dokument-Schlüssel werden über ein asymmetrisches Verfahren mit einem in der Datenbank gespeicherten Schlüssel entschlüsselt. Da die Dokumente ohne den Schlüssel in der Datenbank nicht entschlüsselt werden können, muss bei verschlüsselter Ablage darauf geachtet werden, dass von den DocuWare-System-Tabellen ein regelmäßiges Backup erstellt wird, um bei Verlust der Datenbank insbesondere die Schlüssel-Tabellen wieder herstellen zu können.

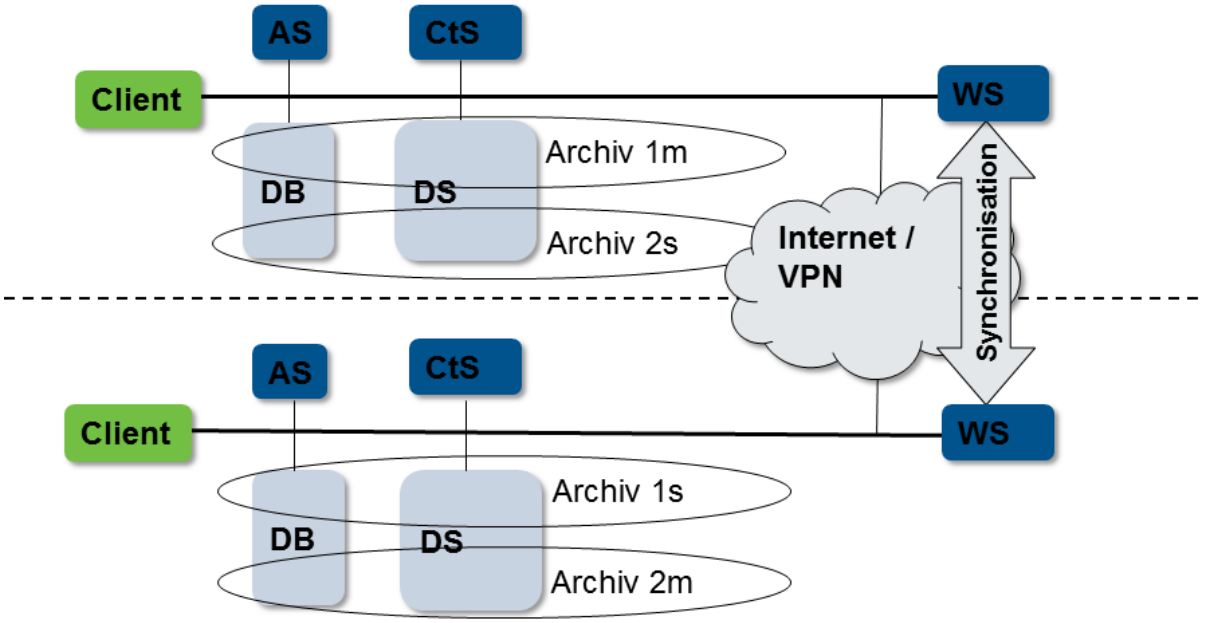
4.5 Backup eines Archivs per Synchronisation

DocuWare erlaubt die Synchronisation zweier Archive. So können Dokumente in einem oder mehreren DocuWare-Systemen gleichzeitig gespeichert werden, beispielsweise um ein Backup von bestimmten Dokumenten anzufertigen.

Die Synchronisation umfasst Dokumente und Datenbank. Ausgangspunkt einer Synchronisation ist immer ein Quellarchiv, das Masterarchiv. Ziel ist immer ein so genanntes Satellitenarchiv. Das kann beispielsweise ein DocuWare-Archiv auf einem Laptop sein, der ohne Netzzugang mit den aktuellen Dokumenten aus einem Masterarchiv arbeiten können muss.

Master- und Satellitenarchiv können unterschiedliche Strukturen haben. Bei der Definition des Workflows können die Datenbankfelder zugewiesen werden. Es können sämtliche Dokumente oder nur einige, ausgewählte Dokumente eines Archivs in das Satellitenarchiv übernommen werden. Um zu bestimmen, welche Dokumente synchronisiert werden sollen, werden sehr differenzierte Filterfunktionen angeboten.

Grundsätzlich funktioniert die Synchronisation in beide Richtungen: Dokumente können vom Masterarchiv in das Satellitenarchiv übergeben werden. Umgekehrt können Änderungen an den Dokumenten oder hinzugekommene Dokumente aus dem Satellitenarchiv dem Masterarchiv übergeben werden. Die Dokumente im Satellitenarchiv bekommen zwar eine eigene DocID, die der Logik des Archivs entspricht; sie erhalten zusätzlich die DocID des Masterarchivs. So kann die Synchronisation vom Satelliten zum Master einfach stattfinden.



AS=Authentication Server, Cl=Client, CtS=Content Server, DB=Datenbank, DS=Dateisystem, WS=Workflow Server

Abbildung 10: Dokumente können per Synchronisation von Masterarchiv (m) und Satellitenarchiv (s) in einem Backup gesichert werden.

Diese Architektur erlaubt nicht nur den wechselseitigen Zugriff auf entfernte Archive, sondern ebenfalls den Aufbau von redundanten Archiven, um, unabhängig von Standort und Übertragungskapazität, auf den gleichen Archiven arbeiten zu können. Unabhängig von der Art des Archivs („Master" oder „Satellit") kann in beiden Standorten die volle DocuWare-Funktionalität, inklusive der Übernahme beliebiger Dokumente genutzt werden. Die Synchronisation zwischen „Master" und „Satellit" erfolgt über den Workflow Server.

Hinweis für Archive mit aktiviertem Versionsmanagement: Versionsmanagement muss sowohl für das Master- wie auch für das Satellitenarchiv mit den gleichen Einstellungen aktiviert sein. Neue Dokumentenversionen können nur im Masterarchiv erstellt werden. Im Satellitenarchiv mit Versionsmanagement sind Dokumente schreibgeschützt.

4.6 Sensible Daten außerhalb von DocuWare schützen

Bestimmte Daten lassen sich nicht mit DocuWare-Sicherheitsmaßnahmen schützen.

Dazu gehören die Indexdaten zu den Dokumenten, der extrahierte Volltext und auch die Thumbnails, die alle in den jeweiligen Datenbanken abgelegt werden. Jeder Systemadministrator mit ausreichenden Rechten kann diese Daten einsehen.

Zudem ist der Volltext in einem separaten Index sgespeichert. Dieser wird vom Volltext Server gesteuert, der auf weit verbreiteten Volltextengine Apache SoLR basiert.

Wenn in diesen Daten sensible Informationen enthalten sind, muss der Zugriff zu den Datenbanken, zum Speicherort vom Volltextindex sowie der Zugang zum Volltext Server – die URL ist standardmäßig http://machinename:9012/solrt (http://machinename:9012/solrt) - vom Administrator mit den allgemein üblichen Maßnahmen geschützt werden, wie beispielsweise Access Control Lists für Dateiverzeichnisse oder Datenbanken.

4.7 Elektronische Signaturen

Mit einer elektronischen Signatur können Sie weitgehend sicherstellen, dass ein Dokument auch wirklich vom Sender stammt. Auch lassen sich Änderungen von Dokumenten nachprüfen und verifizieren.

In DocuWare lassen sich PDF- Signaturen an mit WebScan gescannte Dokumente anhängen oder an Dokumente, die mit dem Modul DocuWare Import in DocuWare archiviert werden. Die Signaturen müssen sich im Windows-Zertifikat-Speicher befinden.

Der Besitzer des privaten Schlüssels kann die Signatur verwenden, so dass der Empfänger vom Dokument den Absender mit einem öffentlichen Schlüssel verifizieren kann. Der öffentliche Schlüssel ist meistens auf der Client-Rechner gespeichert.

5 Ausfallsicherheit

Da ein Dokumentenmanagementsystem meist in eine heterogene IT-Infrastruktur eingebettet ist, kann es für einen Ausfall die verschiedensten Gründe geben, die zunächst nichts mit dem DMS zu tun haben.

Um das Risiko von Ausfällen der Server-Plattformen zu minieren, empfehlen sich „geclusterte" Systeme, die zudem die Lasten zwischen den Komponenten verteilen können, ohne dass sich die DocuWare-Software damit befassen muss.

DocuWare Server können mit geclusterten System arbeiten. Der Authentication Server (http://help.docuware.com/de/#t61104) beispielsweise speichert sämtliche Einstellungen in der Datenbank und arbeitet „stateless". Das heißt, es werden keine Daten programmintern zwischengespeichert. Auf diese Weise kann er die Möglichkeiten der obigen Plattformen uneingeschränkt nutzen und auf einem System, das sich aus mehreren Rechnern zusammensetzt, ablaufen.

Der Content Server arbeitet „stateful". Sofern mehrere Content Server (http://help.docuware.com/de/#t61104) parallel auf den einzelnen Systemen eingesetzt werden, ist aber ebenfalls die Nutzung der zusätzlichen Performance und Sicherheit dieser Plattformen möglich.

Ausgefeilte Verfahren liegen auch für Datenbank-Server vor. Aufgrund der essentiellen Bedeutung der Datenbank für das Funktionieren des DocuWare-Systems wird empfohlen, diese Möglichkeiten zu nutzen. Soweit es sich um die Speichertechnologien, wie beispielsweise Einsatz von RAID-Laufwerken handelt, gilt wiederum, dass DocuWare von solchen Technologien profitiert, selbst aber keinen Einfluss auf diese Komponenten nimmt.

Durch gesicherte Kommunikation und Transaktionsverfahren leistet DocuWare eigene Beiträge zur Ausfallsicherheit. Auch die ausgefeilte Identitätsprüfung der Nutzer und der Systeme untereinander (siehe Zugangssicherheit (http://help.docuware.com/de/#t61104)) minimiert Ausfälle aufgrund vorsätzlichen oder grob fahrlässigen Verhaltens.

Nicht die oben erwähnten Möglichkeiten der Plattformen, sondern nur die Beiträge, die DocuWare selbst zur Ausfallsicherheit leistet, werden im Folgenden detaillierter beleuchtet.

5.1 Failover von DocuWare Servern

Um die Verfügbarkeit der DocuWare-Applikation zu gewährleisten, empfiehlt sich die redundante Installation der DocuWare-Server.

Dazu ein Beispiel: Wenn ein Authentication Server nicht mehr antwortet, wendet sich der Client an den nächsten Authentication Server. Dies geschieht nicht automatisch, sondern der Benutzer führt eine Neuanmeldung durch. Am Client kann hierzu eine Reihenfolge für die gewünschten Authentication Server konfiguriert werden. Bei der Neuanmeldung werden die Authentication Server nacheinander auf Verfügbarkeit geprüft. Das gleiche gilt für DocuWare-Server, die sich ebenfalls beim Authentication Server anmelden müssen, um ein Ticket für den Betrieb zu erhalten.

Bei dem Login ordnet der Authentication Server dem Benutzer nach der erfolgreichen Authentifizierung und Lizenzüberprüfung benötigte und verfügbare Server, wie etwa Content Server, zu. Ist der entsprechende Content Server nicht verfügbar, wendet sich der Client wieder an den Authentication Server, der daraufhin zunächst mit dem Content Server kommuniziert und durch diese Anfrage gegebenenfalls einen Ausfall des Content Servers bemerkt. Bei redundanter Auslegung der Server lässt sich somit ein Content Server-Ausfall durch eine Neuanmeldung umgehen und der Benutzer kann weiterhin mit DocuWare arbeiten.

Aufgrund der Transaktionsorientierung des Content Server werden Änderungen in den Datenbanken erst mit dem abschließendem „Submit"-Kommando wirksam. Bleibt dieses Kommando aufgrund eines Ausfalls des Servers aus, so bleibt der vorherige Zustand erhalten. Inkonsistente Zustände können dementsprechend nicht entstehen, siehe dazu auch das Kapitel Sicherheitsmaßnahmen für Archive (auf Seite 21).

Für die meisten Servermodule sind Failover-Maßnahmen verfügbar. Fragen Sie bitte im Zweifelsfalle beim DocuWare-Support nach.

Weitere Informationen zu Verfügbarkeit und Ausfallsicherheit von DocuWare Systemen finden Sie im White Paper System Architektur im Kapitel Skalierbarkeit http://help.docuware.com/de/#t61324.

5.2 System-Datenbank schützen

Alle Rechte und Lizenzen sind in der System-Datenbank gespeichert. Deshalb ist es wichtig, das Risiko für Missbrauch oder Ausfälle gering zu halten.

- Um maximale Sicherheit zu erreichen, arbeitet der Authentication Server über einen eigenen Datenbank-Account. Der Client benötigt keinerlei Zugriff auf die Authentication Server Datenbank, sondern lediglich auf die Adresse des zuständigen Authentication Server (zuzüglich Backup Authentication Server). Diese Information findet sich in einer lokalen XML-Datei.
- Passwörter werden als „salted Hash-Value (auf Seite 11)" gespeichert und sind damit weder lesbar, noch zu erraten.

5.3 Backup

Wie allgemein üblich sollten auch für die Daten und Dokumente im DocuWare-System Sicherungsläufe etabliert sein. Diese Komponenten sollten als Backup gespeichert werden.

5.3.1 DWSYSTEM: Systemkonfiguration

Alle system- und organisations-relevanten Eigenschaften werden in der Datenbank DWSYSTEM gespeichert. Diese Datenbank sollte mindestens einmal in der Woche, mindestens jedoch nach umfangreichen Änderungen gesichert werden.

5.3.2 Dokumente und Archivdatenbank DWDATA

Die Daten der Archive werden in der Datenbank DWDATA gespeichert. Sichern Sie diese Datenbank so oft, dass immer ein normaler Betrieb gewährleistet ist.

Zusätzlich ist die Sicherung der Archivinhalte selbst, also der eigentlichen Dokumente mit den zugehörigen XML-Dateien erforderlich. Dabei können prinzipiell natürlich ebenfalls klassische Verfahren, zum Beispiel Bandsicherung mit Generationenverfahren, zum Einsatz kommen. Es sind jedoch die teilweise enormen Datenbestände in den Archiven zu berücksichtigen, die vor allem regelmäßige Vollsicherungen unpraktikabel erscheinen lassen. Inkrementelle Sicherungen hingegen sind weitestgehend problemlos, da das laufende Datenvolumen im Allgemeinen gut handhabbar ist. Entsprechend ist mit den Volltext-Index-Dateien umzugehen.

Werden (optische) Wechselmedien eingesetzt, kann die Erzeugung manueller Kopien der Produktionsmedien der einfachste Weg sein. Je nach eingesetztem Speicher-Subsystem1 ist auch die automatische, parallele Erstellung von Sicherungsmedien verfügbar. Einige Subsysteme verfügen über redundante Speicherverfahren oder automatische Spiegelung, die klassische Sicherungsverfahren weitestgehend substituieren können.

Die DocuWare-Funktionen lassen sich ebenfalls für Sicherungszwecke einsetzen. Archive inklusive zugehöriger Indexdaten können über die Exportmöglichkeiten kopiert werden und damit auch als Backup fungieren.

Weiterhin bietet der Aufbau von Master-/Satellitenarchiven eine Möglichkeit, die Sicherungsproblematik ohne manuellen Aufwand zu lösen. Durch die Nutzung der Synchronisation kann für eine automatische Aktualisierung der Backup-Kopie gesorgt werden. Erforderlich sind lediglich ausreichende Speicher- und Übertragungskapazitäten der informationstechnischen Infrastruktur.

So kann beispielsweise ein Satellitenarchiv rein zu Sicherungszwecken an einem anderen verbundenen Standort definiert werden, welches – beispielsweise über Nacht – automatisch mit dem Masterarchiv synchronisiert wird.

5.3.3 Workflow Engine Database

Workflow Engine nutzt die eigene Datenbank DWWORKFLOWENGINE, die alle Informationen für Workflow Manager enthält. Dazu zählen die Konfiguration der Workflows und die Workflowhistorie. Diese Datenbank sollte auf jeden Fall gesichert werden, weil kein Inhalt über diese Workflows in den Dokument-Headern gespeichert wird.

5.3.4 Andere DocuWare Server

Der Volltext Server produziert eigene Indexdateien, die ebenfalls gesichert werden können. Jedoch geht die Erstellung von Indexdateien vergleichsweise schnell, weshalb sich diese nach einem Crash ohne großen Aufwand wieder herstellen lassen.

Notification Server nutzt eine eigene Datenbank, die gesichert sollte, um alle Informationen über E-Mail-Benachrichtigungen zu erhalten. Das gleiche gilt für die Datenbank von Thumbnail Server.

5.4 Wiederherstellung (Recovery)

Der Zugriff auf die abgelegten Dokumente erfolgt immer über die Indexdaten der Datenbank. Ohne diese Informationen ist ein Wiederfinden der Daten kaum möglich.

Selbst wenn die Backup-Kopien der Datenbanken nicht verfügbar und beschädigt sein sollten, kann DocuWare die Daten zurückholen. Dies kann jedoch je nach Archivgröße einige Zeit in Anspruch nehmen.

Für die Wiederherstellung der Indexdaten macht sich DocuWare das Prinzip der doppelten Datenhaltung zunutze. Nach diesem Prinzip werden die Indexdaten, die für jedes Dokument in der Datenbank enthalten sind, zusätzlich in der XML-Header-Datei mitgeschrieben. Die benötigten Dokumentablagen müssen also während der Wiederherstellung verfügbar sein.

Für die Wiederherstellung einer defekten Datenbank benötigt DocuWare folgende Informationen:

- die Datenbankfelder, d.h. die Struktur der Datenbank
- die Ablagepfade der Dokument-Dateien
- die Indexinformationen der abgelegten Dokumente

Auch ist das Wiederherstellen von verschlüsselten Archiven unterstützt. Der Schlüssel steckt in einer zusätzlichen Datei auf dem Speicherort neben dem Dokumentenheader. Ein zweiter Schlüssel ist in der System-Datenbank gespeichert. Damit lässt sich der Dokumentschlüssel ver- oder entschlüsseln.

Die besondere Herausforderung liegt in den Fällen, bei denen wegen der Revisionssicherheit Dokumente und XML-Dateien sehr frühzeitig auf nicht-veränderbare Speichermedien (z.B. WORM) gespeichert wurden. In diesem Fall lassen sich die Indexdaten möglicherweise nicht wieder komplett herstellen, da Änderungen, die nach der Speicherung erfolgten, nicht mehr verfügbar sind, da sie im Header nicht aktualisiert werden konnten (Header war schreibgeschützt).

6 Protokollierung

DocuWare verfügt über eine sehr flexible, leistungsfähige und leicht anpassbare Protokollierung aller relevanten Ereignisse. Damit werden sowohl die Ursachenforschung bei Problemen als auch die Systemüberwachung optimal unterstützt und es wird gegebenenfalls die Basis für die Abrechnung von Leistungen geschaffen.

6.1 Protokollarten

Die einzelnen DocuWare-Servermodule sind verantwortlich für die Protokollierung ihrer jeweiligen Aktivitäten. Je nach Vorgaben und Servermodul können durch die entsprechenden Administratoren die Protokollfunktionen gezielt aktiviert und deaktiviert werden.

Protokollierungsfunktionen unterliegen der DocuWare-Rechteverwaltung. Analog zu den Administratorrollen werden die folgenden Protokolle differenziert und sind von den entsprechenden Administratoren zu konfigurieren:

- Systemprotokoll
- Organisationsprotokoll
- Archivprotokoll

Zusätzlich stehen spezielle Protokollierungen für die vordefinierten Workflows zur Verfügung, um diese Automatismen elegant überwachen zu können.

Die Protokollierung ist sehr flexibel an die jeweiligen Bedürfnisse des Unternehmens anpassbar. Bei der Konfiguration hilft ein Assistent. Die Definition eines Protokolls läuft generell nach dem folgenden Schema ab:

1 Definition der interessierenden Ereignisse und Zielformate

2 Definition der zu protokollierenden Objekte

3 Spezifikation der zu protokollierenden Informationen

4 Definition eventueller Filter (z.B. werden nur Ereignisse protokolliert, die von einem bestimmten Benutzer ausgelöst wurden)

Es wird zunächst bestimmt, welche Art der Ereignisse (Protokollierungsebene) wo aufgezeichnet werden soll, danach sind die Protokollinhalte mit den relevanten Objekten und den zu protokollierenden Informationen zu bestimmen.

6.2 Protokollierungsebenen

Für die Protokollierung kann zwischen verschiedenen Zielformaten (Datenbank, XML-Datei, formatierte Datei) und verschiedenen Ereignissen (Information, Warnung, Fehler, Kritischer Fehler) gewählt werden. Eine tiefere Ebene inkludiert die Ereignisse einer höheren Ebene. Entsprechend werden bei der Aktivierung der Ebene „Information" sämtliche Ereignisse protokolliert.

Fehler der Ebenen "Fehler" und „Kritische Fehler" können automatisch dem Windows-Protokoll zugefügt werden. Weiterhin ist in diesen Fällen die automatische Aussendung einer E-Mail möglich.

Die genannten Ereignisse haben folgende Bedeutungen:

Kritische Fehler:
Ein unerwarteter Fehler, für den keine Behandlungsroutine existiert.

Fehler:
Fehler, für die Behandlungsroutinen vorhanden sind, beispielsweise auf ein bestimmtes Dokument kann nicht zugegriffen werden.

Warnung:
Ein Auftrag konnte nicht ausgeführt werden, der weitere Programmfluss ist aber nicht behindert, beispielsweise fehlende Rechte für das Schreiben von Indexdaten.

Information:
Zusätzliche Information über aufgetretene Ereignisse, die vor allem für Administratoren interessant ist.

Jedes Ereignis, dass zu einer Abweichung von dem vorgesehenen Programmablauf führt, kann einen Eintrag in die Protokollierung bedingen. Protokolle, die sämtliche Ereignisse zur Laufzeit erfassen, können daher sehr umfangreich werden und das System belasten. Es empfiehlt sich, im normalen Betrieb lediglich Fehler protokollieren zu lassen (siehe auch vordefinierte Protokollierung (auf Seite 34)) und die weitergehenden Informationen lediglich während der Fehlersuche einzuschalten.

Für Audits kann ein umfangreiches Logging auf Archivebene eingeschaltet werden, um beispielsweise die Änderung von Indexdaten innerhalb der Protokollierung nachweisen zu können.

6.3 Protokollinhalte

Relevante Ereignisse für die Protokollierung sind einerseits Änderungen der Konfiguration durch die Administratoren und andererseits Ereignisse, die sich zur Laufzeit der Anwendung ergeben.

Generell sind bei der Administration die Erstellung, Änderung und Löschung von den definierten Objekten protokollierbare Ereignisse. Die folgende Tabelle listet die Objekte, für die die Protokollierung während der Administration erfolgt.

Systemebene	Organisationsebene	Archivebene
▪ Authentication Server ▪ Content Server ▪ Workflow Server ▪ Verbindungen ▪ Speicherorte ▪ Externes Benutzerverzeichnis	▪ Lizenzen ▪ Private und öffentliche Stempel ▪ Anzeige- und Bearbeitungsprogramme ▪ Externe Auswahllisten ▪ Validierungen ▪ Verschiedene Einstellungen	▪ Allgemein ▪ Datenbank ▪ Dokumente ▪ Platten ▪ Archivprofile ▪ Suchdialoge ▪ Ablagedialoge

Systemebene	Organisationsebene	Archivebene
	▪ Benutzersynchronsation ▪ Benutzerverwaltung ▪ Signaturtypen ▪ Workflows: ▪ Archivsynchronisation ▪ Export ▪ Migration ▪ DocuWare-4-Archiv konvertieren ▪ Index wiederherstellen ▪ Volltextdienst ▪ Autoindex ▪ DocuWare Request ▪ Löschen ▪ SAP-Barcode-Transfer	▪ Ergebnislisten ▪ Link

Tabelle 1: Objekttypen für Protokollierung bei Administration

Der Protokolleintrag umfasst:

- Name der Einstellung
- Objekttyp
- GUID
- Benutzer, der die Änderung vornahm, mit Name und Organisation

Über eine Filterfunktion lassen sich die zu protokollierenden Ereignisse weiter einschränken. Auf Systemebene kann damit eine Filterung von Organisationen und auf Organisationsebene eine Filterung von Archiven sowie Benutzern erfolgen.

	Systemebene	Organisationsebene	Systemebene
Ereignisse	Öffnen und Schließen	Öffnen und Schließen	Öffnen, Ändern und Schließen
Objekte	▪ Authentication Server ▪ Content Server ▪ Datenbankverbindung ▪ Speicherort ▪ Externes Benutzerverzeichnis	▪ Lizenzen ▪ Benutzersynchronisation ▪ Zusätzliche Organisationen ▪ Archivsynchronisation ▪ Export ▪ Migration ▪ DocuWare-4-Archiv konvertieren ▪ Index wiederherstellen	▪ Dokument ▪ Suchdialoge

	Systemebene	Organisationsebene	Systemebene
		▪ Volltextdienst ▪ Autoindex ▪ DocuWare Request ▪ Löschen ▪ SAP-Barcode-Transfer	
Objektfilter	▪ Organisation ▪ Servername	▪ Archiv ▪ Benutzer	▪ Benutzer
Protokollierte Information	▪ Name ▪ Objekttyp ▪ GUID ▪ Benutzer mit Namen und Organisation	▪ Name ▪ Objekttyp ▪ GUID ▪ Benutzer mit Namen und Organisation	▪ Name ▪ DocID ▪ Index-Informationen ▪ Archivname ▪ GUID ▪ Benutzer mit Namen und Organisation

Tabelle 2: Protokollierung zur Laufzeit

Auf jeder Ebene (System, Organisation, Archiv) können gleichzeitig mehrere Protokollierungen parallel erfolgen.

6.4 Speicherort und -umfang

Der System-Administrator kann die zu nutzenden Datensenken vorgeben, Datenbank-Verbindungen einrichten oder Dateiverzeichnisse anlegen. Es ist die Maximalgröße einer Protokolldatei einstellbar. Wenn die maximale Größe erreicht ist, sollte eine neue Protokolldatei erstellt werden. Dies behindert die Performance weniger, als die alten Dateien zu überschreiben.

Die entsprechenden Grenzwerte und die Bestimmung der Größe der zu überschreibenden Bereiche sind frei wählbar. Bei der Wahl von Datenbanken beziehungsweise XML-Dateien als Speicherort erfolgt die Vorgabe in Form von Datensätzen, ansonsten in Form von MegaByte.

Bei der Erstellung neuer Dateien nach Erreichen des Maximums kann wiederum eine maximale Anzahl vorgegeben werden.

6.5 Berechtigungen

Die Möglichkeit, die Protokollierung zu spezifizieren, unterliegt, wie alle anderen Funktionen, dem Berechtigungskonzept. Das Berechtigungskonzept sieht ein eigenes Recht für das Erstellen und Löschen von Protokollierungsspezifikationen ("Logging-Agenten") vor.

Der Administrator, der einen Speicherort für die Protokollierungen definiert, kann festlegen, ob dieser Speicherort auch von anderen Administratoren verwendet werden darf. Ist dies nicht der Fall, kann nur er Protokollspezifizierungen definieren, die diesen Speicherort verwenden.

Einsicht in die jeweilige Protokollierung kann nur ein Benutzer vornehmen, der für diese Ebene über die entsprechenden Administrations-Rechte verfügt. Ein Organisations-Administrator hat also nicht unbedingt Einblick in die Protokollierung eines Archivs, wenn er in dem Archiv nicht auch über Administrationsrechte verfügt.

6.6 Vordefinierte Protokollierung

Auch ohne benutzerdefinierte Protokolle sollten bestimmte Ereignisse im System aufgezeichnet werden. Bei der Installation erfolgt daher eine automatische Spezifikation je eines Protokolls für die System-, Organisations-, Archivebene.

Bei der Installation einer neuen Organisation oder eines neuen Archivs werden diese Spezifikationen standardmäßig mit installiert. Es handelt sich dabei um Datenbanktabellen mit einer Gesamtgröße von maximal 10.000 Einträgen.

Die vordefinierte Protokollierung auf der System- und Organisationsebene protokolliert alle Fehler (kritisch und nicht-kritisch). Bei einem Archiv werden die Laufzeitereignisse auf Warnung-Ebene und die administrativen Ereignisse auf Fehlerebene protokolliert.

Eigenschaft	Standard-Einstellung
Allgemeine Informationen	
Name	DWArchiv<Archivname>
Status	gestartet
Logging-Level	Fehler
Ziel	DWLOG_<Archivname>
Zusätzliche Ausgabegeräte	keine
Administrative Ansicht	
Objekte	Ereignisse
Alle Einstellungen	Erstellen, Verändern, Löschen
Ansicht zur Laufzeit	
Objekte	Ereignisse
Ausnahmen	
Dokument	Erstellen, Löschen
Mögliche Informationen	
Dokumentname	
DocID	

Eigenschaft	Standard-Einstellung
Index-Informationen und –Ver-änderungen	
Archivname, GUID	
Benutzername	
Benutzerorganisation	
Filter	keine

Tabelle 3: Beispiel: Standardprotokollierung für ein Archiv

Eigenschaft	Standard-Einstellung
Allgemeine Informationen	
Name	DWOrganisation<Organisationsname>
Status	gestartet
Logging-Level	Fehler
Ziel	DWLOG_<Organisationsname>
Zusätzliche Ausgabegeräte	keine
Administrative Ansicht	
Objekte	Ereignisse
Alle Einstellungen	Erstellen, Verändern, Löschen
Ansicht zur Laufzeit	
Objekte	
Ausnahmen	
Mögliche Informationen	
Einstellungsname	
Typ	
GUID	
Benutzername	
Benutzerorganisation	

Eigenschaft	Standard-Einstellung
Allgemeine Informationen	
Name	DWOrganisation<Organisationsname>
Filter	keine

Tabelle 4: Beispiel: Standardprotokollierung für eine Organisation

Eigenschaft	Standard-Einstellung
Allgemeine Informationen	
Name	DWSystem
Status	gestartet
Logging-Level	Fehler
Ziel	DWLOG_SYSTEM
Zusätzliche Ausgabegeräte	keine
Administrative Ansicht	
Objekte	Ereignisse
Alle Einstellungen	Erstellen, Verändern, Löschen
Ansicht zur Laufzeit	
Objekte	Ereignisse
Ausnahmen	
Authentication Server Session	Öffnen, Schließen
Content Server Session	Öffnen, Schließen
Datenbankverbindung	Öffnen
Workflow Server	Öffnen, Schließen
Mögliche Informationen	
Einstellungsname	
Typ	
GUID	

Eigenschaft	Standard-Einstellung
Allgemeine Informationen	
Name	DWSystem
Kurzer Benutzername	
Benutzerorganisation	
Filter	keine

Tabelle 5: Beispiel: Standardprotokollierung für das System

Für die Definition der Protokollierungen werden Assistenten bereitgestellt, die den Benutzer durch die einzelnen Schritte führen.

Weiterhin stehen Standardprotokollierungen für jede Art von Workflow zur Verfügung, die im Einzelnen die Überwachung der Laufzeit dieser automatischen Abläufe ermöglichen.

7 Referenzen

Mehr Informationen finden Sie in folgenden Dokumenten:

- White Paper Intelligent Indexing (http://help.docuware.com/de/#t59237)
- White Paper DocuWare Online (http://help.docuware.com/de/#t58812)
- White Paper System Architektur http://help.docuware.com/de/#t61140

8 Glossar

Ablagedialog	Bevor ein Dokument in ein Archiv abgelegt werden kann, muss es so verschlagwortet werden, dass es bei einer Recherche mühelos wiedergefunden wird. Für die Ablage und Verschlagwortung von Dokumenten dient der Ablagedialog. Ablagedialoge können in DocuWare nach Bedarf pro Archiv definiert und Benutzern und Profilen zugewiesen werden.
Administrative Rechte	Administrative Rechte umfassen die Rechte zur Änderung von Archivdefinitionen oder Definitionen innerhalb einer Organisation.
Archiv	Ein „Archiv" ist in DocuWare eine logische Einheit, die Dokumente entgegennimmt, speichert, sucht und wieder bereitstellt. Ein Archiv umfasst immer die Dateiablage, in der die Dokumente physikalisch gespeichert sind sowie die zugehörigen Datenbanktabellen, die Indexdaten und andere beschreibende oder ergänzende Elemente zu dem Dokument enthalten. Optional kann ein Archiv auch einen Volltext-Index enthalten, der die Dokumente zusätzlich über die Volltext-Information zugänglich macht. Für die Dateiablage können unterschiedliche Ablagemedien Verwendung finden. Dazu werden den Archiven „logische Platten" zugeordnet, die nach vorgegebenen Regeln auf physikalische Ablagemedien abgebildet werden. Ein Archiv ist eine Sammlung verschlagworteter Dokumente. Für Archive können feingranulare Zugriffs- und administrative Rechte vergeben werden.
Archiv-Administrator	Nutzer, dem ein Administrationsrecht für ein Archiv gegeben wurde. Er kann dieses Recht nicht weitergeben.
Archiv-Besitzer	Nutzer, der ein Archiv anlegt und administrieren darf. Dieser verwaltet die Archivstruktur und vergibt die Zugriffsrechte auf das Archiv. Das Recht zur Administration kann weitergegeben werden, d.h. der Besitzer kann die Administrationsaufgabe delegieren.
Archivprofil	Ein Archivprofil umfasst die Zugriffsrechte auf ein Archiv. Dazu gehören unter anderem die Zugriffsrechte auf Indexfelder oder Dokumente, die auch von bestimmten Indexeinträgen abhängig sein können (feldabhängige Rechte). Ein Archivprofil kann auch administrative Rechte innerhalb eines Archivs umfassen. Ein Archivprofil wird innerhalb eines Archivs definiert.
Auswahlliste	Auf Ablage- und Suchmasken stellt DocuWare den Benutzern Auswahllisten zur Verfügung, mit denen Eingaben für die Indexfelder ausgewählt und schnell vorgenommen werden können. Auswahllisten werden auf Organisationsebene definiert und können von allen Archiven der Organisationen genutzt werden.

Authentication Server	Die Hauptfunktionen von Authentication Server sind die Lizenzprüfung und die Rechteverwaltung der Benutzer sowie der Programme. Jede DocuWare-Client-Anwendung stellt beim Start automatisch eine Verbindung zu Authentication Server her. Es wird geprüft, ob für die jeweilige Anwendung sowie für den jeweiligen Benutzer eine Lizenz vorhanden und nutzbar ist. Authentication Server hat jederzeit den Überblick, welche Anwendungen und Benutzer im DocuWare-System arbeiten. Zudem handhabt er die Zuteilung von Ressourcen, beispielsweise bestimmt er, mit welchem Content Server (falls mehrere vorhanden) welcher Benutzer arbeiten kann.
Benutzer	Benutzer haben in den Unternehmensorganisationen verschiedene Rollen. Entsprechende Rollen lassen sich in DocuWare abbilden, um die Installation und Administration zu vereinfachen. Dazu werden Funktionen und Zugriffsrechte in Profilen zusammengefasst, die den Rollen zugewiesen werden. In diesem White Paper ist ein Benutzer immer ein DocuWare Benutzer. Benutzer können zu Gruppen zusammengefasst werden. Benutzer erhalten Rechte sowohl über Einzelrechte, Profile oder Rollen.
Content Server	Content Server ist für den Zugriff der DocuWare-Clients auf DocuWare-Archive zuständig. Dem Client ist der direkte Zugriff auf die im Verzeichnis abgelegten Archiv-Dokumente verwehrt. Alle Archivzugriffe erfolgen ausschließlich über Content Server. Informationen über Lizenzen und Benutzerrechte holt sich der Content Server über Authentication Server.
DocuWare-Installation	Siehe DocuWare-System
DocuWare Organisation	Ein DocuWare-System besteht aus mindestens einer Organisation, welche der installierten Lizenzdatei entspricht. Es können mit weiteren Lizenzen auch weitere Organisationen eingerichtet werden. DocuWare ist mandantenfähig.
DocuWare Server	ist ein Überbegriff und umfasst alle Server-Module wie Authentication Server, Content Server, Workflow Server. Der DocuWare-Server besteht somit aus verschiedenen einzelnen Server-Modulen.
DocuWare-System	Das DocuWare-System umfasst eine funktionierende DocuWare-Installation mit allen dafür erforderlichen sowie eventuell optionalen Komponenten. Ein DocuWare-System kennzeichnet sich durch gemeinsame Hardware und Systemeinstellungen für eine oder mehrere „Organisationen". Teilweise wird anstatt vom DocuWare-System auch einfach von DocuWare gesprochen.

Dokument	Ein „Dokument" ist ein Überbegriff für die im Archiv abgelegten Objekte, die aus Benutzersicht eine logische Einheit - eben ein Dokument - bilden. Ein Dokument kann aus einer beliebigen Anzahl von Dateien bestehen. Häufig wird es sich um Informationen im PDF-Format handeln. Dateien aus Output-Management-Systemen, Office- oder Grafik-applikationen oder gar Binärdateien werden aber gleichartig behandelt. Eine Datei kann eine oder mehrere Seite(n) repräsentieren. Eine Datei kann aber auch Stempel, Signaturen, Anmerkungen o.ä. ergänzende Informationen zum Dokument beinhalten. Dokumente können weiterhin aus Dateien mit unterschiedlich formatierten Inhalten bestehen. So können eine Office-Datei, zusammen mit einer E-Mail-Datei und mehreren JPEG-Dateien zusammen ein Dokument darstellen. Technisch erhält daher jedes Dokument in der Dateiablage ein eigenes Verzeichnis für die beteiligten Dateien, Anmerkungen etc.. Eindeutig identifiziert wird das Dokument über die DOCID. Diese Technik bietet die Möglichkeit, auch Teildokumente, z.B. Seiten, mit getrennten Indexinformationen zu versehen. Weiterhin können aus einem Dokument mehrere Dokumente erzeugt werden und mehrere Dokumente können auch zu einem Dokument zusammengefasst werden („Klammerfunktion").
Ererbtes Recht/Explizites Recht	DocuWare unterscheidet in Bezug auf den Benutzer zwischen ererbten Rechten und expliziten Rechten. Ein explizites Recht ist dem Benutzer direkt zugewiesen, ererbte Rechte erhält er über Profile und Rollen.
Export	Beim Export wird eine Kopie eines Archivs oder einzelner Dokumente erzeugt. Sie exportieren ein Archiv beispielsweise, um eine Sicherungskopie zu erstellen oder um ein Archiv offline auf CD/DVD zu nutzen. Der Export eines DocuWare-Archivs umfasst sowohl die Dokumente als auch die Datenbank. Ziel des Exports können Archive innerhalb des DocuWare-Systems oder ein externes Speichermedium sein. Innerhalb des DocuWare-Systems kann in ein neues oder in ein bestehendes Archiv exportiert werden.
Gruppe	Unabhängig von Rollen können Benutzer zu Gruppen zusammengefasst werden, denen dann ebenfalls Rollen zugewiesen werden können. Eine Gruppe ist somit eine Zusammenfassung von Benutzern. Gruppen können ausschließlich über Rollen Rechte zugewiesen werden. Gruppen dienen der einfacheren Administration von mehreren Benutzern.
Header	DocuWare verwendet XML für die Dokumentablage. DocuWare benutzt dieses Format für die Speicherung der Metadaten und Dokumentergänzungen (Anmerkungen, Stempel etc.). Der Content selbst wird aus Performancegründen separat gespeichert (Ausnahme Export). Zusammengefasst werden diese Informationen in der „XML-Header-Datei". Für jedes in DocuWare abgelegte Dokument existiert eine solche Header-Datei, die mit dem Dokument selbst („Content") in der Dateiablage abgelegt wird.
Indexdaten	Siehe Header

Indexfilter	Über Indexfilter schränken Sie in DocuWare den Zugriff auf Dokumente ein. Sie legen für einzelne Indexfelder fest, welche Kriterien sie enthalten müssen, damit Dokumente im Archiv beispielsweise gesucht oder gedruckt werden dürfen. Kriterien für das Filtern von Dokumenten können beispielweise Texteinträge wie Namen, Daten oder numerische Einträge sein.
Logging-Agent	Ein Logging-Agent ist ein Job, der bestimmte Protokollierungsoptionen umfasst und entsprechende Informationen sammelt. Ein Logging-Agent kann Ereignisse unterschiedlicher Organisationen protokollieren oder in unterschiedliche Logging-Ziele schreiben. Ein Logging-Ziel ist immer eine Datei oder ein Datenbankeintrag.
Logging-Ziel	Eine Datei oder eine Datenbankverbindung, in die die Logging-Einträge geschrieben werden.
Masterarchiv	Ein Masterarchiv ist das Archiv, von dem aus eine Synchronisation von Archiven in DocuWare ihren Ausgang nimmt. Es ist quasi das Basisarchiv. Mit dem Masterarchiv können beliebig viele Satellitenarchive synchronisiert, das heißt, auf denselben Stand gebracht werden.
Metadaten	Siehe Header
Migration	Migration ist der Transfer von Dokumenten innerhalb eines Archivs auf eine andere Platte (http://help.docuware.com/de/#t61104) mit einer anderen Plattennummer. In der Regel wird ein Migrations-Workflow gestartet, um die Plattengrößen innerhalb eines Archivs zu reduzieren oder um Platten zusammenzulegen. So kann man ein Archiv auf Platten in der Größe einer CD/DVD speichern, um den Transfer auf ein externes Speichermedium vorzubereiten.
Notification Server	Versendet E-Mails innerhalb eines docuWare-Systems über ein externes Mail System, sobald ein bestimmtes Ereignis eintritt. Es lässt sich beispielsweise festlegen, dass benutzer immer eine E-Mail erhalten, wenn dokumen tmit einem bestimmten Indexswert erstellt oder geändert worden ist. Noticifiation Server startet ebenso Dokumentn-Workflow, indem eine Benachrichtigung zur Workflow Engine geschickt wird
Organisation	Eine Organisation umfasst im Wesentlichen das Management der Benutzer. Innerhalb der Organisation werden keine Hardware-Administrationen durchgeführt. Die gesamte Systemverwaltung erfolgt auf Systemebene.
Organisations-Administrator	Der Organisations-Administrator verwaltet wie schon sein Name sagt eine Organisation. Ein DocuWare System kann eine oder auch mehrere Organisationen umfassen. Der Organisations-Administrator verwaltet insbesondere die Rechte und Benutzer einer Organisation. Er hat keine Zugriffsrechte auf Archive und ihre Verwaltung.

Profile	Profile sind die Zusammenfassung von Einzelrechten. Profile werden in Archivprofile und Funktionsprofile unterschieden. Profile können entweder administrative Rechte oder Zugriffsrechte z.B. auf ein Archiv enthalten.
Rechte	Rechte erlauben die Ausführung von bestimmten Funktionalitäten innerhalb des DocuWare Systems. Einzelrechte können in Archiven und auf Organisationsebene vergeben werden.
Rolle	Benutzer haben in den Unternehmensorganisationen verschiedene Rollen, die sich aus Ihrer Stellung in der Hierarchie (z.B. Genehmigung von Urlaubsanträgen) und aus Ihrer Aufgabenbeschreibung (z.B. Einkäufer) ergeben. Entsprechende Rollen lassen sich in DocuWare abbilden, um die Installation und Administration zu vereinfachen. Dazu werden Funktionen und Zugriffsrechte in Profilen zusammengefasst, die den Rollen zugewiesen werden. Das Rollenkonzept wird auch vom DocuWare-System selbst benutzt, in dem bestimmte Rollen mit entsprechenden Profilen für administrative Aufgaben bereits vordefiniert sind. Eine Rolle ist eine Zusammenfassung von Profilen. Rollen können keine Einzelrechte beinhalten. Vordefinierte Rollen erlauben die einfache Vergabe von administrativen Rechten.
Satellitenarchiv	Das Satellitenarchiv ist quasi das Zielarchiv bei der Synchronisation von Archiven in DocuWare. Ausgangspunkt der Synchronisation ist immer das Masterarchiv. Das Satellitenarchiv enthält nach der Synchronisation die gleichen Dokumente und Datenbankeinträge wie das Masterarchiv.
Suchdialog	die Recherche nach abgelegten Dokumenten in einem Archiv wird mit Hilfe von Suchdialogen durchgeführt. Auf einem Suchdialog befinden sich Eingabefelder, die jeweils mit dem Namen der Indexfelder betitelt sind. Hier werden die Suchbegriffe eingegeben, beispielsweise soll nach Firma *Peter's Engineering* in dem Indexfeld mit dem Namen *Firma* gesucht werden. Suchdialoge können in DocuWare pro Archiv definiert und Benutzern und Archivprofilen zugewiesen werden.
Synchronisation	DocuWare erlaubt die Synchronisation zweier Archive. Die Synchronisation umfasst Dokumente und Datenbank. Ausgangspunkt einer Synchronisation ist immer ein Quellarchiv, das Masterarchiv. Ziel ist immer ein so genanntes Satellitenarchiv. Das kann beispielsweise ein DocuWare-Archiv auf einem Laptop sein, der ohne Netzzugang mit den aktuellen Dokumenten aus einem Masterarchiv arbeiten können muss. Die Synchronisation kann in beide Richtungen, vom Masterarchiv zum Satellitenarchiv als auch umgekehrt stattfinden.
System	Siehe DocuWare-System

System-Administrator	Der System-Administrator verwaltet das System insbesondere aus Hardwaresicht und was Services wie Mailserver angeht. Dazu gehören u.a. die Verwaltung der Datenbankverbindungen, die Verwaltung der Kommunikationswege und die Ablagepfade der Dokumente. Der System-Administrator hat keine Zugriffsrechte auf Organisationsinformationen insbesondere kann er nicht in die Benutzerverwaltung eingreifen.
Thumbnail Server	Thumbnail Server speichert Miniaturansichten und stellt diese bei Anfragen für die Anzeige im Web Client zusammen. Die Miniaturansichten werden so zentral gespeichert und nicht für jeden Benutzer einzeln erstellt. Die Anzeige geht dadurch schneller.
Ticket	Sobald sich ein Benutzer in DocuWare einloggt und mit dem Passwort seine Identität bestätigt hat, erhält er von Authentication Server einen Ausweis, ein so genanntes Ticket, mit dem er seine Authentizität beweisen kann. Mit diesem Ausweis erhält er Zugang zu DocuWare Servern und ihren Diensten. Aus Sicherheitsgründen hat ein Ticket immer nur eine begrenzte Lebensdauer.
Volltext Server	Der Volltext Server ist für die Erstellung und Aktualisierung der Volltextkataloge verantwortlich. Der Volltext Server ist erforderlich, wenn in DocuWare die Volltextsuche genutzt werden soll.
Vordefinierte Rollen	Vordefinierte Rollen werden vom DocuWare System mitgeliefert und garantieren die Arbeitsfähigkeit des Systems bei einer ersten Installation. Vordefinierte Rollen sind der System-Administrator, der Organisations-Administrator und der Archiv-Besitzer.
Workflow	Generell ist ein Workflow eine vordefinierte Folge von Arbeitsschritten, die bei dem Eintreffen eines vordefinierten Ereignisses automatisch innerhalb von DocuWare ausgeführt wird. Man unterscheidet in DocuWare zwei Arten von Workflows: In der DocuWare Administration können Sie auf Organisationsebene mehrere Schritte kombinieren, um eine Funktionalität wie etwa die Synchronisation zweier Archive bereitzustellen. Ein solcher Workflow wird auf Systemebene über den Workflow Server angestoßen und ausgeführt. Mit dem Modul Workflow Manager erstellen Sie Regeln für einen dokumentenbasierten Workflow und legen fest, welcher Benutzer, welche Rolle oder Vertretungsregel für eine Aufgabe genutzt wird. Diese Art von Workflow wird von den Benutzern ausgeführt. Dokumentenbasierte Workflows werden vom Workflow Engine Server verwaltet.
Workflow Engine Server	Ist die Serverkomponente vom DocuWare Workflow Manager. Nicht zu verwechseln mit dem Workflow Server.
Workflow Server	Der Workflow Server ist das Modul, das die Workflows wie Synchronisation oder Export zur Laufzeit ausführt. Nicht zu verwechseln mit dem Workflow Engine Server.

Zertifikat	Um in der elektronischen Welt einen Unterzeichner identifizieren zu können, braucht man einen privaten Schlüssel, mit dem der Unterzeichner die Signatur erzeugt, und einen öffentlichen Schlüssel, mit dem sich nachweisen lässt, wer die Signatur, die Unterschrift angebracht hat. Der private Schlüssel muss sicher gespeichert sein und darf nur dem Unterzeichner zugänglich sein. Er wird beispielsweise auf einer Smartcard festgehalten. Der öffentliche Schlüssel muss – wie der Name schon sagt – öffentlich zugänglich sein. Er wird in einem Zertifikat gespeichert. Qualifizierte Zertifikate identifizieren den Inhaber eines Schlüsselpaares eindeutig. Sie enthalten den Namen des Inhabers, seinen öffentlichen Schlüssel, eventuell weitere Information zum Zertifikatsinhaber und Informationen zum Zertifikatsherausgeber. Zertifikate und ihre möglichen Inhalte sind standardisiert, so dass auch Dritte, die über ein anderes Signatursystem verfügen, Zertifikate prüfen können. Es entspricht einem Ausweis, der durch vertrauenswürdige Dritte ausgestellt wird.
Zugriffsrechte	Zugriffsrechte umfassen Zugriffe auf Archive oder Funktionen innerhalb von DocuWare.