

d.veLop

d.3 admin: Administrieren

Inhaltsverzeichnis

1. d.3 admin	4
1.1. Einleitung	4
1.1.1. Über d.3 admin	4
1.1.2. Tipps zur Benutzeroberfläche	4
1.1.3. Voraussetzungen	4
1.1.4. Weitere Informationen	4
1.2. Installieren von d.3 admin	5
1.2.1. Setup	5
1.3. Starten von d.3 admin	6
1.3.1. Starten und Anmelden	6
1.3.2. Abmelden	7
1.3.3. Update- bzw. Neuinstallation - Verhalten in d.3 admin	7
1.3.4. Das Anwendungsfenster	7
1.3.5. Menü	10
1.3.6. Navigation	10
1.3.7. Ansichtsmodus/Bearbeitungsmodus	11
1.3.8. Projekte	11
1.3.9. Meilensteine	13
1.3.10. Geschützter Modus	15
1.4. Administration	15
1.4.1. Plugins in d.3 admin	15
1.4.2. Dokumente und Akten	15
1.4.3. Berechtigungen	44
1.4.4. Systemeinstellungen	104
1.4.5. Systemüberwachung	150
1.4.6. Weitere Dienste	153
1.4.7. Webhooks	153
1.4.8. Wertemengen-Webhooks	157
1.5. Allgemeine Erläuterungen	158
1.5.1. Struktur des elektronischen d.3-Repository	158
1.5.2. Fallbeispiel	159
1.5.3. Erweiterte Eigenschaften Felder	159
1.5.4. Plausibilitätskontrolle	159
1.5.5. Zuordnung von Wertevorräten	160
1.5.6. Verwendung von Hook-Funktionen	160
1.5.7. Berechtigungskonzept	161
1.5.8. Hinweise zum Transportsystem	164
1.6. Aufbewahrungsfristen und Löschen von Dokumenten	173
1.6.1. Überblick über die Löschung von Daten	173
1.6.2. Statische Ermittlung der Lebensdauer	174
1.6.3. Dynamische Ermittlung der Lebensdauer	174
1.6.4. Setzen des Ereignisses	174
1.6.5. Löschen von Dokumenten	175
1.7. Problembehandlung	178
1.7.1. Erweiterte Eigenschaftsfelder	178
1.7.2. Benutzer verwalten	179
1.7.3. Postkorb	180
1.7.4. Dokumentarten bearbeiten	181
1.7.5. Beispiel für Berechtigungsmengen	183
1.7.6. d.3-Repository-Konfiguration	184
1.7.7. Serverprozesse	185
1.8. Infrastrukturkomponenten	185
1.8.1. d.ecs task	185

1.9. Weitere Informationsquellen und Impressum 186

1. d.3 admin

1.1. Einleitung

1.1.1. Über d.3 admin

Die Anwendung d.3 admin dient Administratoren zur Verwaltung aller im Netz zugänglichen d.3-Repositorys in den folgenden Punkten:

- Benutzern
- Gruppen
- Erweiterte Eigenschaften
- Wertemengen
- Dokument- und Aktenarten
- Dokumentverzeichnissen
- Berechtigungsprofilen
- Dokumentklassen

Darüber hinaus können verschiedene Parameter für d.3 server gesetzt werden, um eine kundenspezifische Konfiguration vorzunehmen.

1.1.2. Tipps zur Benutzeroberfläche

Hinweis-Balloons/Quick-Info: Wenn Sie den Mauszeiger einen Moment über einem Schalter oder einem Symbol stehen lassen, wird ein kurzer Hinweis angezeigt.

Kontextmenüs: Viele Elemente der Oberfläche enthalten ein Kontextmenü.

1.1.3. Voraussetzungen

Dieses Handbuch erläutert die Verwaltung von d.3-Repositorys und richtet sich daher ausschließlich an d.3-Administratoren.

Für das Verständnis dieses Handbuchs ist es hilfreich, das Handbuch zu d.3 smart explorer gelesen zu haben und über grundlegende Kenntnisse von Microsoft Windows zu verfügen.

1.1.4. Weitere Informationen

Weitere Informationen zu d.3 admin finden Sie in den folgenden Handbüchern:

Administrationshandbuch zur Aktenbildung (d.3 admin folder scheme)

Dieses Handbuch behandelt das Aktenbildungsmodul in d.3 admin.

Administrationshandbuch zu d.3 async job inspector

d.3 async job inspector ermöglicht Ihnen die Überwachung und Steuerung der d.3 async-Aufträge, die auf dem d.3-Server im Hintergrund ausgeführt werden.

Zur Analyse von Problemen (z.B. bei der Aktenverknüpfung) ist diese Erweiterung in d.3 admin eine wertvolle Hilfe.

d.3 async job inspector erweitert die Funktionalität der in d.3 smart explorer vorhandenen Job-Liste (in d.3 smart explorer unter **Ansicht | Job Liste** zu erreichen) um ausführliche Kommentare zu einem d.3 async-Auftrag zu erhalten. Neu ist zudem die Anzeige und Änderung der Job-Parameter.

Mit d.3 async job inspector können Sie Aufträge wiederholen lassen, löschen oder die Ausführungspriorität ändern.

Die Integration in d.3 smart explorer zur Anzeige des Job-Dokumentes und die Kopplung an einen möglichen d.ecs rendition service-Server (ehemals d.tiff) erleichtern die Problemanalyse.

Administrationshandbuch zu d.3 client config (Clientprofile)

Bei dem Modul d.3 client config handelt es sich um ein PlugIn für d.3 admin, das bei der Installation der d.3-Anwendung (ab Version 5.5) automatisch eingerichtet wird.

Mit Hilfe des Client Profile Setup lässt sich die d.3-Anwendung (speziell d.3 smart explorer und d.3 import) individuell konfigurieren und anpassen.

Für jede d.3-Installation und jedes Repository lassen sich verschiedene Profile definieren, die verschiedenen Gruppen zugeteilt und dann entsprechend auf den Client-Arbeitsplätzen ausgewählt werden können. Damit sind Sie in der Lage, Voreinstellungen und Einschränkungen in den genannten Anwendungen für die zugeordneten Gruppen über den Profilmechanismus vorzunehmen.

Sie gestalten hiermit die Oberfläche von d.3 smart explorer und d.3 import und passen diese den Anforderungen der Benutzer an.

Administrationshandbuch zu d.3 admin ldap

Dieses Handbuch stellt das LDAP-Modul vor, das zur Definition von d.3-Benutzern dient.

Administrationshandbuch zu d.ecs rendition service

Dieses Handbuch stellt d.ecs rendition service vor, der zur serverseitigen Vertiffung dient.

Administrationshandbuch zu d.3 search

Dieses Handbuch stellt das Modul d.3 search vor, das zur Volltextsuche im d.3-Repository dient.

Administrationshandbuch zu d.3 abo service

Dieses Dokument enthält Informationen zur Installation, Konfiguration und Wirkungsweise von d.3 abo service.

Administrationshandbuch zu d.3 explorer folder browser

Dieses Dokument enthält Informationen zur Konfiguration von d.3 explorer folder browser.

1.2. Installieren von d.3 admin

1.2.1. Setup

Die Installation erfolgt im Verzeichnis **d3\admin**. Aus diesem Verzeichnis können Sie d.3 admin direkt aufrufen. Bei Freigabe dieses Verzeichnisses können Sie auf die darin befindliche Datei **d3admin.exe** zugreifen.

Systemvoraussetzungen

Beachten Sie die zentralen [Systemvoraussetzungen für d.velop-Produkte \(On-Premises\)](#). Abweichende oder weiterführende Systemvoraussetzungen finden Sie in dieser Dokumentation.

Warnung

Support wird nur für solche Systeme gewährt, die die Mindestanforderungen erfüllen.

Anmerkung

d.3 admin kann auch in 64-Bit Systemen genutzt werden.

Anmerkung

Der Einsatz der d.3 Version 8 ist nur zulässig in der Kombination Server 8.x mit Client 8.x, wobei „x“ für die Minor Releases steht und auch diese immer identisch sein müssen (Beispiel: Server 8.1 nur mit Client 8.1). Ein Support für abweichende Systemumgebungen wird nicht geleistet. Nur im Rahmen des Updateprozesses ist ein kurzfristiger, eingeschränkter Betrieb (Recherche, Anzeige (öffnen) und Ablage) mit einem Client 7.2.2 erlaubt.

1.3. Starten von d.3 admin


1.3.1. Starten und Anmelden

Anmerkung

Das Anmelden an d.3 admin ist unabhängig von der Anmeldung an der d.3-Anwendung. Sie müssen sich demnach auch dann an d.3 admin anmelden, wenn Sie sich bereits an d.3 smart explorer (siehe Handbuch zu d.3 smart explorer) erfolgreich angemeldet haben.


Die Konfigurationsdatei **d3login.ini** für die Administration muss sich im Installationsverzeichnis des Programms **d3admin.exe** (**\d3\d.3 admin**) befinden. Sollte sich die Datei da nicht befinden, so können Sie diese manuell dort hin kopieren:

- Im Fall einer Updateinstallation finden Sie die Datei innerhalb des Verzeichnisses **\d3\d3client.prg\Admin_BAK**
- Im Fall einer Neuinstallation finden Sie die Datei innerhalb des Verzeichnisses **\d3\d3client.prg** (Nachdem ein d.3-Repository erstellt wurde)

1. Starten Sie den Anmeldedialog mit der definierten Programmverknüpfung für d.3 admin (**Programme > d.velop > d.3 admin**).
2. Melden Sie sich als Administrator am d.3- Repository an.
3. Geben Sie als Identifikation folgende Informationen ein:
 - den vordefinierten Benutzernamen **d3_admin**
 - das entsprechende Kennwort
4. Wählen Sie im Pulldown-Feld **Repository** das d.3-Repository aus, an dem Sie sich anmelden möchten.
5. Über das Fragezeichensymbol  erfahren Sie die Zugangsdaten zum ausgewählten d.3-Repository.

Warnung

Beim erstmaligen Anmelden ist das Kennwort ebenfalls "d3_admin". Es muss mit der ersten Anmeldung geändert werden.

Über den Button  neben dem Kennwortfeld gelangen Sie direkt in den Änderungsdialog für das Kennwort.

Als Anmeldesprache stehen Ihnen **Deutsch** und **Englisch** zur Auswahl.

Klicken Sie auf **Abbrechen** , um den Anmeldevorgang abzubrechen.

Anmerkung

Sie können ab der d.3 Version 7.2 auch den Verbindungsaufbau zu d.3 server abbrechen, wenn Sie z. B. erkennen, dass die Serverprozesse nicht gestartet wurden.

Zur Bestätigung der Eingaben und als Abschluss des Login-Vorgangs drücken Sie die **ENTER** -Taste oder klicken Sie auf das Feld **Anmelden** .

Alternative Anmeldung mit OpenID Connect

Über die Pulldown-Schaltfläche **Anmelden** können Sie zwischen der Standardanmeldung und der alternativen Anmeldung mit OpenID Connect wählen. Für die Anmeldung mit OpenID Connect ist ein konfigurierter und aktivierter Identity Provider erforderlich. Bei aktivierter Anmeldung via OpenID Connect wählen Sie lediglich das Repository und die Sprache aus. Die Eingabefelder für Benutzername und Kennwort sind deaktiviert. Klicken Sie nun auf **Anmelden**. Anschließend wird der Dialog für die Anmeldung mit OpenID Connect angezeigt.

Die Variante der Anmeldung wird für alle folgenden Anmeldungen gespeichert, sodass Sie diese nicht bei jeder Anmeldung neu auswählen müssen.

Waren Ihre Angaben korrekt, wird nun d.3 admin gestartet und das Anwendungsfenster erscheint.

1.3.2. Abmelden

Durch das Beenden der Anwendung d.3 admin werden Sie auch automatisch abgemeldet.

Zum Beenden der Anwendung schließen Sie das Anwendungsfenster oder drücken Sie die Tastenkombination **STRG+B**.

1.3.3. Update- bzw. Neuinstallation - Verhalten in d.3 admin

Wird d.3 admin nach einem Update bzw. nach einer Neuinstallation der d.3 Version 8 das erste Mal gestartet, wird das d.3-System für die Verwendung des Transportsystems vorbereitet. Folgende Aktionen werden dabei durchgeführt:

Neuinstallation

- Erstellung des Snapshot-Projektes

Update

- Generierung der Synchronisations-IDs für die Stammdaten-Objekte
- Erstellung des Snapshot-Projektes
- Erstellung eines ersten Meilensteines im Snapshot-Projekt mit dem Backup der aktuellen Stammdaten
- Migration der Anwendungsprofile

Nach Abschluss dieser Aktionen befindet sich d.3 admin im [Ansichtsmodus](#) . Um ab jetzt Änderungen vornehmen zu können, müssen Sie ein [Projekt anlegen](#) und in den Bearbeitungsmodus wechseln.

1.3.4. Das Anwendungsfenster

Das Anwendungsfenster von d.3 admin unterteilt sich in die folgenden Bereiche:

The screenshot shows the d.3 admin interface. At the top, there is a navigation bar with menu items: 'Dokumente und Akten', 'Berechtigungen', 'Systemeinstellungen', 'Systemüberwachung', and 'Weitere Dienste'. Below this is a secondary navigation bar with 'Projekt: d.3 Projekt' and 'Meilenstein: Meilenstein 2'. The main content area is divided into three panels: 'Projekte' (showing 'd.3 Projekt'), 'Meilensteine' (showing 'Meilenstein 2' and 'Meilenstein 1'), and 'Offene Sitzungen'. On the right side, there is a 'Protokoll' (log) table with columns: 'Aktion', 'Objekttyp', 'Objektname', 'Benutzer', and 'Zeitpunkt'. The log entries are:

Aktion	Objekttyp	Objektname	Benutzer	Zeitpunkt
INSERT	Restriktionsmenge	Firmenstandorte	d3_admin	08.07.2015 13:22:26
INSERT	Restriktionsmenge	Firmenstandorte	d3_admin	08.07.2015 13:24:28
UPDATE	Restriktionsmenge	Firmenstandorte	d3_admin	08.07.2015 13:25:34
UPDATE	Restriktionsmenge	Firmenstandorte	d3_admin	08.07.2015 13:30:22
INSERT	Dokumentklasse	Bestellung_Standorte	d3_admin	08.07.2015 13:38:54

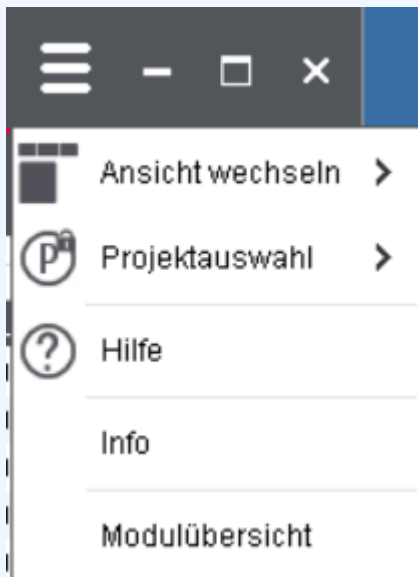
At the bottom right, the 'Systemstatus' section shows system logs and the initialization duration: 'Dauer der Initialisierung 3868ms'.

Oben rechts befindet sich der **Menü**-Button, sowie die Buttons zum Minimieren, Maximieren und Schließen des Fensters.

Über der roten, horizontalen Linie befindet sich die **Navigation** und darunter die Buttons für den **Bearbeitungs- und Ansichtsmodus** sowie die Anzeige für das aktuelle Projekt und den Meilenstein.

Anmerkung

Um zu einer alternativen Ansicht zu wechseln, klicken Sie im Menü auf den Eintrag **Ansicht wechseln**.



Es lassen sich die Bereiche **Navigation**, **Protokoll** und **Systemstatus** wahlweise ein- bzw. ausblenden.

Projekte, **Meilensteine** und **Offene Sitzungen** sind immer sichtbar und können nicht abgeschaltet werden, weil diese für die Nutzung von d.3 admin zwingend erforderlich sind.

Bei der anderen Ansicht wird ein Teil der Navigation in den darunter liegenden Bereich des Fensters gelegt.

Navigation

- Dokumente und Akten
- Berechtigungen
- Systemeinstellungen
- Systemüberwachung
- Weitere Dienste

Projekte

Name	Beschreibung
d.3 Projekt	

Meilensteine

Nummer	Beschreibung
Meilenstein 2	
Meilenstein 1	Erste Einstellungen

Offene Sitzungen

Benutzer	Projekt	Anmeldezeitpunkt
----------	---------	------------------

Protokoll

Aktion	Objekttyp	Objektname	Benutzer	Zeitpunkt
INSERT	Restriktionsme...	Firmenstandorte	d3_admin	08.07.2015 13:2...
INSERT	Restriktionsme...	Firmenstandorte	d3_admin	08.07.2015 13:2...
UPDATE	Restriktionsme...	Firmenstandorte	d3_admin	08.07.2015 13:2...
UPDATE	Restriktionsme...	Firmenstandorte	d3_admin	08.07.2015 13:3...
INSERT	Dokumentklasse	Bestellung_Sta...	d3_admin	08.07.2015 13:3...

Systemstatus

Die DLL C:\d3\d3client.prg\Admin\AdminPlugins\dtiffadm.dll wird geladen ... [OK]
 Die DLL C:\d3\d3client.prg\Admin\AdminPlugins\FolderBrowserAdmin.dll wird geladen ... [OK]
 Die DLL C:\d3\d3client.prg\Admin\AdminPlugins\FolderMapping.dll wird geladen ... [OK]
 Der Navigator wird erstellt. [0 ms]

Dauer der Initialisierung 3868ms.

Verbunden mit Archiv (P)

d.3 Admin [d3_admin]

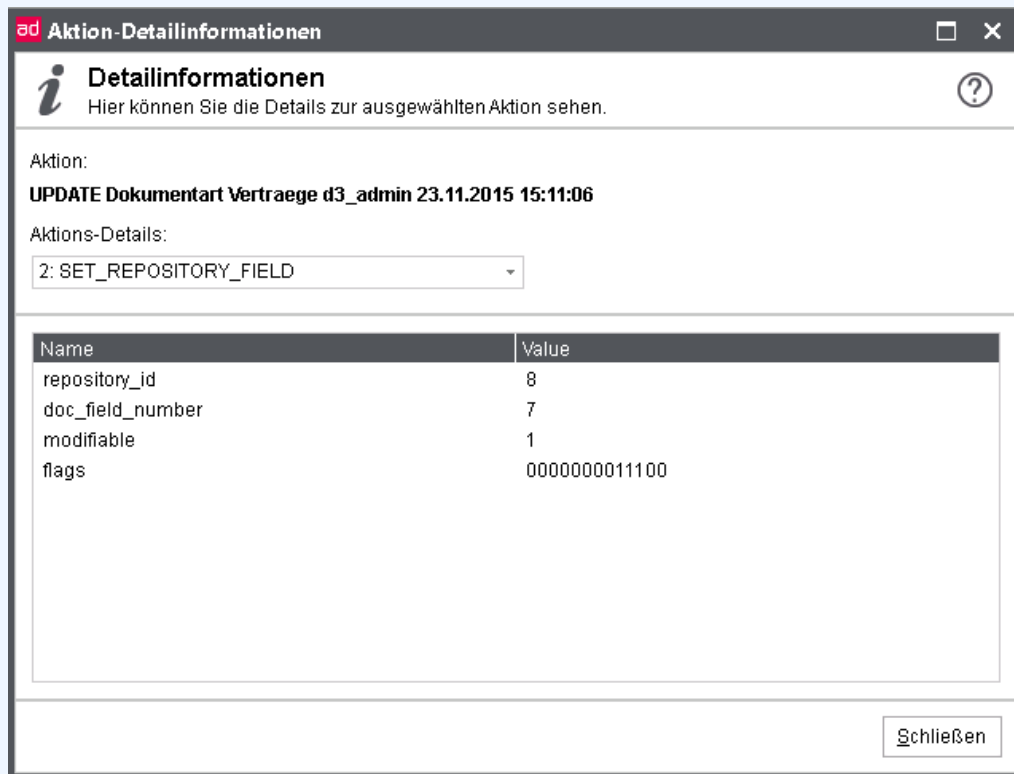
Das Anwendungsfenster hält zudem noch die folgenden Bereiche bereit:

- [Projekte](#)
- [Meilensteine](#)
- Offene Sitzungen (zeigt die aktuell angemeldeten Benutzer samt Bearbeitung in welchem Projekt an)
- Systemstatus (zeigt aktuelle Systemmeldungen an)
- Protokoll (zeigt letzte Änderungen an)

Anmerkung

Die angezeigten Änderungen des aktuell ausgewählten Meilensteins können über die Schaltfläche **CSV-Export** unterhalb der Tabelle als CSV-Datei exportiert werden.

Detailinformationen zum jeweiligen Eintrag können per Doppelklick eingesehen werden:



1.3.5. Menü

Über den Menü-Button finden Sie die Einträge **Ansicht wechseln**, **Projektauswahl**, **Hilfe**, **Info**, **d.velop community store**, **Modulübersicht**.



Anmerkung

Im d.velop community store können Sie sich über aktuelle Produkte und Lösungen informieren und diese beziehen.

1.3.6. Navigation

Die Navigation besteht aus den Hauptmenüpunkten **Dokumente und Akten**, **Berechtigungen**, **Systemeinstellungen**, **Systemüberwachung** und **Weitere Dienste**. Über den Eintrag **Ansicht wechseln** im

Menü können Sie entscheiden, ob Sie für die Navigation ein Dropdown-Menü oder die klassische Baumstruktur verwenden möchten.

Navigation - Ansicht als Dropdown-Menü:



Navigation - Ansicht gewechselt:



1.3.7. Ansichtsmodus/Bearbeitungsmodus

Das Anwendungsfenster von d.3 admin wird standardmäßig im Ansichtsmodus geöffnet. So können z.B. die Einstellungen und der Systemstatus eingesehen werden.

Möchten Sie Änderungen vornehmen, klicken Sie im Anwendungsfenster auf den Button **Bearbeitungsmodus**.



Da Sie beim erstmaligen Start der Anwendung nach der Installation noch kein Projekt angelegt haben, ist die Erstellung eines Projektes auch im Ansichtsmodus möglich.

Um ein neues Projekt anzulegen, klicken Sie im Bereich **Projekte** des Anwendungsfensters auf den Button **Neu**.

Anschließend können Sie, sofern Sie die entsprechenden administrativen Rechte besitzen, die Änderungen durchführen.

1.3.8. Projekte

Bei der Arbeit mit d.3 admin ist darauf zu achten, dass Änderungen immer nur im Bearbeitungsmodus durchgeführt werden. Um in den Bearbeitungsmodus zu gelangen, benötigen Sie mind. ein Projekt, welches sich im Status "geöffnet" befindet. Pro Projekt kann immer nur ein Administrator den Bearbeitungsmodus aktivieren. Mehrere Administratoren können zeitgleich in unterschiedlichen Projekten arbeiten, aber niemals im gleichen Projekt. Unter "Offene Sitzungen" auf der Startseite von d.3 admin können Sie sehen, an welchen Projekten gerade gearbeitet wird.

Beim Wechsel vom Ansichtsmodus in den Bearbeitungsmodus werden Sie gefragt unter welchem Projekt Sie Ihre Bearbeitung vornehmen möchten.

Sie können Projekte verwenden, um bestimmte Konfigurationen in d.3 admin festzuhalten. Sie können dann diese Projekte [exportieren](#) und bspw. auf andere Systeme [importieren](#).

[Erstellen](#) Sie ein Projekt, tragen Sie einen Namen (der Name muss eindeutig sein) ein. Optional kann auch eine Beschreibung angegeben werden. Das Projekt wird im Status "geöffnet" erstellt und kann vom Administrator nicht geschlossen werden.

Es existieren auch geschlossene Projekte, die im Standard nicht angezeigt werden. Dabei handelt es sich entweder um das vom System automatisch erstellte Snapshot-Projekt oder aber es handelt sich um Projekte, die mittels Einspielen von Transportdateien erzeugt wurden. Diese Projekte können nicht wieder geöffnet werden.

Siehe auch: [Hinweise zum Transportsystem](#) , [Datensicherung](#)

Neues Projekt anlegen

Beim Wechsel vom Ansichtsmodus in den Bearbeitungsmodus werden Sie gefragt unter welchem Projekt Sie Ihre Bearbeitung vornehmen möchten.

Sie können Projekte verwenden, um bestimmte Konfigurationen in d.3 admin festzuhalten. Sie können dann diese Projekte exportieren und bspw. auf andere Systeme importieren.

Beim erstmaligen Start oder für ein neues Projekt, klicken Sie im Bereich **Projekte** des Anwendungsfensters auf **Neu**, um ein neues Projekt für Ihre Administration anzulegen.

Projekt importieren

Für das Importieren eines Projekts benötigen Sie eine .d3trans- oder .d3backup-Datei. Sie können sich vor dem Start des Importvorgangs noch Informationen zu den in der Transportdatei enthaltenen Meilensteinen anzeigen lassen. Bei Backupdateien haben Sie diese Möglichkeit nicht, da diese Dateien unabhängig von Projekten und Meilensteinen erstellt werden.

Der Import einer Projekt- bzw. Meilensteindatei durchläuft folgende Schritte:

- Durchführung einer Konsistenzprüfung der in der Transportdatei enthaltenen Einzeldateien. Schlägt diese fehl, ist ein Import nicht möglich. Änderungen an den Dateien sind somit nicht gestattet.
- Durchführung einer Simulation des Importvorgangs zu einer Transportdatei.
- Um die Synchronität der Daten zu gewährleisten, wird geprüft, ob der Meilensteinverlauf zum Projekt auch im Zielsystem lückenlos existiert. Sind nicht alle Meilensteine eines Projektes in der Transportdatei enthalten, stellen Sie sicher, dass Sie durch einen früheren Import die fehlenden Meilensteine schon importiert haben.
- Beim Schreiben der Stammdatenobjekte wird geprüft, ob durch den Import von Transportdateien anderer Projekte schon ein neuerer Stand vorliegt. In so einem Fall wird das Objekt nicht neu geschrieben.
- Der komplette Importvorgang läuft innerhalb einer Datenbanktransaktion ab, so dass jeglicher Fehler (Validierungsfehler oder Datenbankfehler) zu einem kompletten Rollback der Änderungen führt.
- Existierte das Projekt bzw. die Meilensteine vor dem Import noch nicht, werden diese angelegt. Der Status des Projektes bzw. der Meilensteine ist "geschlossen".

So geht's

1. Klicken Sie auf **Importieren**.
2. Wählen Sie eine bereits vorhandene d.3-Projektdatei aus, die Sie in Ihr Repository importieren möchten.
3. Mit **Details anzeigen** können Sie sich einen Überblick über den Inhalt der d.3-Projektdatei verschaffen. Ein Klick auf einen Eintrag im Protokollbereich öffnet eine Übersicht über die Aktionen und Abhängigkeiten, die im Meilenstein enthalten sind. Mit **Zurück** gelangen Sie wieder in den Dialog zum Start des Importvorgangs.
4. Starten Sie die Simulation des Importvorgangs mit **OK**. Nach der erfolgreich abgeschlossenen Simulation sehen Sie unter **Transportdaten** eine Übersicht aller sich ändernden Elemente und Aktionen.
5. Prüfen Sie alle Aktionen in der Übersicht der Transportdaten.
6. Klicken Sie auf **Import starten**, um den tatsächlichen Import durchzuführen.

Warnung

Aktivieren Sie Option **Simulation überspringen** nur dann, wenn Sie sich ganz sicher sind, welche Aktionen mit dem Importieren der ausgewählten Datei durchgeführt werden. Wenn Sie die Option aktivieren, findet vor dem Import keine Simulation statt. Der Import beginnt sofort und Sie haben keine Möglichkeit zur vorherigen Überprüfung.

Projekt exportieren

Sie können ein Projekt sowie einen oder mehrere Meilensteine exportieren.

Anmerkung

Wenn Sie die Daten für ein Projekt exportieren, werden alle geschlossenen Meilensteine in die Transportdatei eingebunden. Wählen Sie ein Ablageverzeichnis für die Datei aus und geben Sie eine Beschreibung für den Export ein. Dieser Text wird beim Import wieder angezeigt. Die Beschreibung im Dialog beinhaltet als Vorschlag das zu exportierende Projekt und die Meilensteine. Sie können den vorgeschlagenen Text ändern.

So geht's

1. Klicken Sie auf **Exportieren** , um ein bereits erstelltes d.3-Projekt zu exportieren.
2. Wählen Sie das Verzeichnis aus, in dem die Datei abgelegt werden soll.
3. Bestätigen Sie die Sicherheitsabfrage dann mit **Ja** , um den Export durchzuführen.

Anschließend erhalten Sie die Information, dass der Export ordnungsgemäß durchgeführt wurde.

1.3.9. Meilensteine

Mit den Meilensteinen können Sie bestimmte Änderungen in d.3 admin festhalten. Sie können Meilensteine exportieren und bspw. auf andere Systeme importieren.

Ein Meilenstein ist immer Bestandteil eines Projektes und kann nicht eigenständig von Ihnen erstellt werden. Ebenso kann ein Meilenstein nicht gelöscht werden.

Bei Erstellung eines Projektes wird automatisch ein Meilenstein erstellt. Jeder Meilenstein trägt eine Nummer, die, pro Projekt, fortlaufend bei 1 beginnt. Meilensteine liegen entweder im Status "geöffnet" oder "geschlossen" vor. Nur, wenn ein Meilenstein den Status "geöffnet" hat (wird rot in der Meilenstein-Übersicht angezeigt), werden darin Änderungen aufgezeichnet. Ein Meilenstein im Status "geschlossen" (wird grün in der Meilenstein-Übersicht angezeigt), kann nicht wieder geöffnet werden. Pro Projekt kann maximal ein Meilenstein im Status "geöffnet" vorliegen. Dabei ist dies immer der zuletzt erstellte. Es gibt auch Projekte, in denen kein Meilenstein den Status "geöffnet" hat. In solchen Projekten können keine Änderungen mehr aufgezeichnet werden. Solche Projekte sind über das Einspielen von Transportdateien aus einem anderen d.3-Repository entstanden.

Folgende Daten werden innerhalb eines Meilensteines aufgezeichnet:

- Wertemengen
- Dokumentarten
- Erweiterte Eigenschaften
- Mehrsprachigkeit
- Aktenbildung
- Gruppen (außer Mitgliedschaften von Benutzern)
- Dokumentklassen
- Berechtigungsprofile
- Berechtigungsprofil-Zuordnungen (nicht für Benutzer)
- d.3 organizational structure
- d.3 policy manager (nicht für Benutzer)
- d.3 restriction set Manager (nicht für Benutzer)
- d.3 config (nicht für alle Parameter)
- d.ecs rendition service Assistent

Warnung

Dateien, die Hook-Funktionen enthalten, sind nicht transportabel!

Sie werden aufgefordert, einen Beschreibungstext zum Meilenstein einzugeben. Schließen Sie einen Meilenstein (nur im Bearbeitungsmodus möglich), werden folgende Aktionen durchgeführt:

- Anhand der Liste der Änderungen an Stammdaten-Objekten werden alle Abhängigkeiten ermittelt und der aktuelle Stand dieser Objekte in eine Transportdatei geschrieben.
 - Abhängigkeiten entstehen z.B. durch Änderungen an Berechtigungsprofilen mit enthaltenen Dokumentklassen, die im Rahmen anderer Projekte erstellt wurden.
 - Der aktuelle Stand eines Objekts spiegelt immer die Sicht auf ein Objekt wider, wenn dieses Objekt zur Bearbeitung geöffnet wird. Es gibt keine projektspezifische Trennung von Objektständen, sondern nur den einen globalen Stand eines Objekts.
- Diese Transportdatei wird in das d.3-Repository importiert (Dokumentart "Audit-Log").
- Der aktuelle Meilenstein wird geschlossen und einer neuer im Status "geöffnet" wird erstellt.

Meilenstein schließen

Sie können einen Meilenstein folgendermaßen sichern bzw. abschließen.

So geht's

1. Klicken Sie auf **Schließen**.
2. Geben Sie im folgenden Dialogfenster eine Beschreibung des Meilensteins ein.
3. Mit **Abhängigkeiten anzeigen** sehen Sie die im Projekt durchgeführten Änderungen und welche zusätzlichen Objekte mit in den Meilenstein aufgenommen werden. Dabei wird auch angezeigt, welche Änderung dazu geführt hat, dass die Abhängigkeit entstanden ist. Mit **Zurück** gelangen Sie wieder in den Dialog zum Schließen des Meilensteins.
4. Bestätigen Sie mit **OK**.

Anmerkung

Geben Sie eine eindeutige Beschreibung für jeden Meilenstein ein, um für einen späteren Import bzw. Export nachvollziehen zu können, welche Einstellungen Sie in diesem Meilenstein getroffen haben.

Meilenstein importieren

Möchten Sie eine bereits vorhandene Meilenstein-Datei in Ihr Repository importieren, können Sie diese über **Importieren** im darauf erscheinenden Dialogfenster auswählen und importieren.

Lesen Sie dazu auch [Projekt importieren](#).

Meilenstein exportieren

Sie möchten einen erstellten Meilenstein exportieren.

So geht's

1. Klicken Sie auf **Exportieren**.
2. Wählen Sie das Verzeichnis aus, in dem die Datei abgelegt werden soll.
3. Bestätigen Sie die Sicherheitsabfrage dann mit **Ja**, um den Export durchzuführen.

Anschließend erhalten Sie die Information, dass der Export ordnungsgemäß durchgeführt wurde.

Anmerkung

Wenn Sie die Daten für Meilensteine exportieren, achten Sie darauf, dass Sie nur geschlossene Meilensteine auswählen können. Sie müssen mindestens einen Meilenstein ausgewählt sein. Es können aber auch mehrere sein, wobei die Liste der Meilensteine lückenlos sein muss. Sie müssen beim Auswählen der Meilensteine aber nicht bei Meilenstein 1 beginnen und auch nicht beim letzten geschlossenen Meilenstein enden. Wählen Sie wieder ein Ablageverzeichnis aus und geben Sie einen Beschreibungstext ein.

Beim Exportvorgang werden die Daten zu den Meilensteinen aus der Dokumentart "Audit-Log" geladen und zu einer ZIP-Datei zusammengefügt. Als Dateierweiterung der Transportdatei wird .d3trans verwendet.

1.3.10. Geschützter Modus

Wenn Sie eine Transportdatei importieren, wird das Repository mit dem Quellsystem der Transportdatei verbunden und das System automatisch in den geschützten Modus versetzt. Im geschützten Modus können Sie Änderungen nur über das Transportsystem durchführen, um die Konsistenz der Objekte zwischen den verbundenen Repositories sicherzustellen.

Vor dem Import einer Transportdatei in einem nicht geschützten System erscheint einmalig ein entsprechender Hinweistext. Wenn Sie den Hinweistext bestätigen, wird die Transportdatei importiert und der geschützte Modus aktiviert. In der Statuszeile von d.3 admin wird der Hinweis **Geschützter Modus** angezeigt.

Weitere Informationen: [Hinweise zum Transportsystem](#)

1.4. Administration

1.4.1. Plugins in d.3 admin

Über verschiedene Plugins von d.3 admin können weitere Komponenten konfiguriert werden.

Die Plugins werden im Plugin-Ordner von d.3 admin abgelegt.

Damit die Plugins geladen werden können, müssen sie eine Reihe von Funktionen zur Verfügung stellen (Export aus der DLL).

Des Weiteren ist die Verwendung der Speicherverwaltung ShareMem zwingend erforderlich, ansonsten kann es später zu undefinierten Fehlermeldungen in d.3 admin kommen (Schutzverletzungen, Abbrüche beim Freigeben der Plugins).

1.4.2. Dokumente und Akten

Wertemengen



Eine Wertemenge ist ein Vorrat von Werten. Diese Wertemenge kann einer erweiterten Eigenschaft zugewiesen werden, welche wiederum einer Dokumentart zugewiesen wird. Somit steht dem Benutzer für dieses Feld der Dokumentart diese Wertemenge als Auswahl zur Verfügung.

Das gilt sowohl für die Suche, als auch (und das ist viel bedeutender) für die Ablage neuer Dokumente. Die Werteliste kann als reine Auswahl oder auch als Vorschlagsliste bereitgestellt werden. Damit können die Werte einer Wertemenge sogar zur Plausibilitätsprüfung herangezogen werden. Die entsprechende Festlegung erfolgt bei der Konfiguration einer Dokumentart.

Beispiel: Angenommen, Sie haben eine Wertemenge mit der Bezeichnung "Firmen" angelegt. Diese Wertemenge umfasst die sechs Einträge

1. "Border Books"
2. "Leonard Krower & Sons"
3. "Simply Save"
4. "Total Sources"
5. "Opticomp"
6. "Sports Unlimited".

Im Anschluss daran haben Sie ein erweitertes Eigenschaftsfeld mit der Bezeichnung "Firma" angelegt. Diesem Feld wurde die Wertemenge "Firmen" zugewiesen.

Zum Schluss legen Sie eine neue Dokumentenart mit der Bezeichnung "Wartung" an. Diese Dokumentenart soll für die Verwaltung der Wartungsverträge einer Software Firma dienen. Dieser Dokumentenart wird nun das Feld "Firmen" zugewiesen. Somit umfasst die Dokumentenart "Wartung" nur ein Eigenschaftsfeld. Wenn nun ein Anwender einen Wartungsvertrag für die Firma "Opticomp" sucht, wählt er zunächst bei den Dokumentarten die Dokumentart "Wartung" aus. Anschließend wählt er die Firma "Opticomp" aus der Auswahlliste (Wertemenge) aus und startet die Suche nach diesen Wartungsverträgen.

Warnung

Der Name einer Wertemenge darf nur die Sonderzeichen "+", "-" und "_" enthalten. Andere Sonderzeichen wie ":" sind nicht erlaubt. Es sind maximal 250 Zeichen für einen Wert in der Wertemenge erlaubt.

In diesem Beispiel wurde die Wertemenge "Firmen" dem erweiterte Eigenschaften-Feld "Firma" zugewiesen. Diese Wertemenge kann jedoch auch weiteren Eigenschaftsfeldern zugewiesen werden. Ein und dieselbe Wertemenge kann also beliebig vielen Eigenschaftsfeldern zugewiesen werden.

Momentan werden vier unterschiedliche Arten von Wertemengen unterstützt. Dies sind die manuell erstellten Wertemengen, die Wertemengen aus einer Datenbank, die Wertemengen aus einer Hook-Funktion und vordefinierte Wertemengen, z.B. die Benutzer/Gruppenliste.

Manuell erstellte Wertemengen

Diese Art von Wertemengen müssen Sie manuell erstellen. Es handelt sich bei dieser Wertemenge immer um eine "statische". Wird diese Wertemenge als Vorschlagsliste genutzt, der Anwender aber einen abweichenden Wert vergibt, erscheint dieser zukünftig NICHT in der Vorschlagsliste. Diese Ergänzung muss also über die Administration vorgenommen werden.

Beispiele für "statische" Wertemengen: Standorte, Abteilungsnamen, Erfassungsquelle von Dokumenten (z.B. Datei, E-Mail, Notiz, Hinweis, Protokoll, ...).

Um eine Wertemenge anzulegen, geben Sie als erstes eine Bezeichnung für diese Wertemenge an. Diese Bezeichnung darf maximal 255 Zeichen lang sein.

Ordnen Sie dieser Wertemenge einen Datentyp zu. An dieser Stelle stehen Ihnen wieder die Datentypen zur Verfügung, welche Sie bei der Definition eines Feldes verwenden.

Zum Abschluss geben Sie die Werte an, welche dieser Wertemenge zugeordnet werden sollen.

Anmerkung

Sie können ab der Version 7.1.1 bestimmen, ob die Werte sortiert werden soll und ob die gewünschte Sortierung aufsteigend oder absteigend erfolgen soll.

Die Werte der Wertemengen lassen sich in die zusätzlich zu unterstützenden Sprachen übersetzen.

Lesen Sie hierzu das Kapitel [Mehrsprachigkeit](#).

Mit der d.3 Version 7 ist es möglich, als Werte nur eine Auflistung von Zahlen vorzunehmen.

Die konkrete Ausprägung als Text wird dann in der Übersetzung der Wertemenge vorgenommen.

Beispiel:



Mit der Übersetzung können nun die konkreten Texte vergeben werden.



Erweiterte Eigenschaften

Unter **Dokumente und Akten** > **Erweiterte Eigenschaften** wird Ihnen eine Übersicht der bereits angelegten erweiterten Eigenschaften und deren Inhalte angezeigt. Hier können Sie auch über den Filter nach bestimmten Eigenschaften suchen, eine **Gesamtübersicht** und eine **Übersicht der DB Felder** einsehen sowie bestehende erweiterte Eigenschaften bearbeiten, kopieren oder entfernen und neue erweiterte Eigenschaften anlegen.



Diese Übersicht der erweiterten Eigenschaften ist eine Art "Vorratskammer". In dieser Kammer werden immer wieder benötigte "Felder" aufbewahrt.

Angenommen, in Ihrem Unternehmen sind zehn Dokumentarten definiert, bei denen eine Eigenschaft mit der Bezeichnung "Maschinen-Nr" vorkommt. Dieser Eigenschaft ist eine Wertemenge zugeordnet und zusätzlich findet eine Eingabekontrolle (Plausibilitätskontrolle) statt. Wenn es diese "Vorratskammer" nicht geben würde, müssten Sie dieses Feld zehnmal definieren.

Durch die Verwendung als erweitertes Eigenschaften-Feld reicht es aus, dieses Feld einmal zu definieren. Anschließend können Sie dieses Feld beliebig oft in einer Dokumentart verwenden. Wenn Sie nachträglich die Wertemenge zu diesem erweitertes Eigenschaften-Feld ändern und dieses Feld in zehn Dokumentarten vorkommt, ist die Wertemenge automatisch in allen zehn Dokumentarten geändert.

Ein erweitertes Eigenschaften-Feld hat eine Vielzahl von Eigenschaften. Diese Eigenschaften werden nachfolgend erklärt.

Feldeigenschaften



Titel

Der Titel einer erweiterten Eigenschaft ist das, was der Anwender sieht, wenn er eine Dokumentart auswählt. Für den Titel können maximal 50 Zeichen angegeben werden. Bitte wählen Sie sinnvolle Namen aus. Wenn möglich, wählen Sie bekannte Bezeichnungen aus Ihrem Unternehmen.

Warnung

Der Name des Titels sollte an Sonderzeichen nur "+", "-" und "_" enthalten. Das Sonderzeichen ":" ist nicht erlaubt. Das d.3 -Repository im Unicode-Modus erlaubt alle verfügbaren Zeichen.

Datentyp

Für jede erweiterte Eigenschaft müssen Sie einen **Datentyp** angeben. Derzeit werden die folgenden Datentypen unterstützt:

- **Alphanumerisch**
- **Numerisch**
- **Datum**
- **Datum und Uhrzeit**
- **Geld**

Vom Datentyp eines Feldes hängt es unter anderem ab, wie Sie Suchanfragen in d.3 smart explorer formulieren müssen. Detaillierte Informationen zu diesem Thema finden Sie im Handbuch zu d.3 smart explorer.

Alphanumerische Felder können beliebige Zeichen aufnehmen. Mit "aufnehmen" ist an dieser Stelle die Eingabe der Eigenschaft beim Archivieren gemeint. Sowohl beim Archivieren im Dialog (d.3 import) als auch bei den automatischen Verfahren (d.3 hostimport).

Bei den numerischen Feldern hingegen können nur die Ziffern "0" bis "9", das Minuszeichen "-", das Pluszeichen "+" und der Dezimaltrenner "." angegeben werden.

Die Felder des Datentyps **Geld** können die gleichen Zeichen aufnehmen wie die numerischen Felder.

Die Datumsfelder dienen dazu, ein Datum aufzunehmen.

Felder vom Typ Datum und Uhrzeit sind an sich normale Datumsfelder, die jedoch zusätzlich eine Uhrzeitangabe ermöglichen.

Bei den Datentypen numerisch und Datum nutzen Sie das Minuszeichen für die Bereichssuche bzw. sogar für eine Suche mit einem offenen Intervall.

Warnung

Für Eigenschaften bei den Batchverfahren (**HOSTIMP**, **D3ASYNC**) müssen folgende feste Syntaxregeln eingehalten werden:

Bei numerischen Feldern muss der Dezimaltrenner "." (Punkt) verwendet werden.

Die Datumsfelder müssen im deutschen Format TT.MM.JJJJ vorliegen.

Anmerkung

Der Datentyp einer Eigenschaft kann nachträglich nur noch geändert werden, wenn die Eigenschaft nicht in einer Dokumentart verwendet wird.

Position

Bevor auf die bevorzugte Position eines Feldes einer erweiterten Eigenschaft eingegangen werden kann, muss zuvor die Ablage der Eigenschaften (Kenndaten) der Dokumente in der Datenbank erläutert werden.

Das d.3 Repository legt die Eigenschaften zu einem Dokument in einer Datenbanktabelle ab, welche 89 Spalten für die Ablage der Kenndaten bereit stellt. Der Datentyp eines Feldes ist abhängig von der Datenbankspalte.

Datenbankspalten von - bis	Typ des Feldes
1 - 49	alphanumerisch
50 - 59	Datum
70 - 79	Geld
80 - 89	numerisch

Die Nummer der Spalte wird auch in einem Begriff (interner Variablenname) verwendet, welcher sich **Datenbankfeld** nennt. Die Mehrfacheigenschaftsfelder liegen in den Spalten 60 bis 69. Ein Feld, welches beispielsweise in der Datenbankspalte "33" abgelegt ist, wird also intern "dok_dat_feld[33]" genannt, ein Mehrfacheigenschaftsfeld "dok_dat_feld_60[x]", wobei x das x-te Element ist.

Durch diese Ablage der Eigenschaften in der Datenbank ist die Anzahl der Eigenschaften einer Dokumentart/Aktenart eingeschränkt. Eine Dokumentart/Aktenart kann somit maximal 49 alphanumerische Felder enthalten, zehn Felder vom Typ Datum usw.. Eine Dokumentart/Aktenart kann niemals zwei Felder (Eigenschaften) enthalten, welche an der gleichen Position liegen, d.h. die die Werte in der gleichen Datenbankspalte ablegen.

Warnung

Ein nachträgliches Ändern der DB-Position ist bei neuen Repositorys, die mit der d.3 Version 7 erstellt wurden, nicht mehr möglich.

Wenn die bevorzugte Position eines Feldes einer erweiterten Eigenschaft geändert wird, dann wird die Position dieses Feldes einer erweiterten Eigenschaft nur in dieser Dokumentart geändert.

Wenn Sie ein Eigenschaftsfeld mit einer Länge von mehr als 35 Zeichen definieren, dieses aber innerhalb einer Dokumentart auf ein anderes Datenbankfeld setzen, welches nur 35 Zeichen unterstützt, so passiert folgendes: Da die erweiterte Eigenschaftsdefinition besagt, dass das Feld länger als der Standard (35 Zeichen) ist, wird der d.3 hostimport auf einen Datenbankfehler laufen. Bei einer vorherigen Validierung der Kenndaten beim API-Import wird das betreffende Feld nach 35 Zeichen abgeschnitten und der Import läuft durch. Sind Wertemengen davon betroffen, kann es zu einem Validierungsfehler führen. Wenn es also dazu kommen sollte, dass ein Feld mit einer Länge von mehr als 35 Zeichen auf ein anderes Datenbankfeld umgesetzt werden soll, muss die betreffende Spalte in der Datenbank ebenfalls erweitert werden.

Länge

Eine Längenangabe ist nur bei den alphanumerischen Feldern möglich. Die Standardlänge dieser Felder beträgt 35 Bytes, lässt sich aber durch eine Tabellenanpassung auf 250 Bytes vergrößern. Eine Ausnahme bilden die alphanumerischen "Mehrfacheigenschaftsfelder". Diese Felder liegen an den bevorzugten Positionen 60 bis 69. Die Standardlänge dieser Felder hängt vom genutzten Datentyp ab. Für den Datentyp alphanumerisch ist die Länge bereits auf die maximal verfügbaren 250 Bytes eingestellt.

Warnung

Bei den Feldern 1-49 verhält sich das anders: Da eine direkte Änderung der Tabelle **firmen_spezifisch** zuviel an Speicherplatz auf einmal verbrauchen würde, ist diese Tabelle zunächst einmal immer noch auf 35 Bytes Länge gesetzt. Erst dann, wenn man ein Feld mit mehr als 35 Bytes Länge anlegen möchte, wird auch nur die betreffende Spalte erweitert.

Dazu geben Sie im Dialog einfach die von Ihnen gewünschte neue Länge an, maximal 250 Bytes. Die Datenbankspalte wird mit der Erstellung der neuen Eigenschaft automatisch auf die gewünschte Länge aktualisiert.

Anmerkung

Gehen Sie sorgsam mit der Vergrößerung von Datenbankspalten um. Planen Sie diese sorgfältig, damit Sie nicht unnötig viel Speicherplatz für die Daten auf der Datenbank belegen müssen.

Die Verwendung unterschiedlicher Zeichenkodierungen resultiert in unterschiedlich großen Speicherbelegungen einzelner Zeichen. Daher wird in diesem Kapitel auf "Bytes" verwiesen.

Sollte die Aktualisierung nicht automatisch erfolgen, wird ein Datenbankskript `mod_doc_field_XX.jpl` (XX = Repository-Kürzel) erstellt, das die notwendigen Datenbank-Statements enthält und über das d.3 server interface des d.3-Repository gestartet werden muss.

Gehen Sie dann bitte folgendermaßen vor:

1. Melden Sie sich über das d.3 server interface an.
2. Über den Menüpunkt **Programs > External Program** wählen Sie die Datei `mod_doc_field_XX.jpl` aus und starten diese.

Alle notwendigen Änderungen sind in dieser Datei gesammelt und werden ausgeführt.

Mehrfacheigenschaftsfeld

Wie bereits erwähnt, ist ein Mehrfacheigenschaftsfeld eine besondere Art von erweiterter Eigenschaft, welches nur an den bevorzugten Positionen "60" bis "69" liegen darf. Aus diesem Grund werden diese Felder auch "60er Felder" genannt.

Die "normalen" Felder der erweiterten Eigenschaften dienen dazu, genau einen Wert aufzunehmen, beispielsweise die Rechnungsnummer, das Bestelldatum oder einen Firmennamen. Ein Mehrfacheigenschaftsfeld kann mehrere Werte aufnehmen.

Angenommen, Sie benötigen für eine Dokumentart ein Feld mit der Bezeichnung "E-Mail Adressen". Sie könnten an dieser Stelle auch mehrere "normale" Felder verwenden, denn es können z.B. maximal 49 alphanumerische Felder definiert werden. Diese Vorgehensweise wäre jedoch sehr beschränkt. Ein Mehrfacheigenschaftsfeld kann im Standard bereits 100 Werte aufnehmen.

Über die d.3-Konfiguration (**d.3 config**, Sektion Dokumentablage) kann die Anzahl Einträge der 60-er Felder vergrößert werden.

Der maximale Wert für die Vergrößerung ist 2000.

Da momentan für eine Dokumentart maximal 89 Felder (Eigenschaften) vergeben werden können, hätte man gar nicht die Felder "E-Mail 1" bis "E-Mail 100" bilden können. Ein Mehrfacheigenschaftsfeld mit bis zu 2000 Feldern wäre somit die einzige Lösung.

Anmerkung

Mehrfacheigenschaftsfelder werden in den d.3-Anwendungen durch ein Tabellensymbol kenntlich gemacht.

Sie können die Mehrfacheigenschaftsfelder auch in Dokumentklassen Definitionen nutzen.

Beschreibung

Die Beschreibung für ein Feld einer erweiterten Eigenschaft ist rein informativ.

Sie können an dieser Stelle maximal 255 Zeichen Text angeben. Dieser informative Text wird auch in d.3 import und d.3 smart explorer angezeigt, wenn ein Anwender in der Eingabemaske die rechte Maustaste betätigt und anschließend den Punkt **Eigenschaften** auswählt.

Werteveorrat

Sie können einem Feld einer erweiterten Eigenschaft einen Wertevorrat zuordnen. Der Wertevorrat kann aus einer statischen Wertemenge, einer Datenbanktabelle (oder Datenbank-View), einer Hook-Funktion und auch durch bereits vordefinierte dynamische Wertemengen bereitgestellt werden.



Anschließend können Sie unterhalb von Wertemenge eine manuell erstellte Wertemenge zuordnen (siehe Kapitel [manuell erstellte Wertemengen](#)). Beachten Sie, dass Sie nur Wertemengen des gleichen Datentyps auswählen können.

Datenbanktabelle

Wenn Sie Werte direkt aus einer Datenbanktabelle des d.3-Repository auslesen wollen, geben Sie den Tabellennamen und den Spaltennamen an. Dadurch ist die Wertemenge eindeutig gekennzeichnet. Über diesen Weg können Sie allerdings nur eine Tabelle der Datenbank desselben d.3 -Repository ansprechen. Die Daten der Datenbanktabelle müssten entweder von d.3 oder über von Ihnen zu erstellende Funktionen eingetragen werden.

Anmerkung

Sie haben aber auch die Möglichkeit, im Datenbanksystem sogenannte Datenbank-Views (Sichten) anzulegen. Dann tragen Sie hier den Namen dieser View und den vergebenen Spaltennamen ein.



Anmerkung

Wenn Sie auf die Daten in einer Datenbanktabelle zugreifen möchten, welche sich nicht innerhalb des d.3-Datenbanksystems befindet, müssen Sie eine Hook-Funktion erstellen (siehe Kapitel Hook-Funktion).

Es werden maximal 10000 Einträge zurückgegeben. Wenn mehr benötigt werden, muss ein dynamischer Wertemengenhook basierend auf der Funktion `user_dataset_add_value` ausgeführt werden.

Hook-Funktion

Bei dieser Art von Wertemenge müssen Sie eine Hook-Funktion programmieren.

Hook-Funktionen sind kundenindividuelle Funktionen, welche die Funktionalität des d.3- Serverkerns erweitern bzw. verändern. Sie ermöglichen, dass bei bestimmten d.3-Aktionen benutzerspezifizierte Aktionen ausgelöst werden.

Hook-Funktionen müssen in der Interpretersprache JPL (Jam Programming Language) geschrieben werden. Diese Programmiersprache ähnelt der bekannteren Sprache "C", ist jedoch wesentlich einfacher zu erlernen, dafür aber auch nicht so leistungsstark.

Angenommen, in Ihrem d.3-Repository ist die Dokumentart "Software-Bestellung" definiert worden. Diese Dokumentart hat die beiden Eigenschaften "Software-Firma" und "Anwendung". Beim Archivieren von Dokumenten im Dialog mittels der d.3-Archivierung, und bei der Suche nach Dokumenten mit d.3 smart explorer soll der Anwender für die Eigenschaft "Software-Firma" eine Auswahlliste mit den Werten "Simply Save" und "Total Sources" zur Verfügung haben. Für diesen Zweck wird einfach eine manuelle Wertemenge angelegt.

Für die Eigenschaft "Anwendung" soll der Anwender ebenfalls eine Auswahlliste erhalten. In diesem Fall soll die Auswahlliste jedoch in Abhängigkeit der Eigenschaft "Software Firma" gebildet werden. Hat der

Anwender für das Feld "Software-Firma" den Wert "Simply Save" ausgewählt, soll die Wertemenge die Werte "File Storage Tool" und "Screenshot Creator" enthalten. Für den Wert "Total Sources" soll die Wertemenge die Werte "Total Sources Photo Editor" und "Total Sources Video Editor" enthalten.

Dieses Problem lässt sich nur mit einer Hook-Funktion lösen, welche die Wertemenge dynamisch in Abhängigkeit der Eigenschaft erstellt. Dazu wurden im d.3-Repository die folgenden Schritte vorgenommen:

1. Erstellen einer alphanumerischen Wertemenge mit der Bezeichnung "Software-Firmen" und den Inhalten "Simply Save" und "Total Sources".
2. Erstellen eines alphanumerischen erweiterten Eigenschaftfeldes mit der Bezeichnung "Software-Firma" an der bevorzugten Position 1. Diesem Feld wird als Wertevorrat die Wertemenge mit der Bezeichnung "Software-Firmen" zugewiesen.
3. Erstellen eines alphanumerischen erweiterten Eigenschaftfeldes mit der Bezeichnung "Anwendung" an der bevorzugten Position 2. Diesem Feld wird als Wertevorrat die Hook-Funktion mit der Bezeichnung "BuildDataset" zugewiesen.
4. Erstellen einer Dokumentart mit der Bezeichnung "Software-Bestellung". Dieser Dokumentart werden die beiden zuvor angelegten Felder zugewiesen.
5. Einem oder mehreren Benutzern die Berechtigung auf diese Dokumentart erteilen, z.B. in Form einer Dokumentklasse, eines Berechtigungsprofils oder der Zuordnung zu einer Gruppe.
6. Erstellen der Hook-Funktion. Wie Hook-Funktionen erstellt und verwaltet werden, erfahren Sie in der d.3 hook -Schulung der d.velop AG.
7. Hinzufügen der Hook-Funktion zu denen, welche vom d.3 -Server bei Programmstart geladen werden sollen. Gehen Sie dazu in die d.3 -Konfiguration und wählen Sie den Parameter **HOOK_JPL_FILES_CUSTOMER** aus. Die d.3 -Konfiguration finden Sie in d.3 admin unterhalb der **Systemeinstellungen**. Wählen Sie dort den Punkt **d.3 config** aus. Tragen Sie bei dem Parameter **HOOK_JPL_FILES_CUSTOMER** den zusätzlichen aktuellen Wert **hook_dataset.jpl** ein. Wenn beispielsweise bereits drei Hook-Funktionen dort angegeben sind, wählen Sie die vierte Zeile aus und tragen dort den Namen der Hook-Funktion ein (Doppelklick auf die vierte Zeile).
8. Wollen Sie, dass mit jedem Zugriff die Werte der Wertemenge neu zusammengestellt und geladen werden, aktivieren Sie die Checkbox im Bild der Wertemengen über Hook.



9. Danach speichern Sie die d.3 config-Einstellungen.
10. Beenden Sie d.3 admin .
11. Starten Sie den d.3-Server neu.

Quellcode

Im Folgenden sehen Sie den Quellcode der Hook-Funktion, welcher für diese Aufgabe erstellt wurde.

Diese Datei können Sie mit einem einfachen Texteditor wie beispielsweise Notepad erstellen.

Die Datei hat den Namen **hook_dataset.jpl** und muss sich in dem Programmverzeichnis des d.3-Servers befinden.

Die linke Spalte in der Tabelle enthält die Zeilennummern. Diese gehören nicht zum Quellcode. Sie wurden lediglich mit dargestellt, um den Quellcode zu beschreiben.

```

###
# Modul zum Ermitteln einer Wertemenge in Abhängigkeit von DOK_DAT_FELD_1
###
call d3_server_api_error_log("Hook-Demo: Modul geladen", 1, 9)
proc BuildDataset(repos_id, user, doc_type_short, row_no)
{
    call d3_server_api_error_log("Hook-Demo: Modul aufgerufen", 1, 9)
    call d3_server_api_error_log("Hook-Demo: DOK_DAT_FELD_1 =

```

```

:dok_dat_feld[1]", 1, 9)
  if (dok_dat_feld[1] = "Simply Save")
  {
    call d3_server_api_error_log("Hook-Demo: Simply Save", 1, 9)

    d3server_field_no_allowed [1] = ""
    d3server_value_char_allowed[1] = "File Storage Tool"
    d3server_date_1_array [1] = ""
    d3server_value_num_allowed [1] = ""
    d3server_repos_id_allowed [1] = repos_id
    d3server_field_no_allowed [2] = ""
    d3server_value_char_allowed[2] = "Screenshot Creator"
    d3server_date_1_array [2] = ""
    d3server_value_num_allowed [2] = ""
    d3server_repos_id_allowed [2] = repos_id
  }
  else if (dok_dat_feld[1] = "Total Sources")
  {
    call d3_server_api_error_log("Hook-Demo: Total Sources", 1, 9)
    d3server_field_no_allowed [1] = ""
    d3server_value_char_allowed[1] = "Total Sources Photo Editor"
    d3server_date_1_array [1] = ""
    d3server_value_num_allowed [1] = ""
    d3server_repos_id_allowed [1] = repos_id
    d3server_field_no_allowed [2] = ""
    d3server_value_char_allowed[2] = "Total Sources Video Editor"
    d3server_date_1_array [2] = ""
    d3server_value_num_allowed [2] = ""
    d3server_repos_id_allowed [2] = repos_id
  }
  return 0
}

```

Warnung

Bevor Sie eigene Hook-Funktionen erstellen, sollten Sie unbedingt an einer Schulung bei der d.velop AG teilnehmen.

Die Zeilen 1-3 sind Kommentarzeilen und haben keinen Einfluss auf das Programmverhalten. In der Zeile 4 wird ein Protokolleintrag im Logviewer vorgenommen. Diese Zeile gibt bei Programmstart des d.3-Servers den Eintrag "Hook-Demo: Modul geladen" im Logviewer aus. Wenn Sie alle Einstellungen korrekt vorgenommen haben, sollten Sie diesen Eintrag im Logviewer sehen, sobald der d.3 Server gestartet wird. In der Zeile 9 wird ebenfalls ein Eintrag im Logviewer ausgegeben. Hier wird diesmal der Inhalt von **DOK_DAT_FELD_1** ausgegeben. Es ist wichtig, den vorangestellten Doppelpunkt anzugeben, da ansonsten nicht der Inhalt des Feldes, sondern nur der Text "dok_dat_feld[1]" dargestellt würde.

In der Zeile 11 wird nun der Inhalt von **DOK_DAT_FELD_1** abgefragt. Wenn es sich um den Begriff "Simply Save" handelt, dann werden die Zeilen 14 bis 26 durchlaufen, und wenn es sich um den Begriff "Total Sources" handelt, werden die Zeilen 30 bis 44 durchlaufen.

Der Befehl in der Zeile 15 ist aus Kompatibilitätsgründen anzugeben. In der Zeile 16 wird dann der erste Eintrag der Wertemenge zugewiesen. Da in unserem Beispiel die Wertemenge einem alphanumerischen erweiterten Eigenschaftsfeld zugewiesen werden soll, ist unbedingt die globale Liste (Array) **d3server_value_char_allowed** zu verwenden. Wenn es sich um ein Datumsfeld handelt, muss das Array **d3server_date_1_array** verwendet werden, und im Falle eines numerischen Feldes das Array mit der Bezeichnung **d3server_value_num_allowed**. Bei Datumsangaben muss die deutsche Schreibweise "TT.MM.JJJJ" verwendet werden.

In der Zeile 19 wird zum Abschluss die Kennung des erweiterten Eigenschaftsfeldes einem globalen Array zugewiesen. Diese Kennung wird an die Hook-Funktion von dem d.3-Server beim Aufruf übergeben (Zeile 6).

Weiterführende Literatur zu dem Thema "Hook-Programmierung" erhalten Sie bei der d.velop AG.

Vordefinierte dynamische Wertemengen

Als dynamische Wertemengen stehen zusätzlich die Benutzer, Gruppen sowie bereits erfasste Werte (dynamische Datasets) als Auswahlmöglichkeiten zur Verfügung.



Alle Benutzer: Sie erhalten alle zur Laufzeit existierenden Benutzer des d.3 -Repository aufgelistet.

Alle Gruppen: Analog werden über diese Zuordnung alle Gruppen des d.3 -Repository aus dem Wertevorrat aufgelistet.

Alle Benutzer/Gruppen: Alle Benutzer und Gruppen des d.3-Repository werden als Wertevorrat zur Auswahl bereitgestellt.

Alle existierenden Werte: Es wird die Datenbanktabelle gelesen und jeder bereits erfasste Wert dieses Eigenschaftsfeldes (der gewählten Dokumentart) präsentiert.

Diese Funktionalität musste in früheren Versionen zum Teil über Hook-Funktionen realisiert werden.

Anmerkung

Aus der Datenbanktabelle werden alle Werte der angesprochenen Dokumentart gelesen, auf einfaches Vorkommen reduziert und sortiert präsentiert.

Plausibilitätskontrolle erweiterte Eigenschaften

Die Plausibilitätskontrollen eines Feldes einer erweiterten Eigenschaft dienen dazu, die Attribute zu einem Dokument während des Archivierens auf Gültigkeit zu überprüfen.

Angenommen, ein Anwender möchte eine Rechnung archivieren. Die Dokumentart "Rechnung" enthält ein Feld einer erweiterten Eigenschaft mit der Bezeichnung "Firma", in welches der Anwender den Firmennamen der ausgestellten Rechnung eintragen muss. An dieser Stelle muss verhindert werden, dass der Anwender einen Namen wie beispielsweise "12345" als Firmenname angibt. Als Firmenname ist als erster Buchstabe ein ["A" - "Z"] gefolgt von ["a" - "ü"] beliebig oft zulässig.



Wenn keine Eingabeüberprüfung (Plausibilitätskontrolle) vorgenommen wird, würde die Rechnung unter einem "falschen" Firmennamen im d.3-Repository abgelegt werden. Ein gezieltes Wiederfinden dieser Rechnung wäre dann fast ausgeschlossen.

In der Anwendung d.3 import wird diese Plausibilitätskontrolle bei jedem Archivierungsvorgang durchgeführt. Sie können diese Überprüfung jedoch auch manuell anstoßen, in dem Sie die Funktion **Eingaben prüfen** (über das Kontextmenü, den Link in der Navigationsleiste oder die Drucktaste) abrufen.

Warnung

Die Plausibilitätskontrollen greifen sowohl bei den automatischen Importverfahren HOS-TIMP, als auch beim Archivieren im Dialog mit der Anwendung d.3 import.

Wenn jedoch der Konfigurationsparameter **NO_ATTRIBUTE_CHECK_ON_BATCH** auf den Wert "Ja" gesetzt ist, dann wird bei den automatischen Importverfahren keine Plausibilitätskontrolle durchgeführt. Diesen Parameter können Sie mit der d.3-Konfiguration einstellen.

Hook-Funktion

Wie bereits in dem Kapitel <https://confluence.d-velop.de/display/DDAD/Wertemengen+aus+einer+d.3+Hook-Funktion+v7.2.2> Wertemengen erwähnt wurde, ist eine Hook-Funktion eine in JPL geschriebene Routine, welche vom d.3- Server ausgeführt wird. Bei der Plausibilitätskontrolle können Sie ebenfalls Hook-Funktionen verwenden. In der Hook-Funktion selbst können Sie wiederum komplexe Überprüfungen vornehmen. Sie könnten beispielsweise überprüfen, ob ein angegebener Wert in einer bestimmten Datenbanktabelle vorkommt (vgl. Beispiel im Kapitel [Plausibilitätskontrolle](#)).

Bei den Einstellungen zu dem erweiterten Eigenschaftensfeld muss an dieser Stelle wieder der Name der Hook-Funktion eingetragen werden. Die weitere Vorgehensweise ist vergleichbar mit der Vorgehensweise bei Wertemengen. Sie müssen ebenfalls eine Textdatei erstellen, in der eine Funktion mit dem konfigurierten "Hook-Funktionsnamen" enthalten ist. Es dürfen auch mehrere Hook-Funktionen in einer Datei vorkommen. Somit könnten Sie den Programmcode dieser Funktion auch in die Datei **hook_dataset.jpl** aufnehmen (siehe Kapitel [Wertemengen aus einer d.3 Hook-Funktion](#)). Weiterhin muss die Datei **hook_dataset.jpl** (wenn nicht schon geschehen) in die Liste der ladbaren Hook-Funktionen mit aufgenommen werden.

Minimum/Maximum

Die Überprüfung von **Minimum** und **Maximum** bezieht sich nur auf numerische Felder einer erweiterten Eigenschaft.

Muss beispielsweise der numerische Wert eines Feldes in dem Bereich 500 bis 1000 liegen, geben Sie als Minimum den Wert 500 und als Maximum den Wert 1000 an.

Regulärer Ausdruck

Regular Expressions findet man sehr häufig im Unix-Umfeld zum Suchen oder Editieren von Texten. Sie dienen zur Beschreibung von Textmustern in einer formalen Sprache.

In d.3 werden Regular Expressions verwendet, um die Eingabe von Eigenschaften beim Importieren auf Texte eines bestimmten Musters zu beschränken. Im Folgenden werden "Ein-Zeichen-Muster" und "Multipliiert" erklärt und anhand von Beispielen verdeutlicht.

Anmerkung




Regular Expressions haben nur eine Wirkung auf die alphanumerischen Felder von d.3. Sie können nicht für numerische Felder, Datumsfelder oder Geldfelder verwendet werden.

Weiterführende Literatur zu Regular Expressions finden Sie in UNIX-Handbüchern und im Internet. Beachten Sie jedoch, dass einige Ausdrücke, die in UNIX-typischen Dialekten vorkommen, wie Anker und Klammern zur Speicherung, in d.3 ggf. nicht funktionieren. Prüfen Sie unbekannte Syntax immer zuerst mit Hilfe der Testfunktion.

Über die d.3-Konfiguration können Sie den Interpreter der regulären Ausdrücke bestimmen (POSIX, PERL, JPL). Dabei kann sich dann die erlaubte Syntax unterscheiden.





Ein-Zeichen-Muster

Das Grundelement der Regular Expressions ist das Ein-Zeichen-Muster. Bei der Verwendung eines Ein-Zeichen-Musters als Regular Expression in d.3 ist nur die Eingabe des Ein-Zeichen-Musters selbst erlaubt.

Regular Expression	Benutzereingabe	
A	A	
A	B	
A	Easy	

Menge

Mehrere Zeichen oder Bereiche können in einer Menge zusammengefasst werden. Mengen werden in eckigen Klammern angegeben. Eine Menge ist als Ganzes auch ein Ein-Zeichen-Muster. Bei Verwendung einer Menge als Regular Expression ist die Eingabe zulässig, wenn eines der in der Menge angegebenen Zeichen eingegeben wird.

Regular Expression	Benutzereingabe	
[abc]	Kleinbuchstabe "b"	
[abc]	D	
[0-9]	F	
[0-9]	7	

Negation




Umgekehrt kann man auch eine Menge von Zeichen als Menge angeben, die NICHT im Eigenschaftswert enthalten sein dürfen. Dazu geben Sie als erstes Zeichen das Zeichen "^" in der Mengenklammer an. Bitte beachten Sie, dass zwischen der Groß- und Kleinschreibung unterschieden wird.

Regular Expression	Benutzereingabe	
[^abc]	D	
[^abc]	Kleinbuchstabe "a"	

Muster




Schließlich lassen sich noch mehrere Ein-Zeichen-Muster zu einem Muster zusammenstellen. Diese Muster können natürlich auch Mengen enthalten. Bereiche werden gemäß dem ASCII-Zeichensatz interpretiert. Bei der deutschen Sprache müssen Sie daher die Umlaute besonders beachten.

Regular Expression	Benutzereingabe	
[A-ZÄÖÜ][a-zäöü][a-zäöü][a-zäöü]	Otto	

Regular Expression	Benutzereingabe
[A-ZÄÖÜ][a-zäöü][a-zäöü][a-zäöü]	Säge 
[A-ZÄÖÜ][a-zäöü][a-zäöü][a-zäöü]	Administrator  (es werden nur genau vier Zeichen zugelassen)
[A-Z][a-z][a-z][a-z]	Säge  (ein ä ist nicht gestattet)

Punkt

Der Punkt ist ein besonderer regulärer Ausdruck. Er erlaubt die Eingabe eines beliebigen Zeichens, außer "#013" (carriage return).

Regular Expression	Benutzereingabe
[A-ZÄÖÜ].[0-9].	BE13 
[A-ZÄÖÜ].[0-9].	A999 
[A-ZÄÖÜ].[0-9].	A1 





Multiplii






Multiplii Zeichen geben an, wie oft ein Ein-Zeichen-Muster eingegeben werden soll:

beliebig häufig, aber auch 0 mal	soll ein Zeichen gar nicht oder beliebig oft eingegeben werden, hängt man einen Stern an das Ein-Zeichen-Muster ("**")
genau n mal	soll ein Zeichen genau n mal eingegeben werden, hängt man die Zeichen \"{n}\" an das Ein-Zeichen-Muster und ersetzt n durch die entsprechende Anzahl
mindestens n mal	soll ein Zeichen mindestens n mal eingegeben werden, hängt man die Zeichen \"{n,}\" an das Ein-Zeichen-Muster und ersetzt n durch die Mindestanzahl
mindestens n mal, höchstens m mal	soll ein Zeichen mindestens n mal und höchstens m mal eingegeben werden, hängt man die Zeichen \"{n,m}\" an das Ein-Zeichen-Muster und ersetzt n durch die Mindest- und m durch die Höchstanzahl

Anmerkung

Wird für die Interpretation der regulären Ausdrücke die "POSIX Extended Regular Expression Syntax" genutzt, müssen die Backslashes "\" entfallen.

Regular Expression	Benutzereingabe
Alpha.*	Alpha 
Alpha.*	Alphabet 
Alpha.*sch	Alphanumerisch 
x{3}	X 

Regular Expression	Benutzereingabe	
x\{3}	xxx	
Ja\{4\}!	Ja!	
Ja\{4\}!	Jaaaa!	
Schif\{2,3\}ahrt	Schiffahrt	
Schif\{2,3\}ahrt	Schiffahrt	

Die Drucktaste **Test** können Sie zum Testen der Regular Expressions benutzen. Dazu geben Sie in dem Feld ein Wort ein und drücken Sie anschließend auf **Test**.

Anmerkung

Die Regular Expression-Validierung läuft über den JPL-Interpreter. Dieser entfernt bei jeder Zuweisung alle angehängten Leerzeichen. Leerzeichen in einem Eigenschaftsfeld am Ende werden also vor der Validierung gelöscht.

Gesamtübersicht aller erweiterten Eigenschaften

Mit dieser Funktion wird Ihnen die Möglichkeit gegeben, alle eingetragenen erweiterten Eigenschaften und Ihre dazugehörigen Eigenschaftsfelder innerhalb der Datenbank übersichtlich in einer Tabelle anzeigen zu lassen. Um die Überblickstabelle anzeigen zu lassen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Übersicht der erweiterten Eigenschaften**.
2. Klicken Sie mit der rechten Maustaste auf ein beliebiges Feld.
3. Wählen Sie im Kontextmenü den Eintrag **Gesamtübersicht**.



Sie erfahren über die Zuordnungen, welche erweiterten Eigenschaften welchem Datenbankfeld zugeordnet wurden. Auch die Doppelbelegungen können erkannt werden.

Übersicht der Datenbankfelder

Mit dieser Funktion wird Ihnen die Möglichkeit gegeben, alle eingetragenen erweiterten Eigenschaften und Ihre dazugehörigen Eigenschaftsfelder innerhalb der Datenbank übersichtlich in einer Tabelle anzeigen zu lassen. Um die Überblickstabelle anzeigen zu lassen, gehen Sie wie folgt vor:

1. Öffnen Sie das Fenster **Übersicht der Felder**.
2. Klicken Sie mit der rechten Maustaste auf ein beliebiges Feld.
3. Wählen Sie im Kontextmenü den Eintrag **Gesamtübersicht**.



Sie erfahren über die Zuordnungen, welche Eigenschaften welchem Datenbankfeld zugeordnet wurden. Auch die Doppelbelegungen können erkannt werden.

Dokumentarten

Das zentrale Merkmal zur Klassifizierung von Dokumenten im d.3- Umfeld ist die Dokumentart. Alle Dokumente, sei es ein Microsoft Word Dokument, eine AutoCAD Zeichnung, eine Sounddatei, ein

Anwendungsprogramm oder ein Videoclip, werden bei der Ablage im d.3 (über den d.3 import bzw. Hostimport) einer Dokumentart/Aktenart zugewiesen. Für den Endanwender ist die Dokumentart das wichtigste Kriterium für die Suche nach Dokumenten.

Anmerkung

Es ist also unbedingt darauf zu achten, dass Sie Dokumentarten/Aktenarten bilden, welche Ihrem Unternehmen entsprechen. Verwenden Sie Namen, welche bereits in Ihrem Unternehmen bekannt sind.

Warnung

Sie können maximal 2.000 Dokument-/Aktenarten für das d.3 -Repository definieren.

Anmerkung

In der Übersicht der Dokumentarten werden Systemdokumentarten ausgeblendet. Bei der Dokumentklassen-Erstellung stehen diese zur Verfügung.



Angaben zur Dokumentart

Zur Anlage einer Dokument- bzw. Aktenart sind verschiedene Informationen zu erfassen. Sie werden in einer Dialogfolge entsprechend geleitet.



Basiskonfiguration

Für jede Dokument- bzw. Aktenart müssen Sie neben dem Namen weitere Informationen zuordnen.



Name

Der Name einer Dokumentart ist das wesentlichste Merkmal für den Anwender zur Unterscheidung von Dokumentarten. Dieser Name findet sich in allen d.3-Anwendungen wieder.

Anmerkung

Der Name oder auch die Bezeichnung einer Dokumentart kann maximal 50 Zeichen lang sein.

Warnung

Der Name einer Dokumentart darf alle Zeichen enthalten. Die Bezeichnung der Dokumentart muss immer eindeutig sein.

Anmerkung

Wenn Sie den Namen einer Dokument-/Aktenart nachträglich ändern, ist es erforderlich, dass sich die Anwender neu an d.3 anmelden.

Dem Anwender wird das deutlich gemacht, indem das d.3-Symbol im Infobereich (Systemray) ein Ausrufezeichen anzeigt oder in den Ergebnissen das Einbahnstraßen-Symbol erscheint.

d.3 smart explorer kann in diesem Fall die Darstellung nicht erzeugen, da die Struktur der "neuen" Dokumentart nicht geladen wurde.

Warnung

Beachten Sie, dass eine Änderung des Namens unter Umständen Probleme hervorrufen kann. Probleme entstehen immer dann, wenn in Ihrem d.3- Umfeld Prozesse/Verfahren den Namen einer Dokument-/Aktenart zur Weiterverarbeitung verwenden. Dies ist z.B. bei Verwendung des Produktes d.cold der d.velop AG der Fall.

Ebenso kann d.3 hostimp so konfiguriert sein, dass der Name der Dokument-/Aktenart verwendet wird. Der Name kann auch in Hook-Funktionen verwendet werden.

Es sollte immer versucht werden, das maximal fünfstellige Kürzel einer Dokumentart zur Referenzierung einer Dokumentart zu verwenden. Denn im Gegensatz zu dem Namen einer Dokumentart bleibt das Kürzel einer Dokumentart für die gesamte Lebensdauer konstant. Der Name einer Dokumentart hingegen kann ohne Probleme geändert und auch übersetzt werden.

Art

Im d.3- Umfeld wird zwischen Dokumentarten und Aktenarten unterschieden.

Der wesentliche Unterschied besteht darin, dass Akten untergeordnete und übergeordnete Dokumente enthalten können.

In Akten wird in der Regel KEIN Dokument direkt abgelegt, sie dienen lediglich der strukturierten Ablage (ähnlich wie früher in Papierarchiven auch).

Kürzel

Das Kürzel einer Dokument-/Aktenart ist das eindeutige Kennzeichen und entscheidende Merkmal für Verfahren im d.3- Umfeld. Bei dem Kürzel wird zwischen Groß- und Kleinschreibung unterschieden. Somit kennzeichnen die Kürzel "XAKTE" und "Xakte" zwei unterschiedliche Arten. Die maximale Länge des Kürzels beträgt fünf Zeichen. Das Kürzel darf nur die folgenden Zeichen enthalten: "a..z", "A..Z", "0..9" und das Minuszeichen "-".

Vorschlag für die Vergabe eines Kürzels:

- Nutzen Sie alle fünf Stellen aus.
- Nutzen Sie nur die Großschreibweise.
- Nutzen Sie ein A für eine Aktenart als erstes oder letztes Zeichen, ein D für eine Dokumentart.

Da das Kürzel bei Fehlern auch im zentralen Protokoll angegeben wird, erleichtert Ihnen diese Vergabe ggf. die Zuordnung bei der Fehlersuche.

Anmerkung

Das Kürzel einer Dokument-/Aktenart kann nicht nachträglich geändert werden. Sie müssten in diesem Fall die Dokument-/Aktenart entfernen und anschließend neu hinzufügen. Um jedoch eine Dokument-/Aktenart zu entfernen, müssen Sie zuerst die Dokumente, welche dieser Dokument-/Aktenart zugeordnet sind, entfernen.

Warnung

Eine Änderung des Kürzels (Entfernen + Hinzufügen) kann Probleme hervorrufen. Bitte bedenken Sie, dass eventuell Verfahren im d.3 -Umfeld das Kürzel zur Weiterverarbeitung verwenden. Möglicherweise wird das Kürzel von d.cold, dem d.3 hostimp oder in Hook-Funktionen verwendet.

Repository-ID

Das d.3 -Repository unterstützt über d.ecs storage manager unterschiedliche Sekundärspeicher-Systeme. Für die Ansteuerung des Sekundärspeichers wird d.ecs storage manager zur Verfügung gestellt. Sie haben die Möglichkeit, Dokumente in unterschiedliche „logische Archive“ (Pools) auf dem Sekundärspeicher abzulegen.

Beispielsweise sollen die Dokumente der Dokumentart "Lieferschein" in das eine "logische Archiv" (z.B. Kürzel "LA") und die Dokumente der Dokumentart "Rechnungen" in ein anderes "logisches Archiv" (z.B. Kürzel "RA" für Rechnungsarchiv) geschrieben werden. Für diesen Zweck wird die Repository-ID verwendet.

Für die Repository-ID können Sie maximal zwei Zeichen verwenden. Es wird momentan zwischen Groß- und Kleinschreibung unterschieden. Weiterhin werden zurzeit nur fünf unterschiedliche Repository-IDs unterstützt. Die erlaubten Kennungen werden mit d.3 config in der Sektion Dokumentablage eingestellt. Wählen Sie dort als Parameter den Begriff `server_archive_id_array` aus. Diese Einstellung erreichen Sie auch, indem Sie den Punkt [d.3 Dokumentablage](#) auswählen und anschließend die Option **zusätzliche Serverkürzel**.

Die eindeutige Kennung von Dokumenten (Dokument-ID) wird bei der Verwendung einer Repository-ID aus dieser gebildet. Wählen Sie beispielsweise für Rechnungen die Repository-ID "RE", dann könnte die Dokument-ID "RE500000" lauten.

Selbst wenn Sie keinen Sekundärspeicher verwenden, können Sie eine Repository-ID vorgeben. Somit könnten Sie schon jetzt eine Klassifizierung der Dokumentarten vornehmen. Bei einem späteren Einsatz eines Sekundärspeichers können die Dokumente dann anhand dieser Klassifizierung ausgelagert werden.

Warnung

Wenn Sie unterschiedliche Repository-IDs verwenden, müssen Sie zusätzlich das Produkt d.ecs storage manager anpassen. Eine genaue Beschreibung der Konfigurationsmöglichkeiten finden Sie in dem Handbuch zu dem Produkt d.ecs storage manager. Eine Anpassung ist auch erforderlich, wenn Sie nachträglich eine Repository-ID ändern, ansonsten werden die Dokumente nicht ausgelagert.

Ungeschützter Webzugriff

Diese Einstellung wird notwendig, wenn Sie d.3 webpublisher der d.velop AG verwenden möchten.

Dieses Produkt ermöglicht einem Anwender den Zugriff auf Dokumente im d.3-Repository über das World Wide Web. Der Anwender muss sich hierbei nicht dem System gegenüber autorisieren. Es erfolgt also keine Abfrage des Benutzernamens oder des Kennwortes.

Die Software d.3 webpublisher wird mit der Version 6.3 nicht mehr ausgeliefert, da er die veraltete Technik der CGI-Skripte nutzt.

Nachdem der Anwender die URL für d.3 webpublisher auswählt, werden ihm all die Dokument-/Aktenarten zur Recherche angeboten, bei denen die Option **Web veröffentlicht** gesetzt ist.

Von einer für das Web veröffentlichten Dokument-/Aktenart sind wiederum nur die Dokumente zugänglich, welche zuvor mittels d.3 smart explorer veröffentlicht wurden.

Damit Sie mit d.3 smart explorer Dokumente veröffentlichen können, muss sich in dem Arbeitsverzeichnis die Datei **WebPub.DXP** befinden. Wenn eine solche Datei nicht vorhanden ist, können Sie zum einen diese Datei in den Verteilmechanismus des d.3-Anwendungen mit aufnehmen oder diese Datei manuell in das Arbeitsverzeichnis kopieren. Wenn Sie die Datei manuell in das Verzeichnis kopieren, setzen Sie bitte das Dateiattribut "Versteckt" (Kommandozeilenaufwurf: **attrib +h WebPub.DXP**), da ansonsten bei dem nächsten Start von d.3 smart explorer diese Datei gelöscht wird.

Wenn diese Datei nun in dem Verzeichnis vorhanden ist, müssen Sie d.3 smart explorer neu starten. Sie können anschließend die entsprechenden Dokumente, die veröffentlicht werden sollen, im d.3-Repository suchen und durch Betätigen der rechten Maustaste und Auswahl von **Web veröffentlicht** veröffentlichen.

Denken Sie daran, dass die Veröffentlichung nur für freigegebene Dokumente möglich ist.

Wenn Ihnen der Menüeintrag **Web veröffentlicht** in d.3 smart explorer nicht zur Verfügung steht, haben Sie entweder d.3 smart explorer nicht neu gestartet, oder die Datei WebPub.DXP befindet sich nicht in dem Arbeitsverzeichnis von d.3 smart explorer.

4-Augen-Prinzip

Dokumente, die einer Dokument-/Aktenart angehören, bei denen diese Option gesetzt ist, darf der Bearbeiter nicht selber prüfen (Status: Prüfung > Prüfung abschließen), auch wenn er die nötigen Rechte hat. Bearbeiter ist immer derjenige, der das Dokument in seiner Bearbeitung hält, Besitzer ist derjenige, der das Dokument im d.3 abgelegt hat bzw. bei mehreren Versionen die Freigabe-Version erstellt hat.

Somit muss der Bearbeiter (der Ersteller/Ändernde) eines Dokumentes eine andere Person sein als die, die das Dokument anschließend prüft.

Vorbuchen

Das Vorbuchen von Dokumenten ist ein spezielles Verfahren der d.velop AG.

Dieses Verfahren wird dazu verwendet, Eigenschaften (Kenndaten) für ein Dokument anzulegen, ohne dass ein Dokument mit angelegt wird. Das Dokument wird bei diesem Verfahren zu einem späteren Zeitpunkt nachgereicht (z.B. **spätes Scannen** mit Barcode).

Dieses Verfahren wird von d.3 import verwendet. Wenn man bei d.3 import in den Vorbuchen-Modus wechselt, werden zum einen nur die Dokument-/Aktenarten zur Auswahl angeboten, bei den die Option **Vorbuchen** eingestellt ist, und zum Zweiten wird beim Betätigen von **Vorbuchen** kein Dokument archiviert, sondern nur die Kenndaten im d.3-Repository angelegt.

Zusätzlich kann ein Barcode-Deckblatt gedruckt werden, das dann auf das beim Sachbearbeiter liegende "analoge" Dokument gelegt und anschließend zur zentralen Scanstelle gebracht wird. Über den Barcode wird dann das Dokument den bereits erfassten Eigenschaften zugeordnet.

Im Customizing-Handbuch zu d.3 import können Sie nachlesen, wie Sie in den Vorbuchen-Modus umschalten können.

Beim Vorbuchen wird bei der Anlage der Eigenschaften (Kenndaten) ein Eintrag in der Datenbanktabelle **firmen_spezifisch** vorgenommen. Standardmäßig wird der Eintrag in der Datenbankspalte **dok_dat_feld_88** getätigt. Diese Voreinstellung können Sie jedoch mit d.3 config ändern. Wählen Sie

dazu unter **Systemeinstellungen > d.3 config > Import Einstellungen > Feldnummer für Barcode Status** den Parameter **BARCODE_STATUS_FIELD_NR** aus.

Bei der Anlage der Kenndaten wird in diese Datenbankspalte der Wert "0" (Null) eingetragen. Dieser Wert zeigt an, dass es zu den Kenndaten noch kein Dokument gibt. Wenn nun zu einem späteren Zeitpunkt das Dokument (Nutzfile) nachgereicht wird, dann wird der Eintrag in dieser Datenbankspalte auf den Wert "1" gesetzt.

Lebensdauer

Da für jede Art von Dokumenten ggf. eine andere Aufbewahrungspflicht besteht, vergeben Sie hier die Daten zur Aufbewahrung. Die Standardeinstellung zur Lebensdauer ist 50 Jahre.



Für die DSGVO-konforme Planung bzw. Konfiguration Ihres d.3ecm-Systems kann es jedoch sein, dass diese Einstellung geändert werden muss. Informieren Sie sich daher vor dem Anlegen von Dokumentarten mit den Anforderungen der DSGVO/GDPR, damit Sie die richtigen Aufbewahrungsfristen setzen können. Ein ECM-System wie d.3ecm kann erst dann eingerichtet bzw. in Betrieb genommen werden, wenn die Aufbewahrungsfristen für die einzelnen Dokumentarten sauber definiert und konfiguriert sind. Eine nachträgliche Änderung der Aufbewahrungsfristen auf dem Sekundärspeicher - nach Inbetriebnahme - ist extrem aufwändig oder auch gar nicht möglich.

Bitte überprüfen Sie auch, ob die gewünschten Einstellungen zum Löschen von Dokumenten/Objekten in d.3 admin unter [d.3 config](#) eingestellt sind. Beachten Sie dazu folgende Einstellungen:

- „Logical“ Deletion of Expired Documents
- „Physical“ Deletion of Expired Documents
- Delete Documents from Secondary Storage

Anmerkung

Wenn bei einer Akte eine andere Lebensdauer als ewig angegeben wird, erscheint die Warnmeldung: "Um ein unbeabsichtigtes, automatisches Entfernen von Akten zu vermeiden, sollte die Lebensdauer bei einer Akte immer auf 'ewig' stehen."

Beachten Sie, dass die Lebensdauer nicht "0" sein kann.

Lebensdauer in Monaten

Die Lebensdauer wird als Wert bei jeder neuen Version eines Dokuments auf das aktuelle Tagesdatum addiert und als Aufbewahrungszeit in der Datenbank vermerkt .

Für jede Dokumentart können Sie definieren, ob Sie **Ereignisloses Löschen** (bisherige Standardeinstellung) oder **Ereignisorientiertes Löschen** durchführen möchten.

Lebensdauer ab

Für ereignisunabhängiges Löschen können Sie definieren, ab wann die Lebensdauer beginnen soll.



Im Standard wird die Lebensdauer ab dem Importdatum bestimmt, d.h. auf das Importdatum wird die Anzahl Monate addiert und somit das Aufbewahrungszeit festgelegt.

Die Lebensdauer kann aber auch auf das Ende eines gewählten Monats hochgerechnet werden, um besonderen Forderungen zu genügen, z.B. Ende eines Quartals oder Geschäftsjahres.

Auf Sekundärspeicher auslagern

Diese Option gibt an, dass die Dokumente dieser Dokument-/Aktenart auf ein angeschlossenes Sekundärspeicher-System ausgelagert werden sollen, um die Revisionsicherheit zu gewährleisten. Ausgelagert werden nur Dokumente im d.3 -Status "Freigabe" und "Archiv".

Anmerkung

Diese Einstellung allein bewirkt noch nicht das automatische Auslagern von Dokumenten. Sie müssen zusätzlich in der d.3- Konfiguration die Option **AUTO_DOCS_ON_SEC_STORAGE** auf "Ja" setzen. Diese Einstellung finden Sie unterhalb der Sektion **Sekundärspeicher** . Bitte überprüfen Sie an dieser Stelle auch die anderen Einstellungen für das Ansprechen des Sekundärspeichers. Weiterhin muss das Produkt d.ecs storage manager installiert und konfiguriert sein. Eine Jukebox mit einem Jukebox Controller wird unterstützt.

Warnung

Wenn Sie die Sekundärspeicher Auslagerung für eine Dokumentart aktivieren und ebenfalls die Einstellungen in der d.3- Konfiguration vornehmen, jedoch kein Sekundärspeicher vorhanden ist, werden die Cache Bereiche für den Status "**Freigabe**" bzw. "**Archiv**" dennoch mit einer Kopie des Dokuments beschrieben, aber durch die „fehlende“ Quittung nicht gelöscht.

Anmerkung

Damit das Auslagern von Dokumenten reibungslos funktioniert, müssen die Komponenten d.3 async und d.ecs storage manager korrekt arbeiten.

Wenn die Option **Auf Sekundärspeicher auslagern** für eine Dokumentart eingestellt ist und Sie betätigen beispielsweise in d.3 smart explorer die rechte Maustaste und wählen **Dokumentstatus ändern > Freigabe** aus, dann wird das Dokument auf den Sekundärspeicher geschrieben.

Ereignisorientiertes Löschen

Wird ereignisorientiertes Löschen gewählt, wird die Aufbewahrungszeit über ein definiertes Ereignis, z.B. Produktaufkündigung, bestimmt.

Näheres finden Sie im Kapitel [Aufbewahrungsfristen und Löschen](#).

Für das eigentliche Löschen müssen weitere Parameter in der d.3- Konfiguration gesetzt werden (siehe d.3 [Asynchrone Verarbeitung](#)).

Cache-Verweildauer

Wenn ein Dokument in den Status "Freigabe" oder "Archiv" transferiert wird, sei es direkt bei der Anlage eines Dokumentes, z.B. mittels d.3 hostimp und automatischem Statustransfer in die Freigabe, oder beim manuellen Statustransfer mittels d.3 smart explorer , dann wird dieses Dokument in das **Jukebox**-Austauschverzeichnis auf dem d.3- Dateiserver kopiert, sofern die Einstellungen für die Option [Auf Sekundärspeicher auslagern](#) vorgenommen wurden.

Wird das Dokument erfolgreich auf das Sekundärspeicher-System übertragen, dann verbleibt das Dokument noch entsprechend lange auf dem Datei-Server.

Wird ein gelöscht Dokument von einem Anwender angefordert, dann wird es wieder vom Sekundärspeicher auf den d.3- Dateiserver überspielt. Auf dem Datei-Server wird dieses Dokument in dem Austauschverzeichnis **Jukebox** abgelegt. Dort steht das Dokument solange zur Verfügung, bis d.3 gateway dieses wieder löscht. Die genauen Einstellungen, die für das Löschen der Dokumente in dem Verzeichnis **Jukebox** zuständig sind, können Sie in den Handbüchern zu d.3 gateway und d.ecs storage manager der d.velop AG nachschlagen.

Die Cache-Verweildauer in Tagen hat keinen Einfluss auf das Löschen in dem Verzeichnis **Jukebox**.

Anmerkung

Damit das Löschen von Dokumenten reibungslos funktioniert, müssen die Komponenten d.3 async und d.ecs storage manager korrekt arbeiten.

Für die Recherche muss weiterhin d.3 gateway korrekt arbeiten.

Vorzeitige Entfernung

Anmerkung

Falls die freie Festplattenkapazität auf dem d.3- Dateiserver zu knapp wird, werden bereits auf das Sekundärspeicher-System ausgelagerte ("gebrannte") Dokumente auf jeden Fall von der Festplatte gelöscht, unabhängig von der Einstellung **Cache-Verweildauer**, wenn dies mit der Option **Vorzeitige Entfernung bei Speicherplatzmangel erlauben** erlaubt wurde.

Cache-Verweildauer ewig

Anmerkung

Ab der d.3 Version 6.3 gibt es die Möglichkeit zu bestimmen, dass Dokumente nie vom Cache gelöscht werden (Dauer: ewig). Dieser Eintrag ist allerdings mit Vorsicht zu verwenden. Er sollte nur bei Dokumentarten mit geringem Dokumentaufkommen genutzt werden. Sie erhalten daher auch eine Warnmeldung.

Die Cache-Verweildauer kann nicht mehr "0" sein.

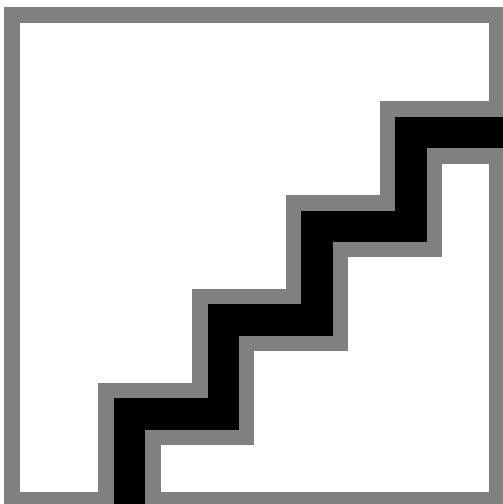


Definition für Farbmarkierungen

Sie können zu der Dokumentart eine Farbmarkierung definieren, indem Sie auf **Hinzufügen** klicken oder einen Doppelklick in den leeren Bereich durchführen.



Es öffnet sich ein Fenster "Farbmarkierung", welches die Farbpalette abbildet und ein Textfeld zur Beschreibung und Sprachauswahl anbietet.



1. Wählen Sie die gewünschte Farbe aus der Farbpalette aus.
2. Geben Sie optional einen Beschreibungstext an.
3. Ändern Sie ggf. die Sprache.
4. Mit **OK** bestätigen Sie Ihre Farbmarkierung.

Anmerkung

Bei Farbmarkierungen handelt es sich um eine flexibel nutzbare Markierung von Dokumenten, die jedes Unternehmen intern mit Bedeutungen belegen kann. Ähnlich wie bei realen Akten (gefüllt mit Seiten aus Papier) können nun Dokumente und Akten mit einer Art Haftnotiz in einer bestimmten Farbe markiert werden.

Es stehen 24 Farben zur Verfügung. Es bietet sich an, Farben unternehmens- oder abteilungsweit für bestimmte Prozesse als Signal und eine gewisse Anzahl für die individuelle Nutzung durch d.3-Anwender zu definieren. Eine Farbe könnte z.B. bedeuten, dass ein Dokument noch überarbeitet werden muss, vor Ausdruck geprüft werden sollte oder sich in einem bestimmten Workflowschritt befindet.

Darüber hinaus können Sie als d.3-Administrator auch in jeder Kategorie (Dokumentart oder Aktenart) pro Farbe einen Text definieren, der den Anwendern dann angezeigt wird, wenn sie mit der Maus darauf zeigen.

Der Text wird dann nur angezeigt, wenn die Farbe einem Dokument oder einer Akte in der bestimmten Kategorie zugewiesen wird. Dieselbe Farbe kann also auch einen anderen Text in einer anderen Kategorie haben.

Erweiterte Eigenschaften auswählen

Jeder Dokument- oder Aktenart werden 1 bis maximal 89 erweiterte Eigenschaften zugewiesen. Diese zugewiesenen erweiterten Eigenschaften nehmen die Eigenschaften zu den Dokumenten dieser Dokumentart/Aktenart beim d.3 import auf. Wenn Sie später Dokumente in das d.3- Repository einbringen, sei es im Dialog oder im Batchverfahren, dann werden diese Eigenschaften mit Werten gefüllt. Bei der Suche nach Dokumenten können Sie dann gezielt nach diesen Werten suchen.

Pro Dokumentart können Sie maximal folgende Eigenschaften zuordnen:

- 49 alphanumerische Eigenschaften
- 10 Datumseigenschaften
- 10 Geldeigenschaften
- 10 numerische Eigenschaften
- 10 Mehrfacheigenschaften

Anmerkung

Ändern Sie die Zuordnung der erweiterten Eigenschaften nachträglich, ist es erforderlich, dass sich die Anwender neu an das System anmelden.

Beim nachträglichen Ändern dieser Zuordnungen gehen keine Daten verloren, selbst wenn Sie zuvor schon eine Vielzahl von Dokumenten mit einer anderen Zuordnung archiviert haben. Wenn Sie anschließend die ursprüngliche Zuordnung wieder herstellen, werden Sie auch die "alten" Eigenschaften wieder in d.3 smart explorer sehen.



Im Fenster **erweiterte Eigenschaften** legen Sie fest, welche erweiterte Eigenschaften der Dokumentart zugeordnet werden.

1. Dazu wählen Sie Eigenschaften von der rechten Seite aus **Verfügbare erweiterte Eigenschaften**.
2. Fügen Sie der Dokumentart auf der linken Seite hinzu (< **Einzeln**, << **Alle**).

Wenn Sie eine erweiterte Eigenschaft entfernen wollen, geht dies wie folgt:

1. Wählen Sie es auf der linken Seite unter **Ausgewählte erweiterte Eigenschaften** aus.
2. Klicken Sie auf **Einzeln** > bzw. **Alle** > >.

Positionen der erweiterten Eigenschaften

Um die Anzeigereihenfolge der Spalten in den Ergebnissen in d.3 smart explorer bzw. der Felder in der Eigenschaftenmaske für die Recherche und Import zu beeinflussen, gehen Sie wie folgt vor:

1. Markieren Sie einen Feldeintrag in der Liste.
2. Verschieben Sie diesen wie gewünscht durch Klick auf die Schaltflächen.
3. Sie können die Position auch einfach über Drag & Drop verändern, indem Sie eine Zeile mit der linken Maustaste "greifen" und an die gewünschte Position ziehen.



Anmerkung

Beachten Sie, dass der Benutzer die Spaltenreihenfolge in den Ergebnissen in d.3 smart explorer durch manuelles Verschieben übersteuern kann. In d.3 smart explorer kann aber auch die Standardreihenfolge durch **Ansicht | Spaltenanordnung zurücksetzen** wiederhergestellt werden.

Eigenschaften Folgende Kontextmenüpunkte stehen Ihnen bei der Auswahl einer Eigenschaft zur Verfügung:

- Verwendung
- Modifizierbar Ja/Nein
- Ausblendbare Eigenschaft

Anmerkung

Es ergeben sich keine Probleme, wenn Sie die Anzeigepositionen nachträglich ändern. Es ist jedoch erforderlich, dass sich die Anwender neu an der d.3-Anwendung anmelden.

Warnung

Eine nachträgliche Änderung der Datenbankposition ist mit der d.3 Version 7 bei einem neu erstellten d.3 -Repository **nicht mehr** möglich.

Eigenschaften verwalten

Um eine Übersicht der Eigenschaften in den Dialogen **Übersicht der Dokumentarten**, **Erweiterte Eigenschaften** und **Positionen der erweiterten Eigenschaften** zu erhalten, öffnen Sie das Kontextmenü und wählen Sie die Option **Eigenschaften**.



In diesem Fenster erhalten Sie Informationen über die ausgewählte Eigenschaft.

Klicken Sie auf die Schaltflächen < **Zurück** oder **Weiter** >, um zu den übrigen Eigenschaften in der Liste zu navigieren.

Verwendung des Eigenschaftensfeldes

Um eine Übersicht der Dokumentarten und -klassen zu erhalten, welche das Eigenschaftensfeld nutzen, öffnen Sie das Kontextmenü und wählen Sie die Option **Verwendung** .



In diesem Fenster erhalten Sie Informationen über die Verwendung des ausgewählten Eigenschaftensfeldes.

Klicken Sie auf die Schaltflächen < **Zurück** oder **Weiter** >, um zu den übrigen Eigenschaften in der Liste zu navigieren.

Details für die Eigenschaft angeben

Um die Eigenschaften zu ändern, markieren Sie einen Eintrag in den Positionen der erweiterten Eigenschaften und klicken Sie auf den Button **Eigenschaften**.

Alternativ: Öffnen Sie den Dialog **Eigenschaften** durch Doppelklick.



Es öffnet sich der folgende Bearbeitungsdialog.



Datenbankposition

Ab der d.3 Version 7 ist eine nachträgliche Änderung der Datenbankposition nicht mehr vorgesehen. Bei einem Update auf die Version 7 wird allerdings berücksichtigt, dass dies in älteren Versionen noch möglich war.

Warnung

Die folgenden Erläuterungen betreffen NUR d.3- Repositorys, die mit einer Version älter als 7 erstellt wurden.

Alphanumerische Felder 1 bis 49 Diese Option verändert die Datenbankposition eines Eigenschaftensfeldes.

Wenn die Datenbankposition verändert wird, müssen Sie die Anforderungen des entsprechenden Eigenschaftensfeldes beachten:

- Datumsfelder 50 bis 59
- Mehrfacheigenschaftfelder 60 bis 69
- Geldfelder 70 bis 79
- numerische Felder von 80 bis 89.

Warnung

Ein nachträgliches Ändern der Datenbankposition kann über einen Server-Parameter untersagt werden! Somit sollten alle Positionen in einer gründlichen Planung erarbeitet und festgelegt werden!

Pflicht

Wenn die Option **Pflicht** auf "Ja" eingestellt ist, dann muss das Feld beim Import (manuell oder Hostimport) eines Dokuments gefüllt werden. Bleibt dieses Feld bei der Ablage von Dokumenten leer, wird eine Fehlermeldung erzeugt.

Warnung

Versteckte Felder sollten nie gleichzeitig auch Pflichtfelder sein.

Modifizierbar

Wenn diese Option auf "Ja" gesetzt ist (Standard), dann kann der Eigenschaftswert auch nach dem Import des Dokuments bearbeitet werden. Ansonsten wird die Änderung nicht durchgeführt.

Wird die Eigenschaft somit für eine Dokumentart als "geschützte" Eigenschaft definiert, kann nur eine berechnete Person den Wert der Eigenschaft ändern.

Titelfelder

Titelfelder dienen zur besseren Darstellung der Dokumenteigenschaften in d.3 smart explorer .



Wenn Sie z.B. ein Dokument in d.3 smart explorer öffnen und aus dem Kontextmenü **Verknüpfungen anzeigen** aufrufen, erhalten Sie normalerweise die Dokument-ID zusammen mit dem Namen der Dokumentart, z.B. "T000065565 Rechnung Eingang".

Wenn Sie sprechende bzw. aussagekräftige Bezeichner benutzen wollen, können Sie ein oder mehrere Titelfelder auswählen. Ab d.3 Version 7.2 können Sie auch verschiedene d.3-Systemfelder als Titelfelder festlegen.

Ausblendbar

Mit dieser Funktion können Sie Eigenschaften in einer Dokumentart ausblenden.

Über die Berechtigungssteuerung bei Dokumentklassen oder Profilen können Sie die versteckte Eigenschaft wieder anzeigen.

Diese Funktion finden Sie im Kontextmenü > **Ausblendbare Eigenschaft** bzw. über den Dialog **Eigenschaften**.

Wird eine Eigenschaft als ausblendbar markiert, erscheint das Symbol in der Übersicht durchsichtig (im Beispiel beim Eintrag "Orte"):



Auch in der Übersicht der Dokumentarten sehen Sie, dass eine Eigenschaft als ausblendbar markiert ist:



Wie Sie aus der Abbildung erkennen können, muss in der Spalte **Ausblendbar** ein "Ja" stehen, damit eine Eigenschaft ausgeblendet wird, im anderen Fall steht dort ein "Nein".

Anmerkung

Standardmäßig ist bei allen Eigenschaften der Wert **Ausblendbar** auf "Nein" gesetzt.

Warnung

Wenn Sie ein Pflichtfeld ausblenden, dann kann der Anwender dieses Pflichtfeld beim Import natürlich nicht mehr mit "Inhalt" füllen und erhält eine Fehlermeldung.

Blenden Sie deshalb nie Eigenschaften aus, die gleichzeitig Pflichtfelder sind, wenn Sie diese nicht durch Funktionen automatisch füllen.

Um versteckte Eigenschaften für einzelne Benutzer wieder einzublenden, müssen Sie die Berechtigung **Lesen versteckter Eigenschaften** und ggf. **Ändern versteckter Eigenschaften** erteilen.

Beachten Sie auch die Möglichkeit, einzelne Felder nur für d.3 import oder d.3 smart explorer auszublen- den.

Anmerkung

Versteckte Eigenschaften (ausblendbare) werden per Standard nicht an d.3 search wei- tergeleitet. Dieses muss man explizit mit dem Schalter `DSEARCH_ADD_HIDDEN_ATTR` einschalten.

Dieser Parameter muss manuell in die `d3addon.ini` des Repositorys gesetzt werden:

```
DSEARCH_ADD_HIDDEN_ATTR=1
```

Nach dieser Änderung müssen alle d.3- Prozesse (`d.3 hostimp`, `d.3 async` und `d.3 server`) für das betreffende Repository neu gestartet werden, damit die Einstellungen aktiv werden.

Erweitert

Unter **Erweitert** können Sie Einstellungen zur Konvertierung und Anzeige in d.3 import und der Ergebnis- liste sowie erweiterte Suche in d.3 smart explorer vornehmen.



Sie können pro Eigenschaft entscheiden, ob die Werte in Großbuchstaben, Kleinbuchstaben oder im Original angezeigt werden sollen.

Um kategorienspezifisch bestimmte Eigenschaftsfelder in d.3 import oder in d.3 smart explorer (Suche und Ergebnisliste), haben Sie in der Sektion **Sichtbar in** die Möglichkeit, die Anzeigoption zu bestimmen. Wenn Sie eine Option deaktivieren, wird die Eigenschaft im Feature nicht mehr angezeigt.

Warnung

Bitte beachten Sie unbedingt, dass diese Einstellung unter **Sichtbar in** nicht äquivalent zur globalen Steuerung über die Eigenschaft **Ausblendbar** in Verbindung mit dem Klas- sen-Berechtigungskonzept ist, sondern diese nur ergänzt.

Wenn Sie die Sichtbarkeit für eine Eigenschaft deaktivieren, kann ein Benutzer die Eigenschaft trotzdem wieder anzeigen. Die Eigenschaft wird in d.3 smart explorer unter **Ergebnisliste > Spalten anordnen** in **Verfügbare Spalten** weiterhin angezeigt.

Aktivieren Sie jedoch **Ausblendbar** für eine Eigenschaft, kann der Benutzer die Eigen- schaft nicht anzeigen. Die Einstellung **Ausblendbar** gilt sowohl für d.3 import als auch für d.3 smart explorer in der erweiterten Suche und Ergebnisliste.

Führen Sie eine Suche für die Dokumentart (Kategorie) durch. Die d.3-Benutzer können in d.3 smart explorer eine Eigenschaft, die Sie unter **Sichtbar in** deaktiviert haben, folgendermaßen wieder anzeigen:

1. Wählen Sie die Kontextaktion **Ergebnisliste** und dann **Spalten anordnen** aus.
2. Unter **Verfügbare Spalten** wählen Sie diejenigen Eigenschaften aus, die Sie in der Ergebnisliste anzeigen möchten.

Zusätzliche Angaben zu den erweiterten Eigenschaften

Sie können zusätzlich die Anzeige der Ergebnisliste für Dokumentarten vorbestimmen.

Ergebnisse standardmäßig nach dieser erweiterten Eigenschaft sortieren :

Diese Voreinstellung kann in d.3 smart explorer über die Benutzertätigkeit "überschrieben" werden.

Ergebnisse standardmäßig nach dieser erweiterten Eigenschaft gruppieren:

Auch diese Einstellung ist nur eine Voreinstellung und kann in d.3 smart explorer in jeder Ergebnisliste angepasst werden.

Dynamische Lebensdauer nach dieser erweiterten Eigenschaft berechnen: Über diese Einstellung lässt sich angeben, dass ein Dokument dieser Dokumentart anhand eines Datums in der erweiterten Eigenschaft (nur Datumsfelder) ein berechnetes Löschedatum erhält. Die Angabe bei "In Monaten" gibt dabei an, wann das Dokument abhängig vom Wert der erweiterten Eigenschaft gelöscht werden soll. Es sind neben der Auswahl auch freie Eingaben möglich. Negative Werte sowie "0" sind nicht erlaubt. Sollte in der erweiterten Eigenschaft ein Wert in der Vergangenheit eingegeben werden, wird das Dokument dennoch erst in einem Monat gelöscht.

Mehrsprachigkeit

Bei den mehrsprachigen Eigenschaften handelt es sich um die Bezeichnungen der Dokumentarten, der erweiterten Eigenschaften, der Gruppennamen sowie der Werte einer statischen Wertemenge. Diese Bezeichnungen sollten immer dann übersetzt werden, wenn Sie für Ihr d.3-Repository mehrere Sprachen unterstützen möchten.

Angenommen, Sie haben ein d.3- System, das als Basissprachen immer Deutsch und Englisch bereitstellt. Möchten Sie für Anwender weitere Sprachen bereitstellen, muss das Produkt d.3 national installiert werden, zum Beispiel für die Sprache Niederländisch.

Damit dann die Eigenschaftsbezeichnungen, Dokumentartnamen oder die Gruppennamen in z. B. Niederländisch dargestellt werden, erfassen Sie in diesem Bereich die Übersetzungen.



Derzeit werden in d.3 admin die Sprachen Deutsch und Englisch standardmäßig unterstützt.

Sprache hinzufügen

Um eine Sprache, z.B. Spanisch, hinzuzufügen, gehen Sie folgendermaßen vor:

1. Klicken Sie auf die Schaltfläche **Sprache hinzufügen**. Es öffnet sich ein neues Fenster.



2. Wählen Sie die entsprechende Sprache aus.
3. Klicken Sie auf den Schalter **Übernehmen**.

Zum Entfernen von Sprachen dient der Schalter **Sprache entfernen**. Die Sprachen Englisch und Deutsch können nicht entfernt werden. Für alle weiteren Sprachen wird ein Eintrag in der Datei `d3admin.ini` im Konfigurationsverzeichnis des Repositorys erstellt.



Warnung

Editieren Sie die `d3admin.ini` NICHT per Hand, da sie ab d.3 Version 8 vom Server geschrieben wird! Direkte Änderungen der Datei würden zu Inkonsistenzen von d.3 admin und des Transportsystems führen.

Übersetzen

Wenn Sie alle gewünschten Sprachen hinzugefügt haben, können Sie an die Übersetzung herangehen.

Dazu wählen Sie zwischen folgendem aus;

- Dokumentarten
- Repositoryfelder
- Tätigkeitsprofile

oder

- Wertemengen

Je nach Auswahl erhalten Sie dann ein Fenster, in dem die gewünschten Übersetzungen eingetragen werden können.

Um z.B. die Bezeichnung einer Dokumentart zu übersetzen, wählen Sie einfach in der Oberfläche die Schaltfläche **Dokumentarten** aus.



Anschließend können Sie jede Bezeichnung durch einen Doppelklick in der entsprechenden Zeile übersetzen.



Bei den Übersetzungen der Gruppen erkennen Sie die unterschiedlichen Gruppenarten wieder an den Symbolen.

 Gruppe ohne Postkorbverteilung

 Gruppe mit Postkorbverteilung

 Mitglieder einer Gruppe mit Lastverteilung

 Organisationseinheit



Anmerkung

Auf die gleiche Weise können die erweiterte Eigenschaften und die Gruppennamen übersetzt werden.

1. Wählen Sie hierzu die jeweiligen Seiten über die Schaltflächen aus.
2. Für den Rücksprung auf das Startfenster der mehrsprachigen Eigenschaften wählen Sie den Schalter **Information**.

Um Übersetzungen der statischen Wertemengen vorzunehmen, gehen Sie folgendermaßen vor:

1. Wählen Sie zunächst die Wertemenge aus.
2. Übersetzen dann in die ausgewählte Sprache.



Im Gegensatz zur Übersetzung von erweiterten Eigenschaften und Dokumentarten wird die Übersetzung erst mit Bestätigung des Schalters **Übernehmen** abgelegt.

Mit **Verwerfen** können alle noch nicht übernommenen Änderungen zurückgesetzt werden.

Bitte beachten Sie, dass in den Eigenschaftsfeldern, die auf eine Wertemenge greifen, immer die Kennung in der Datenbank abgelegt wird. Die Übersetzungen werden nur bei der Suche und der Darstellung ermittelt.

Sie können aber auch die in der statischen Wertemenge angegebenen IDs in die jeweilige Landessprache übersetzen (siehe [Manuell erstellte Wertemenge](#)).

Aktenbildung

Detaillierte Informationen zur Aktenbildung finden Sie im Handbuch zu d.3 admin folder scheme.

d.3 explorer folder browser admin

Zur Konfiguration von d.3 explorer folder browser schauen Sie bitte in das entsprechende Handbuch.

Automatische Ablage

Um die Ablage mehrerer Dokumente für die Anwender zu erleichtern, kann es ermöglicht werden, dass die abzulegenden Dokumente per Drag & Drop auf die "Zielakte" gezogen werden (d.3 smart start oder d.3 smart explorer). Alle Dokumente werden anschließend automatisch ohne weitere Benutzeraktion im d.3-Repository abgelegt. Über einen Fortschrittsbalken wird der Benutzer über den laufenden Import informiert.

Sind Pflichtfelder in der Ablage-Dokumentart definiert, die durch die Eigenschaften der Akte nicht gefüllt werden, öffnet sich d.3 import. Alle Änderungen, die hier getätigt werden, gelten anschließend für alle weiteren abzulegenden Dokumente.

Hat der Benutzer auf die hinterlegte Dokumentart keinen Schreibzugriff, erhält er eine entsprechende Fehlermeldung und kann die Eigenschaften entsprechend abändern, dass eine Ablage möglich ist. Diese Eigenschaften gelten anschließend für alle weiteren anzulegenden Dokumente.

Diese Funktionalität setzt ein Regelwerk voraus, das mit diesem Plugin definiert wird.

Dieses Regelwerk beschreibt in etwas folgendes:

Werden Dokumente auf die Akte einer hier gelisteten Aktenart gezogen, so importiere die Dokumente mit den Eigenschaften der Akte in die zugeordnete Dokumentart.

Regeln für eine automatische Ablage werden im folgenden Dialog-Baustein erfasst.



1. Klicken Sie **Neu**, um eine neue Zuordnung anzulegen.



2. In der oberen Auswahlliste wählen Sie die Akte aus, zu der Sie eine Verknüpfungsregel erstellen wollen.
3. In der unteren Auswahlliste wählen Sie die Dokumentart aus, die die Eigenschaften der Akte später übernehmen soll.



Haben Sie verschiedene Zuordnungen getroffen, können Sie diese über die entsprechenden Schaltflächen verwalten.

1. Markieren Sie hierzu die Zuordnung.
2. Betätigen Sie die nötige Schaltfläche.

Entfernen: Zuordnung löschen (ohne Nachfrage!)

Bearbeiten: Zuordnung einer anderen Dokumentart

Schließen: Anwendung beenden

Vergessen Sie nicht, die Konfiguration durch **OK** zu speichern.

1.4.3. Berechtigungen

Nachfolgend finden Sie die einzelnen Kapitel, die sich mit dem Thema Berechtigungen befassen.

Benutzer

Nachfolgend erhalten Sie nicht nur allgemeine Informationen zu den Benutzerberechtigungen, sondern auch, wie Sie Benutzer anlegen, suchen, konfigurieren und entfernen.

Benutzer allgemein

Jede Person, die Zugriff auf das d.3-Repository erhalten soll, muss ein eingetragener d.3-Benutzer sein. Die Benutzer "batchimp", "hostimp", "d3_server" und "d3_async" sind Systembenutzer und werden in der Benutzerübersicht von d.3 admin nicht angezeigt.

Anmerkung

In diesem Kapitel wird die Anlage und Verwaltung lokaler Benutzer im d.3 -Repository beschrieben.

Bei einer Anbindung über LDAP werden die Benutzer mit der ersten Anmeldung am d.3-Repository automatisch angelegt und in der Gesamtübersicht der Benutzer dargestellt.

Ein weiterer Systembenutzer ist der Benutzer "d3_admin". Es ist nicht notwendig, diesen Benutzer zu verwalten. Sie müssen diesem Benutzer keine Berechtigungsprofile, Klassen oder Gruppen zuordnen.

Warnung

Den Benutzernamen im d.3-Umfeld können Sie nicht ändern. Sie könnten lediglich den Benutzer kopieren und unter einem neuen Benutzernamen anlegen, dann alle Dokumente aus der Bearbeitung des alten Benutzernamens in die Bearbeitung des neuen Benutzers übertragen, verfahren Sie ebenso bei den Wiedervorlagen bzw. den Postkorb-Einträgen. Ist dies erfolgt und hat der alte Benutzername keine Dokumente mehr in seiner Bearbeitung und im Postkorb, können Sie den alten Benutzer löschen.



In der Übersicht können Sie erkennen, ob ein Benutzerkonto gesperrt oder deaktiviert ist. Über das Kontextmenü können Sie Benutzer wieder entsperren. Hierbei wird unterschieden, ob der Benutzer durch mehrmalige Falscheingabe des Kennworts gesperrt wurde, oder ob er über Policies (Gruppenzugehörigkeit) (siehe [d.3 policy manager](#)) gesperrt wurde. In diesem Fall muss die Entsperrung explizit bestätigt werden.

Warnung

Legen Sie keinen Benutzer namens "dummy" an, da dieser Benutzername intern von den Serverprozessen verwendet wird.

Filtern und Suchen von Benutzern

Mit dem Filter- und Suchmechanismus wird gerade in einer Umgebung mit vielen Benutzern die Verwaltung stark vereinfacht.



Im oberen Teil des Übersichtsfensters der Benutzerverwaltung steuern Sie die Filter bzw. Suchmechanismen.

Suchen nach: Zunächst legen Sie das Suchmuster fest, die Zeichen(folge) wird in allen Felder der Benutzerliste gesucht und die Auflistung unmittelbar entsprechend reduziert.

Suchen in: Die definierte Zeichenfolge kann anschließend in einer Spalte gesucht werden, die Sie hier vorgeben.

Anzahl: Gibt die Maximalzahl der aufzulistenden Benutzer an, die Anzahl kann über die Konfigurationsdatei in d.3 admin vordefiniert werden.

Suchen: Führt die Suche nach der Zeichenfolge aus und hebt der Reihe nach die Zeilen hervor, die das Suchmuster in der ausgewählten Spalte enthalten.

Zurücksetzen: Setzt alle Einträge auf ihren Standardwert zurück, die Suchfelder werden gelöscht, die Anzahl wird auf den Wert aus der Konfigurationsdatei (`ManyUserFindLimit`) gesetzt.

Konfiguration des Benutzerfilters

Das Verhalten des Benutzerfilters lässt sich in der Konfigurationsdatei von d.3 admin anpassen. Hierzu gibt es zwei Sektionen.

Beispiel der Datei d3admin.ini

```
[Performance]
ManyUserSupportEnabled=1
ManyUserLimit=500
ManyUserUpdateCount=500
ManyUserFindLimit=500
```

Die Parameter haben folgende Bedeutung bzw. Auswirkung:

Sektion **Performance**:

Parameter

- **ManyUserSupportEnabled**: Aktivieren des Benutzerfilters auch für Benutzerzuordnungen, z.B. bei Berechtigungsprofilen, Gruppen. Werte: 1 (default: ja), 0.
- **ManyUserLimit**: Anzahl der Benutzer, ab der die erweiterte Suche aktiv wird. Wert: 500.
- **ManyUserUpdateCount**: Anzahl der darzustellenden Benutzer, nach deren Bearbeitung die Anzeige aktualisiert wird. Wert: 500.
- **ManyUserFindLimit**: Maximalzahl Benutzer bei der Suche über Filter. Wert: 500.

Benutzer anlegen

Bei der Anlage eines neuen lokalen Benutzers müssen verschiedene Angaben erfasst werden. Im Folgenden wird die Dialogfolge bei der Anlage eines neuen Benutzers beschrieben.

Anmerkung

Wird eine Anbindung über einen [LDAP](#) -Server realisiert, werden die Benutzer mit der ersten Anmeldung im d.3- System angelegt und in der Übersicht dargestellt. Vor der d.3-Version 8.0 war es irrtümlicherweise möglich, einen über LDAP synchronisierten Benutzer zu bearbeiten, obwohl diese Änderungen mit der nächsten Synchronisierung verloren gingen. Mit Version 8.0 können solche Benutzer nicht mehr vollständig bearbeitet werden.

Vollständiger Name

Sie können an dieser Stelle den vollständigen Namen des d.3- Anwenders angeben.

Dieser Name wird in den d.3-Anwendungen häufig verwendet, u.a. wenn der Postkorbmechanismus von d.3 verwendet wird. Dieses Feld darf maximal 50 Zeichen enthalten. Dieser Name ist sprechender als der technische Name, zumal dieser auf zehn Stellen gekürzt wird.

Der vollständige Name erscheint in der Titelleiste von d.3 smart explorer , aber auch in verschiedenen Auswahllisten.

Abteilung

Zur Unterscheidung der Benutzer können Sie dem Anwender eine Abteilung zuordnen. Die Auswahlliste der Abteilungen wird dynamisch erweitert. D.h., wenn Sie den ersten Benutzer in d.3 anlegen, ist diese Auswahlliste noch leer. Beim Anlegen des n-ten Benutzers haben Sie dann alle unterschiedlichen Abteilungen zur Auswahl, denen die bisherigen Benutzer zugeordnet wurden. Die Abteilung darf maximal 50 Zeichen enthalten.

Organisation

Ein weiteres Unterscheidungsmerkmal ist die Organisation. Auch diese Auswahlliste wird dynamisch erweitert. Für dieses Feld stehen Ihnen maximal 50 Zeichen zur Verfügung.

Telefon

Für die Telefonnummer können maximal 40 Zeichen vergeben werden.

E-Mail

Die E-Mail-Adresse eines Anwenders darf maximal 100 Zeichen umfassen.

Wenn die SMTP Unterstützung für das d.3- Repository eingeschaltet ist, wird an diese E-Mail-Adresse eine vom d.3 -Server generierte E-Mail geschickt, Das bedeutet, dass mit dem Empfang eines Dokuments im d.3- Postkorb eines d.3- Benutzers automatisch eine E-Mail generiert wird. Somit bleibt das E-Mail-System für die Versendung von Informationen das führende System.

Wird der Abo-Service von d.3 genutzt, werden die Informationen über geänderte Dokumente ebenfalls an diese E-Mail-Adresse geschickt.

Benutzername

Geben Sie an dieser Stelle den d.3 Benutzernamen an. Dies ist der Name, mit dem sich der d.3- Anwender an das d.3- Repository anmeldet. Sie können maximal 30 Zeichen verwenden. Diese Zeichen sollten aus der Menge ["a".."z", "A".."Z", "0".."9", "_"] stammen. Alle anderen Zeichen sollten nicht im Benutzernamen vorkommen.

Unterstützt das d.3- Repository Unicode, sind alle Zeichen erlaubt. d.3 erzeugt einen maximal achtstelligen eindeutigen Namen, der Sonderzeichen nicht enthält.

Im Verzeichnis `bearbeit` im Dokumentenbaum des d.3- Repositories wird für jeden Benutzer ein Ordner mit dem technischen Namen (achtstellig) angelegt.

Warnung

Benutzer- und Gruppennamen sind in den ersten zehn Zeichen signifikant, d.h. jeder Benutzer- und jeder Gruppenname muss sich in den ersten zehn Zeichen von jedem anderen Benutzer- und Gruppennamen unterscheiden. Wurden für den Benutzernamen mehr als zehn Zeichen vergeben, wird der Name vom d.3 -System auf zehn Stellen gekürzt und eindeutig vergeben. Der Originalname wird als Alias für die Anmeldung nutzbar.

Beispiel: Der Benutzername ClausChef wird zu ClausCh1. Unter diesem Namen wird er in der Benutzerverwaltung eingetragen.

Es ist mit d.3 admin nicht möglich, eine Gruppe und einen Benutzer mit gleichem Namen anzulegen. Wenn Sie beim Anlegen eines Benutzers eine Meldung diesbezüglich erhalten, prüfen Sie bitte, ob mit dem Benutzernamen nicht bereits eine Gruppe bezeichnet wurde.

Kennwort/Kennwort Bestätigung

Bei der Anlage eines Benutzers ist immer zwingend ein Kennwort erforderlich. Auch bei der Änderung eines Kennwortes ist ein neues Kennwort zu vergeben. Dabei hängt das Format des neuen Kennwortes von einer Reihe von Konfigurationsparametern ab.

Der Parameter `PASSWORD_MIN_CHARS` gibt die minimale Länge eines Kennwortes an. Diesen Parameter können Sie über d.3 config verwalten.

Der Parameter `PASSWORD_EXTENDED_SYNTAX` gibt die Syntaxregeln für die Kennwörter an. Wenn Sie diesen Parameter auf "Ja" setzen, dann muss das Kennwort jeweils mindestens ein Zeichen aus drei der folgenden vier Zeichen-Gruppen enthalten: A-Z, a-z, 0-9, Sonderzeichen.

Die Option `PASSWORD_EXPIRE_DAYS` gibt die Default Lebensdauer eines Kennwortes in Tagen an, jedoch nur dann wenn die Option `PASSWORD_EXTENDED_SYNTAX` auf „Ja“ gesetzt ist.

Die Default Einstellung für diese Option ist "10957", das entspricht einem Zeitraum von 30 Jahren.

Beim Bearbeiten eines Benutzers wird Ihnen das Kennwort nicht angezeigt. Somit sind die beiden Felder Kennwort und Kennwort Bestätigung leer. Änderungen an den Einstellungen des Benutzers haben somit auch keinen Einfluss auf das Kennwort des Benutzers. Nur wenn Sie explizit ein neues Kennwort angeben, wird das alte Kennwort des Benutzers überschrieben.

Sie können maximal zwanzig Zeichen für das Kennwort eines Benutzers verwenden. Die Länge und Regeln zum Kennwort werden in der d.3-Konfiguration festgelegt.

Sollte das Kennwort den gültigen Regeln nicht genügen, erfolgt sofort eine entsprechende Meldung.

Erweiterte Eigenschaften - Benutzerrechte

Die erweiterten Eigenschaften (Policies) werden im Kapitel d.3 policy manager ausführlich beschrieben. Daher wird hier nur kurz auf die Konfiguration eingegangen.



Für jeden Benutzer können Rechte auf die aufgelisteten Eigenschaften vergeben werden. Die Zuweisung hat hierbei die gleiche Bedeutung wie bei der Rechtevergabe in den Berechtigungs-Profilen.

Zuweisung

ja: Recht erteilt

nein: Recht verweigert

<LEER>: Recht ignoriert

Sie vergeben die Berechtigungen entweder über Betätigung der entsprechenden Drucktaste oder einfach über einen Klick auf die Eigenschaft. Hierbei wird mit jedem Klick "durchgeschaltet".

Dem Benutzer wird die Anmeldung über d.3 login manager ermöglicht. Wird der Benutzer allerdings als Service-Benutzer eingerichtet, kann dieser sich NICHT mehr im Dialog anmelden (implizite Verweigerung).

Sie können sowohl Rechte auf Anwendungen, als auch auf Dokumente festlegen.



Optionale Felder

Die optionalen Felder bieten Ihnen die Möglichkeit, zusätzliche Informationen zu einem Benutzer abzulegen. Sie können in jedem dieser zehn optionalen Felder maximal 50 Zeichen eingeben. In älteren d.3-Systemen wurden die optionalen Felder oft zur Ablage der E-Mail-Adresse verwendet.

In einem optionalen Feld kann aber auch der Vorgesetzte eingetragen sein. Damit wird die Voraussetzung geschaffen, dass der Vorgesetzte z.B. bei Krankheit des Mitarbeiters den Abwesenheitsstatus verändern kann.

Auch d.3 abo service liest ein optionales Feld aus. Das optionale Feld 1 kann die Kennung für den Abo-Verwalter enthalten (siehe Dokumentation d.3 abo service).

Die Führungstexte sind nicht änderbar.



Gruppenzugehörigkeit

Jeder Anwender kann Mitglied in mehreren Gruppen sein. Gruppen fassen Mitarbeiter mit gleichen Aufgabengebieten und auch gleichen Berechtigungen zusammen. Mehr Informationen dazu finden Sie im Kapitel [Gruppen](#).

Warnung


Achten Sie bei der Zuordnung der Gruppen darauf, dass bei der Auswahl von mehr als zehn Gruppen das Erstellen der Zuordnungen unter Umständen mehrere Minuten dauern kann.



Dabei bedeuten die Symbole bei den verfügbaren Gruppen:

 Verteilung von Dokumenten an alle Mitglieder der Gruppe (Postkorb ohne Lastverteiler)

 Verteilung an ein Mitglied der Gruppe (Postkorb mit Lastverteiler)

 keine Verteilung, die Gruppe wird für Berechtigungszuordnungen genutzt

Berechtigungsprofile

Mit dem Berechtigungskonzept von d.3 besteht die Möglichkeit, die Berechtigung direkt per Berechtigungsprofil zu setzen.

Sie können an dieser Stelle dem Benutzer mehrere Berechtigungsprofile gleichzeitig zuordnen.



1. Wählen Sie aus dem rechten Fenster die gewünschten Berechtigungsprofile aus.
2. Fügen diese über den Schalter < dem linken Fenster zu.

Um ein Berechtigungsprofil zu entfernen, gehen Sie folgendermaßen vor:

1. Wählen Sie umgekehrt aus dem linken Fenster eines aus.
2. Betätigen die Schaltfläche > .

Der neue Benutzer wird angelegt, sobald Sie auf **OK** klicken.

Dokumentklassen zuweisen

Zusätzlich oder alternativ können Dokumentklassen einem Benutzer auch direkt zugeordnet werden. Damit ist es u.a. möglich, Rechte zu erweitern, z.B. für KeyUser, oder zu reduzieren.



Übersicht der Benutzerdaten

1. Rufen Sie die Benutzerübersicht über **Berechtigungen > Benutzer** auf.
2. Wählen Sie einen Benutzer aus.

3. Öffnen Sie über das Kontextmenü die **Eigenschaften** .

Sie erhalten eine Übersicht über die gewählten Werte des Benutzers.

Über die jeweilige Registerkarte (**Allgemein**, **Zuordnungen**, **Erweiterte Eigenschaften**) können Sie die konfigurierten Daten einsehen und auch bearbeiten.

Allgemein

Auf der Registerkarte **Allgemein** können Sie die **Benutzerdaten** einsehen und ändern, **optionale Felder** eintragen und eine **Abwesenheitsmeldung** hinterlegen.



Kennwort zurücksetzen

Über die Schaltfläche **Kennwort zurücksetzen** können Sie für den Benutzer ein neues Passwort für den d.3-Login vergeben.



LDAP-Bindung lösen

Die Schaltfläche **LDAP-Bindung lösen** ist verfügbar, wenn es sich um einen LDAP-Benutzer handelt und kann dann diese Bindung lösen.

Dokumente verschieben

Möchten Sie alle Dokumente oder Dokumentarten eines Benutzers übernehmen oder entfernen, nutzen Sie dazu den Dialog **Dokumente verschieben**, den Sie über die gleichnamige Schaltfläche erreichen.



In der linken Hälfte des Fensters sehen Sie die **Informationen zum Benutzer** und die **Dokumentarten** in denen der Benutzer Dokumente besitzt. Dazu ist die Anzahl der **nicht übergebenen Dokumente** pro Dokumentart in den einzelnen Kategorien sichtbar.

In der rechten Hälfte können Sie einen anderen **Benutzer oder eine Gruppe für die Übergabe der Dokumente** auswählen. Für den Benutzer oder die Gruppe werden ebenfalls die gleichen Informationen angezeigt. Zudem werden für Benutzer alle Dokumentarten angezeigt, für die er die erforderlichen Rechte besitzt. Für die Übernahme können Sie zwischen Dokumenten aus dem **Postkorb** oder Dokumente in **Bearbeitung** wählen. Die **zu übernehmenden Dokumente** werden dann darunter angezeigt.

Um Dokumente zu verschieben sind die folgenden Schritte notwendig:

1. Wählen Sie eine Kategorie aus, aus der die Dokumente verschoben werden sollen (Postkorb, Bearbeitung).
2. Haken Sie in der Liste die Dokumente der gewünschten Dokumentarten an, die verschoben werden sollen.
3. Klicken Sie auf **Übernehmen**, um die Dokumente zu verschieben oder
4. auf **Zurücksetzen**, um die Angaben zu verwerfen.

Anmerkung

Das Verschieben ist nicht unriskant und sollte mit Bedacht vorgenommen werden!

Bei Benutzern können Postkorbeinträge und Dokumente in Bearbeitung verschoben werden.

Das Entfernen der Einträge ist eine zusätzliche Möglichkeit bei Postkorbeinträgen und Tätigkeitsprofil-Links. Die Dokumente müssen vorher übergeben werden.

Zuordnungen

Auf der Registerkarte **Zuordnungen** können Sie die Zuordnungen des Benutzers in **Gruppen**, **Berechtigungsprofilen** und **Dokumentklassen** einsehen und ändern.



Erweiterte Eigenschaften

Die Registerkarte **Erweiterte Eigenschaften** zeigt die entsprechenden Rechte des Benutzers an, die Sie hier auch über die Schaltflächen **Zuweisen**, **Entziehen** und **Ignorieren** verwalten können, siehe [Erweiterte Eigenschaften - Benutzerrechte](#).



Benutzer entfernen

Um einen Benutzer zu entfernen, gehen Sie folgendermaßen vor:

1. Wählen Sie den entsprechenden Benutzer aus der **Übersicht der Benutzer** aus.
2. Klicken Sie dann auf die Schaltfläche **Entfernen**.
3. Bestätigen Sie die dann erscheinende Abfrage mit **Ja**.

Sollte der zu löschende Benutzer noch Dokumente zur Bearbeitung in seinem Postkorb haben, so erscheint ein weiterer Dialog, der Ihnen die Möglichkeit bietet, diese Dokumente einem anderen Benutzer zuzuweisen oder die Dokumente ebenfalls zu löschen.

Lizenzierung

Concurrent-User

Bei diesem Modell teilen sich mehrere Anwender eine Lizenz.

Führt ein Anwender eine Funktion im d.3-Repository aus, wird eine freie Lizenz vom ihm für 30 Minuten belegt. Wenn derselbe Anwender innerhalb der 30 Minuten weitere Aktionen ausführt, wird die Belegung jeweils wieder auf 30 Minuten festgesetzt. Werden innerhalb der 30 Minuten keine Aktionen ausgeführt, kann nach dem Zeitraum die Lizenz von einem anderen Mitarbeiter verwendet werden.

Die Anmeldung an d.3 smart explorer bzw. d.3 smart start belegt keine Lizenz.

Warnung

Ab der Version 8.0 von d.3 smart explorer wird die Lizenz beim Schließen der Anwendung nicht direkt freigegeben. Diese ist erst nach 30 Minuten verfügbar.

Named-User

Bei diesem Modell belegt jeder Anwender eine Lizenz. Für jeden Anwender, der mit dem System arbeiten soll, muss also eine Lizenz vorhanden sein. Das gilt auch für Teilzeitkräfte.

Allgemeines

Mit der d.3 Version 8.1 wurde der neue Lizenztyp `d.3ecm user S` eingeführt. Benutzer mit diesem Lizenztyp haben nur Lesezugriff auf die Dokumente im d.3-Repository und können an einem Workflow teilnehmen.

Der d.3-Server unterscheidet bei diesem Lizenztyp zwischen einem "nur lesenden" Benutzer (Readonly-User genannt) und einem "schreibenden" Benutzer (Full-User genannt).

Einlesen der Lizenzdaten

Beim Start der d.3-Prozesse werden folgende Lizenztypen aus der `liccheck.lic` ausgelesen:

- "d.3-named" für Full-User
- "d.3-named read only" für Readonly-User

Im d.3 Log wird das durch die Log-Einträge kenntlich gemacht:

- "Max. number of full users = ..." und
- "Max. number of readonly users =..."

Systemgruppe "\$ReadOnly\$"

Es wurde eine neue Systemgruppe "\$ReadOnly\$" eingeführt, über deren Mitgliedschaft ein Benutzer entweder eine Full-User-Lizenz (nicht Mitglied in dieser Gruppe) oder eine Readonly-User-Lizenz (Mitglied in dieser Gruppe) belegt wird.

- Die Gruppe wird nur dann angelegt, wenn auch wirklich Readonly-User Lizenzen in der Lizenzdatei ausgewiesen sind.
- Die Gruppe ist nicht änderbar bzw. löscherbar.
- Es können nur die Benutzer-Mitgliedschaften geändert werden.
- Service-Benutzer können kein Mitglied in dieser Gruppe sein. Es ist auch nicht möglich andere Gruppen als Mitglieder aufzunehmen. Diese Gruppe kann auch nicht Mitglied einer anderen Gruppe sein.

Readonly-User

Ein Benutzer, der eine Readonly-User Lizenz belegt, hat nur noch Leserechte auf Dokumente. Ein Dokumenten-Import, Änderungen an den Dokumenteigenschaften oder Verknüpfen von Dokumenten sind für diese Benutzer somit nicht möglich.

Phase nach Austausch der Lizenzdatei

Wenn nach dem Start der d.3-Prozesse erstmalig eine Named-User-Lizenz in der Lizenzdatei gefunden wird, beginnt der 30-tägige Einführungszeitraum. In dieser Phase können die Benutzer ohne Zeitverzug bzw. Sperrung der Lizenzen zwischen der Full-User-Lizenz und der Readonly-User-Lizenz hin und her wechseln.

Da alle d.3-Benutzer zunächst als Full-User eingeordnet werden, müssen nach der erstmaligen Installation einer Readonly-User-Lizenz die Benutzer, die als Readonly-User fungieren sollen, über d.3 admin in die Gruppe "\$ReadOnly\$" eingruppiert werden.

Belegung einer Lizenz

Eine Named User Lizenz wird erst dann belegt, wenn ein Benutzer sich aktiv am d.3-System anmeldet. Bei der Benutzeranlage findet keine Lizenzierung statt. Bei Benutzeränderungen, insbesondere die, bei denen eine Lizenzänderung stattfindet, wird nur noch die bisher belegte Lizenz beim Lizenzserver registriert und nach der Einführungszeit für 5 Tage gesperrt. Die neue Lizenz wird nicht registriert.

Tägliche Registrierung der Lizenzen

Der Async-Prozess durchläuft einmal täglich eine Routine, bei der Benutzer beim Lizenzserver registriert werden. Dabei gelten folgende Regeln:

- Deaktivierte Benutzer werden nicht registriert.
- Die Registrierung unterscheidet zwischen der Readonly- und Full-Lizenz.

Wechsel eines Benutzers auf eine Readonly-User-Lizenz

Innerhalb der 30-tägigen Einführungszeit der Named-User-Lizenz können Benutzer jederzeit ohne Sperrung einer Lizenz zu Readonly-User umfunktioniert werden.

Ansonsten gelten folgende Regeln:

- Die eingeschränkten Rechte für die Benutzer wirken sofort.
- Nach Ablauf der Einführungszeit wird die vorher belegte Full-Lizenz noch für 5 Tage gesperrt.
- Die Readonly-Lizenz wird bei der nächsten Anmeldung oder bei der nächsten täglichen Registrierung durch den Async Prozess belegt.

Wechsel eines Benutzers auf eine Full-User-Lizenz

Eine vorher belegte Readonly-Lizenz wird sofort freigegeben. Eine Full-Lizenz wird bei der nächsten Anmeldung oder bei der nächsten täglichen Registrierung durch den Async-Prozess belegt.

Service-Benutzer

Ein Service-Benutzer belegt keine Named-User Lizenz. Wird aus dem Service-Benutzer allerdings ein "normaler" Benutzer, belegt dieser eine Lizenz, die bei der nächsten Anmeldung oder durch die tägliche Registrierung durch den Async-Prozess aktiv wird.

Wenn ein Named-User zu einem Service-Benutzer, wird nach der Einführungszeit die jeweilige Lizenz (Full oder Readonly) für 5 Tage gesperrt.

Löschen von Benutzern

Nach dem Löschen eines Benutzers wird die bisher belegte Lizenz für 5 Tage gesperrt.

Deaktivieren von Benutzern

Bei Deaktivierung eines Benutzers wird die belegte Lizenz für 5 Tage gesperrt.

Umgang mit den Lizenzen bei einer LDAP-Anbindung

- Jeder neue LDAP-Benutzer belegt zunächst einmal keine Lizenz.
- Durch eine Zuweisung der Systemgruppe "\$ReadOnly\$" über die LDAP-Konfiguration belegt der Benutzer eine Read-Only-Lizenz.
- Die Lizenzwechsel verhalten sich genauso wie ohne eine LDAP-Anbindung: Bei einem Lizenzwechsel auf eine Lizenz mit einem geringeren Funktionsumfang wird die bisherige Lizenz für 5 Tage weiter belegt.
- Komfortfunktion: Verliert ein Benutzer alle Rechte, weil über die LDAP-Konfiguration keine Gruppen oder Berechtigungsprofile mehr zugewiesen sind, wird der Benutzer in d.3 deaktiviert. Somit wird auch die Lizenz dieses Benutzers nach 5 Tagen freigegeben.
- Komfortfunktion: Erhält ein deaktivierter Benutzer über die LDAP-Konfiguration wieder d.3-Zugriffsrechte, wird der Benutzer automatisch wieder aktiviert. Dieser Benutzer belegt eine Lizenz, wenn er in der Vergangenheit bereits angemeldet war.
- Wenn ein Benutzer im d.3-Repository noch existiert, aber nicht mehr im Directory Service, wird dieser in d.3 deaktiviert. Dabei wird auch die Lizenz freigegeben (nach 5-tägiger Sperre aufgrund eines Lizenzwechsels).

- Durch eine automatische Prüfung wird außerdem regelmäßig geprüft, ob ein Benutzer noch irgendwelche Rechte in d.3 hat oder nicht. Es reicht daher den Benutzern die d.3-Rechte zu entziehen und der Rest wird durch die automatische Lizenzfreigabe erledigt.

Warnung

Wenn die Meldung "The system group '\$disable\$' no longer exist! Please create a new group with the right 'Account is disabled' and assign it instead." nach einer Anmeldung eines Benutzers bzw. bei der Synchronisierung der LDAP-Benutzer durch den d.3 async Prozess erscheinen, ist folgendermaßen vorzugehen:

Auslöser der Meldung ist, dass die Systemgruppe "\$Deactivate\$" in der LDAP Konfiguration aufgenommen wurde, um Benutzer gezielt zu deaktivieren und gleichzeitig zu erreichen, dass diese keine Lizenz belegen. Da ab der Version 8.1 Hotfix 6 des d.3 Servers deaktivierte Benutzer keine Lizenz mehr belegen, wurde die Gruppe ersatzlos gestrichen. Stattdessen muss jetzt eine weitere Gruppe (am besten eine Gruppe mit der Option "Keine Verteilung in einen Gruppenpostkorb") angelegt werden, bei der die erweiterte Eigenschaft "Benutzer->d.3->Benutzerkonto->Konto ist deaktiviert" auf "Ja" gesetzt wird. In der LDAP-Konfiguration muss dann diese Gruppe anstatt der Gruppe "\$Deactivate\$" gesetzt werden. Wenn diese empfohlene Änderung nicht durchgeführt wird, ist trotz der Entfernung der Gruppe "\$Deactivate\$" die Funktionalität aber genauso wie vorher gegeben.

Gruppen

Nachfolgend erhalten Sie nicht nur allgemeine Informationen zu den Gruppenberechtigungen, sondern auch, wie Sie Gruppen anlegen und verwalten.

Gruppen allgemein

Gruppen haben im d.3-Repository die Aufgabe, Benutzer mit gleichen Aufgaben zusammenzuführen, um z.B. im Postkorbdialog oder im Berechtigungskonzept diese als Adressaten anzugeben.

Anmerkung

Die Bezeichnung einer Gruppe kann maximal 100 Zeichen enthalten.


Der Gruppenname muss sich in den ersten acht Zeichen von allen anderen Benutzer- und Gruppennamen unterscheiden.


Klassische Grenzen für Benutzergruppen und Berechtigungsprofile existieren nicht mehr. Halten Sie dennoch die Hauptspeicherauslastung und die Performance bei der Auswertung von Dokumentrechten im Blick. Insbesondere eine hohe Zahl an Berechtigungszuweisungen erhöht den Hauptspeicherbedarf und wirkt sich in Summe bei einer hohen Anzahl an Ergebnissen auf die Suchgeschwindigkeit aus.

Im Übersichtsbild der Gruppen werden alle verfügbaren Gruppen angezeigt. Über das jeweilige Icon wird zusätzlich der Typ der Gruppe angedeutet.

Markieren Sie eine Gruppe, werden die Mitglieder im rechten Fenster gelistet. Wie Sie sehen, können auch Gruppen wiederum Mitglieder sein (geschachtelte Gruppen).



 Verteilung von Dokumenten an alle Mitglieder der Gruppe (Postkorb ohne Lastverteiler), Gruppentyp nachträglich nicht mehr änderbar.

 Verteilung an ein Mitglied der Gruppe (Postkorb mit Lastverteiler), Gruppentyp nachträglich nicht mehr änderbar.

 K eine Verteilung, es werden (zunächst) nur Mitarbeiter gruppiert, der Gruppentyp lässt sich später aber noch ändern, wenn z.B. die Art der Postkorbverteilung geklärt ist.

Über die entsprechenden Icons oberhalb der Auflistung können Sie nach den Gruppentypen filtern.

Über die Schaltfläche **Entfernen** können Gruppen wieder gelöscht werden. Eine Mehrfachselektion ist in der Gruppenübersicht möglich, sodass in einem Arbeitsschritt mehrere Gruppen entfernt werden können. Die Anzeige der Mitglieder wird hierbei jedoch geleert und die Schaltflächen **Neu**, **Bearbeiten** und **Kopieren** werden deaktiviert.

Anmerkung

Sollten beim Löschen noch Dokumente einer Gruppe zugeordnet sein, wird Ihnen ein entsprechender Dialog angezeigt. Hier können die Dokumente verschoben werden.

Beim Löschen mehrerer Gruppen wird dieser Dialog für jede Gruppe einzeln angezeigt. Sollten die Dokumente nicht verschoben werden, können Sie durch eine erneute Abfrage den Vorgang für diese Gruppe abbrechen und mit der nächsten fortfahren.

Wird der Vorgang für eine Gruppe nicht abgebrochen, die Dokumente aber auch nicht verschoben, landen Sie in einer Art Endlosschleife.

Gruppe anlegen

Über den Button **Neu** auf der Seite Übersicht der d.3-Gruppen legen Sie eine neue Gruppe im d.3 Repository an.



Zunächst erfassen Sie die allgemeinen Informationen.

Art der Dokumentenverteilung:

Verteilung an alle Mitglieder (Gruppe)

Wird ein Dokument in den d.3 Postkorb versandt, kann dieses Dokument an alle Gruppenmitglieder gleichberechtigt versandt werden. Jedes Gruppenmitglied erhält einen Eintrag in seinem d.3 Postkorb.

Gruppendokumente sollten von einem Mitglied der Gruppe dann zur weiteren Bearbeitung angenommen werden (siehe d.3 smart explorer- Handbuch).

Verteilung an ein Mitglied (Tätigkeitsprofil)

Wird ein Dokument in den d.3 Postkorb versandt, kann das Dokument auch an ein Tätigkeitsprofil gesendet werden. Im Gegensatz zum Versand an eine Gruppe erhält nur (genau) ein Mitglied dieser Gruppe das Dokument als Aufgabe in seinen Postkorb. Für die Steuerung vergeben Sie später zusätzliche Werte für die Lastverteilung.

Keine Verteilung

Diese Gruppe erscheint nicht in den d.3-Anwendungen, z.B. Postkorb-Dialog. Sie gruppieren hiermit lediglich Mitarbeiter. Der Typ lässt sich nachträglich noch ändern. Ebenso können Sie diese Gruppe bei der Erstellung der Organisationsstruktur nutzen.

Gruppe anlegen - Erweiterte Eigenschaften



Weitere Informationen entnehmen Sie den Hinweisen zu den [erweiterten Eigenschaften](#) bei den Benutzerangaben bzw. dem Kapitel [d.3 policy manager](#).

Mitglieder

Mitglieder einer Gruppe können sowohl Benutzer als auch Gruppen sein.



Wählen Sie aus der Liste im rechten Fenster die Mitglieder der neu anzulegenden Gruppe aus. Eine Mehrfachmarkierung ist über die übliche Microsoft Windows-Funktionalität möglich. Sie können nur normale Postkorbgruppen zuordnen.

Berechtigungsprofile für Gruppen

Ab der d.3 Version 7 können einer Gruppe auch Berechtigungsprofile zugeordnet werden.



Nach der erfolgreichen Anlage der neuen Gruppe erscheint eine entsprechende Information.

Lastverteilung (Tätigkeitsprofil)

Wird eine Gruppe für die Verteilung an ein Mitglied (Tätigkeitsprofil) angelegt, erscheinen die ausgewählten Mitglieder dieser Gruppe in der Übersicht.

Für jedes Mitglied können im nächsten Dialog die Eckdaten zur Berücksichtigung bei der Aufgabenverteilung vergeben werden.

Sie können die Art der Lastverteilung bestimmen:

Lastverteilung

Gemäß der Gewichtung und der vorhandenen Postkorbeinträge wird der Versand in den Postkorb gesteuert. Hierzu werden die Parameter in der d.3 -Konfiguration ausgewertet.

Füllstandsverteilung

Der Postkorbversand wird gemäß der Schwellwerte gesteuert. Es werden solange Aufgaben zugeordnet, bis der Maximalwert erreicht ist. Die Gewichtung und die aktuelle Verteilung wird dabei berücksichtigt.

gleichmäßige Verteilung

Der Postkorbversand richtet sich nach der Zahl der Dokumente, die bisher über dieses Tätigkeitsprofil an den Benutzer versendet wurden und nicht an der aktuelle Zahl der Postkorbeinträge. Die Gewichtung wird hier mit eingerechnet.

Über einen Doppelklick konfigurieren Sie für das ausgewählte Mitglied die Gewichtung.

Für den ausgewählten Benutzer bzw. die Gruppe können Sie die Einstellungen zur Lastverteilung erfassen bzw. ändern.

Vertreter

Tragen Sie hier den Vertreter des Mitarbeiters ein. Dieser Vertreter kann über den Mechanismus der Vertreterregelung bei Abwesenheit seines Kollegen die Dokumente aus dessen Postkorb erhalten. Es ist auch möglich, eine Gruppe als Vertreter anzugeben, dann sind alle Mitglieder automatisch Vertreter des Mitarbeiters.

Gewichtung

Wollen Sie eine Umsetzung realisieren, die z.B. Teilzeit von Vollzeitkräften unterscheidet, sodass dies beim Versand von Dokumenten berücksichtigt wird, dann definieren Sie hier eine (selbstgewählte) Gewichtung. Erlaubt sind beliebige Werte.

Beispiel 1: "8" könnte einem Acht-Stunden Tag (Vollzeit) entsprechen, "4" einem Vier-Stunden Tag (Teilzeit)

Beispiel 2: Anzahl Aufgaben (auf dem "Schreibtisch") eines Mitarbeiters, bei Erreichen des Maximalwertes wird ihm zunächst keine weitere Aufgabe zugeordnet (relativ zu allen anderen Mitarbeitern dieser Gruppe).

Oberer Schwellenwert für Dokumentenverteilung

Für den Mechanismus der Füllstandsverteilung geben Sie hier eine frei wählbare Obergrenze an, die bestimmt, ab wann der Mitarbeiter keinen Postkorbeintrag mehr erhalten soll.

Beispiel: Tragen Sie die Anzahl Postkorbeinträge ein. Ob alle Einträge oder nur die ungelesenen gezählt werden, wird über den entsprechenden Parameter in der Vertreterregelung gesteuert.

Anmerkung

Wird für alle Benutzer der obere Schwellenwert erreicht, bestimmt ein intern ermittelter Koeffizient den nächsten Empfänger eines Dokuments. Es ist also gewährleistet, dass ein Dokument in jedem Fall einen Empfänger findet.

Unterer Schwellenwert für die Dokumentenverteilung

Für den Mechanismus der Füllstandsverteilung geben Sie hier eine frei wählbare Untergrenze an, ab der der Mitarbeiter wieder Postkorbeinträge erhalten soll.

Beispiel: Tragen Sie hier die Anzahl Postkorbeinträge ein, ab der ein Mitarbeiter wieder Dokumente erhalten soll.

Leiter des Tätigkeitsprofils

Wenn der Mitarbeiter diesen Bereich leitend steuern soll, aktivieren Sie die Checkbox. Dieser Mitarbeiter ist dann in der Lage, die Mitarbeiter seines Tätigkeitsbereichs abwesend bzw. auch anwesend zu melden. (siehe [Vertreterregelung](#)) Falls ihm das Recht zugeordnet wurde, kann dieser Mitarbeiter auch die Postkorbeinträge seiner Gruppenmitglieder einsehen.

Nimmt an der Dokumentenverteilung teil

Sie können Mitarbeiter aus der Verteilung der Dokumente herausnehmen, z.B. für den Vorgesetzten eine mögliche Einstellung.

Anmerkung

Wird für die Konfiguration der Lastverteilung eine Gruppe ausgewählt, lassen sich nur die Gewichtung bzw. Schwellenwerte eintragen.

Ferner kann die Gruppe aus der Dokumentverteilung herausgenommen werden.

Werden verschiedene Gewichtungen bzw. Schwellenwerte für Benutzer (direkt) und Gruppe zugeordnet, dann "gewinnen" immer die der Gruppe zugeordneten Werte. Die Einträge des Benutzers werden dann gar nicht erst interpretiert. Das gilt auch für die Teilnahme an der Dokumentenverteilung.

Gruppeneigenschaften

Die Gruppeneigenschaften erreichen Sie nach Aufruf der **Übersicht der Gruppen (Berechtigungen > Gruppen)**.

- Klicken Sie die gewünschte Gruppe an und dann auf die Schaltfläche **Bearbeiten**.
- Oder führen Sie einen Doppelklick auf den Namen der Gruppe aus.



Auf den Registerkarten **Allgemein**, **Erweiterte Eigenschaften**, **Mitglieder** und **Berechtigungsprofile** können Sie die Angaben, die beim [Anlegen der Gruppe](#) getätigt wurden, einsehen und zum Teil über **Bearbeiten** auch noch nachträglich ändern.

Die Schaltfläche **Dokumente verschieben** dient zum Verschieben von Dokumenten oder Postkorbeinträgen einer Gruppe zu einer anderen Gruppe oder Nutzer. Die Funktionsweise ähnelt der gleichnamigen Schaltfläche in der [Übersicht der Benutzerdaten](#).

Zusätzlich zu den Postkorbeinträgen und den Dokumenten in Bearbeitung können bei Gruppen Dokumente in Prüfung und Tätigkeitsprofil-Links verschoben werden.

Anmerkung

Im Gegensatz zu Benutzern werden bei Gruppen in der rechten Liste des Dialoges ausschließlich Dokumentarten angezeigt, zu der die Gruppe bereits Dokumente besitzt.



Dokumentklassen

Dokumentklassen allgemein

Dokumentklassen sind Bestandteil des Berechtigungskonzepts. Sie können unter Verwendung der Dokumentklassen Berechtigungen auf "Dokumente einer Dokumentart" setzen.

Ein einfaches Beispiel für eine Berechtigung auf "Dokumente einer Dokumentart" ist "alle Rechnungen mit einem Rechnungsbetrag kleiner als 10.000 €".

Dokumentklassen legen immer eine Teilmenge der möglichen Dokumente fest.



Es gibt grundsätzlich zwei Arten von Dokumentklassen. Die eine ist die dokumentartabhängige Klassenart (hier Bestellung (K)) und die andere ist die dokumentartunabhängige (oder auch dokumentartübergreifende) Klassenart.

Die Verwendung einer dokumentartabhängigen Dokumentklasse ist noch sehr verständlich, da diese Klassenart dazu dient, Dokumente einer bestimmten Dokumentart einzugrenzen, wie im obigen Beispiel eine Eingrenzung der Rechnungen auf diejenigen mit einem Rechnungsbetrag kleiner als 10.000 €.

Im Gegensatz dazu wird eine dokumentartunabhängige Dokumentklasse dazu verwendet, die "Dokumente aller relevanten Dokumentarten" im d.3-Repository einzuschränken. Diese Arten von Dokumentklassen verstehen sich nur als zusätzliches Kriterium, um den Zugriff einzuschränken. Sie können einem Benutzer nicht als einzige Dokumentklasse zugeordnet werden, da diese keinen Bezug zu einer Dokument bzw. Aktenart hat und in den Anwendungen diese somit nicht zur Auswahl stehen.

Angenommen, Sie möchten einem Benutzer Zugriff auf alle freigegebenen Dokumente erteilen. Dann reicht es nicht aus, eine **dokumentartunabhängige** Dokumentklasse anzulegen mit der Restriktion "Sta-

tus = Freigabe", und diese anschließend dem Benutzer zuzuordnen. Der Benutzer würde dann keine (konkreten) Dokument- bzw. Aktenarten in d.3 smart explorer bzw. d.3 import sehen.

Sie müssen vielmehr ein Berechtigungsprofil anlegen und alle für die Aufgaben des Mitarbeiters relevanten Standardklassen sowie die **dokumentartunabhängige Klasse** zuordnen.

Die Standardklassen werden automatisch vom d.3-Server beim Anlegen einer neuen Dokumentart oder Aktenart erzeugt. Erkennen können Sie Standardklassen an dem Namenszusatz "(K)" (bei englischen Repositories "C") und einem Klassenkürzel mit dem Präfix "CLAS_".

Dann vergeben Sie die Rechte NUR für die **dokumentartunabhängige Klasse**. Abschließend können Sie das Berechtigungsprofil z.B. mit der Bezeichnung "ALLE DOKUMENTE" benennen und fertig stellen.

Dieses Berechtigungsprofil wird dem Benutzer zugeordnet aber erst nach erneuter Anmeldung wirksam. Der Benutzer wird anschließend nur freigegebene Dokumente in den Ergebnissen einer Suche erhalten.

Wollen Sie eine Berechtigung umgekehrt realisieren, also in unserem Beispiel einem Benutzer alle Dokumente bereitstellen, die NICHT freigegeben sind, beachten Sie folgende Hinweise:

Sie verbieten für die dokumentartunabhängige Klasse das Leserecht ("NEIN" bzw. "Recht verweigert"), müssen aber für die Standardklassen das Leserecht erteilen ("JA" bzw. "Recht erteilt"). Betrachten Sie zum Verständnis die dokumentartunabhängige Klasse einfach als Schablone mit schwarzen Bereichen und die anderen Klassen als Schablonen mit "Löchern". Alle Schablonen werden übereinandergelegt. Durchschauen kann man nur durch die "Löcher", die schwarzen Bereiche sind immer undurchsichtig.

Warnung

Die direkte Benutzer - Klassenzuordnung sollte bei der Nutzung von Berechtigungsprofilen nur noch verwendet werden, wenn man z.B. Rechte explizit verweigern will.

Dokumentklasse hinzufügen

1. Um eine neue Dokumentklasse hinzuzufügen, betätigen Sie den **Neu** in der Übersicht.
2. Zunächst wählen Sie die Dokumentart aus, zu der Sie Restriktionen definieren wollen, z.B. "Bestellung".



Definition der Restriktionen

Sobald Sie eine Dokumentart auswählen, auf die sich die Dokumentklasse beziehen soll, werden Ihnen die Eigenschaften zu dieser Dokumentart angezeigt. Sie können dann in den einzelnen Feldern Ihre Restriktionen definieren.

In Abhängigkeit des Datentyps eines Feldes können Sie auch mit Sonderzeichen und Makros arbeiten.



Unter **Identifikation** geben Sie der neuen Dokumentklasse eine beschreibende Bezeichnung, aus der ein Teil der Einschränkungen hervorgeht.

Der Name einer Dokumentklasse hat ausschließlich informativen Charakter. Sie können für den Namen maximal 255 Zeichen verwenden. Somit besteht die Möglichkeit, Namen zu vergeben, die leicht verständlich sind. Ein sinnvoller Name ist zum Beispiel "Rechnungen mit einem Rechnungsbetrag unter 10.000 €".

Zusätzlich müssen Sie einen maximal zehnstelligen eindeutigen technischen Namen (Kürzel) vergeben. Dieser Name wird in der Hook-Programmierung genutzt. Das Kürzel ist case-sensitiv, d.h. Groß-/Kleinschreibung wird streng unterschieden.

Alle Standarddokumentklassen haben als Kürzel das Präfix `CLAS_`. Dieses Präfix ist ausschließlich für die Standarddokumentklassen reserviert. Sie können keine Dokumentklasse mit einem solchen Präfix anlegen.

Über die Option **Aufnahme der Filter als Suchbedingung** kann eingestellt werden, dass die Restriktionen der Dokumentklasse in das SELECT-Statement bei der Dokumentensuche integriert werden können.

Dabei ist folgendes zu beachten:

- Es werden nur die Dokumentklassen berücksichtigt, die dem Benutzer über Berechtigungsprofile oder direkt Dokumentklassen-Zuordnungen zugewiesen sind.
- Wird eine Suche über genau eine Dokumentart durchgeführt, werden die Restriktionen der auf Basis dieser Dokumentart erstellten Dokumentklassen herangezogen.
- Wird eine Suche über keine oder mehrere Dokumentarten durchgeführt, werden nur Dokumentart unabhängige Dokumentklassen herangezogen.
- Es können immer nur die Restriktionen einer Dokumentklasse in die Suchbedingungen integriert werden, da die Dokumentklassen-Auswertung immer per ODER-Verknüpfung ausgeführt wird und sich dies nicht, gerade, wenn mehrere Restriktionen pro Dokumentklasse gesetzt sind, in SQL-Kommandos umgesetzt werden kann. Das bedeutet: Sind dem Benutzer mehrere Dokumentklassen mit dieser Option zugewiesen, und diese Dokumentklassen beziehen sich auf dieselbe Dokumentart, wird gar keine Dokumentklasse berücksichtigt.
- Bei der Integration der Dokumentklassen-Restriktionen werden nur die Eigenschaften in den Suchkriterien gesetzt, die nicht schon durch den Anwender gesetzt sind.
- Folgende Makros werden unterstützt: `@D3USER`, `@D3GROUP`, `@D3USER_REALNAME`, `@D3USER_LONG`, `@D3USER_EMAIL`, `@D3USER_LDAPDN`, `@D3USER_OPTFIELD`, `@D3SET`

Beispiel:

Gegeben ist eine Dokumentklasse der Dokumentart "E-Mail" (Dokumentartkürzel EMAIL) mit der Restriktion `"@D3USER_EMAIL"` auf dem Eigenschaftsfeld "Empfänger" (DB-Position 1).

Der Benutzer "user1" hat als E-Mail Adresse folgenden Eintrag: user1@firma.de

Bei der Dokumentensuche in der Dokumentart "E-Mail" ohne weitere Suchkriterien wird das folgende SQL-Kommando generiert (verkürzt dargestellt):

```
SELECT * FROM firmen_spezifisch WHERE kue_dokuart = 'EMAIL' AND dok_dat_feld_1 = 'user1@firma.de'
```

Restriktionen

Eine Dokumentart kann mit einer Restriktion eingeschränkt werden, ähnlich wie bei einer Suche im d.3 . Somit können auch die üblichen Wildcards in der Restriktion verwendet werden. Die möglichen Wildcards sind wiederum vom Datentyp des Feldes abhängig. Beachten Sie die erweiterten Möglichkeiten bei alphanumerischen Sonderzeichen.

Alphanumerische Felder

Bei Textfeldern können Sie Platzhalter nutzen, die in der d.3-Konfiguration definiert sind. Standardmäßig sind das "%" (Prozent) und "_" (Unterstrich). Dabei ist das Prozentzeichen ein Platzhalter für eine unbekannte Anzahl von Zeichen und der Unterstrich ist ein Platzhalter für genau ein Zeichen.

Angenommen, in Ihrem d.3- Repository existiert eine Dokumentart mit der Bezeichnung "Lieferscheine". Diese Dokumentart enthält ein Feld mit der Bezeichnung "Lieferant". Dieses alphanumerische Feld soll die Namen der Lieferanten enthalten. Um einem Benutzer Zugriff auf die Lieferscheine des Lieferanten "d.velop AG" zu erteilen, müssen Sie für dieses Feld die Restriktion "d.velop AG" angeben.

Der Nachteil dieser exakten Angabe liegt aber nun darin, dass Dokumente, welche als Lieferant die Angabe "Fa. d.velop AG" tragen, nicht gefunden werden. An dieser Stelle wäre es besser, die Restriktion "%d.velop AG" anzugeben. Dadurch werden beide Schreibweisen gefunden. Wenn bei einigen Dokumenten für das Feld Lieferant der Wert "Firma d.velop" angegeben wurde, dann würde dieses Feld wiederum nicht der Restriktion entsprechen. Diesen Umstand kann man durch die Restriktion "%d.velop%" umgehen. Ein letztes Problem könnte der "Punkt" in dem Firmennamen darstellen. Dokumente bei denen als Lieferant "Firma d-velop AG" (mit Bindestrich) angegeben wurde, werden immer noch nicht gefunden. Abhilfe schafft an dieser Stelle der Platzhalter "Unterstrich". Somit lautet die endgültige Restriktion für das Feld Lieferant der Dokumentart Lieferscheine "%d_velop%". Diesen Wert müssten Sie bei der Definition der Dokumentklasse angeben.

Anmerkung

Als Platzhalter können statt der Zeichen "%" und "_" auch die gleichbedeutenden Platzhalter "*" und "?" verwendet werden. Ab der d.3 Version 6.2 können weitere Sonderzeichen für die alphanumerische Suche definiert werden.

Diese individuell definierten Sonderzeichen können sowohl in der Recherche als auch bei der Dokumentklassen-Definition genutzt werden.

Für die Dokumentklassen-Definition gilt allerdings die Einschränkung, dass die Sonderzeichen nicht kombinierbar sind!

Ausnahme: Kombinationen mit "*", "%", "_" und "?".

Datumsfelder

Bei Datumsfeldern können Sie das Minuszeichen ("-") verwenden. Dadurch lassen sich die Bereichsangaben "von - bis", "seit -" und "- bis" definieren.

Bereichsangaben	Restriktionen
von - bis	01.01.1997 - 31.12.2001
seit	01.01.1997 -
bis	- 31.12.1999
{-m}-{+n}	Beispiel: {-28}-{+28} Restriktion für den Zeitraum von (vor 4 Wochen) bis (in 4 Wochen)

Angenommen, in Ihrem d.3 -Repository existiert eine Dokumentart mit der Bezeichnung "Rechnung". Diese Dokumentart besitzt eine Eigenschaft "Datum", in welchem das Rechnungsdatum abgelegt ist.

Wenn Sie einem Benutzer den Zugriff auf die Rechnungen bis zum Datum "31.12.2000" erteilen möchten, müssen Sie beim Erstellen dieser Dokumentklasse die Dokumentart "Rechnung" auswählen.

Weiterhin muss für das Feld **Datum** dieser Dokumentart die Restriktion "-31.12.2000" angegeben werden. Anschließend muss dem Benutzer diese Dokumentklasse zugeordnet werden.

Numerische Felder

Bei numerischen Feldern können Sie den Bindestrich ("-") als Bereichszeichen angeben.

Ein Beispiel hierfür ist der "Rechnungsbetrag". Wenn Sie beispielsweise eine Dokumentklasse für die Rechnungen mit einem Rechnungsbetrag kleiner als 10.000 € erstellen möchten, dann müssen Sie für das Feld "Rechnungsbetrag" die Restriktion "-10.000" angeben. Um Rechnungen mit einem Rechnungsbetrag größer als 10.000 € anzugeben, müssen Sie die Restriktion "10.000-" angeben.

Um einen negativen Wert zu definieren, müssen Sie das Zeichen "\" (Backslash) dem Bindestrich ("-") voranstellen.

Feld **Abweichung in mm (länger / kürzer)** bei der Produktion eines Guts von der Standardnorm.

- 100-
Alle Abweichungen, bei denen das produzierte Gut länger als 100 mm gegenüber dem Norm-Gut ist.
- -10
Alle Abweichungen, bei denen das produzierte Gut bis zu 10 mm kürzer als das Norm-Gut ist.
- \-10
Suche nach Gütern, die genau 10 mm kürzer als das Norm-Gut sind.
- 10-100
Suche nach Gütern, die mindestens 10 mm länger und höchstens 100 mm länger sind als das Norm-Gut.

Wertemengen-Restriktionen

Bei der Definition der Dokumentklassen werden bei allen Eigenschaften mit einer zugeordneten Wertemenge die Werte dieser Wertemenge nach Betätigen der Combobox rechts zur Auswahl angeboten.



Die hinterlegte Wertemenge wird angezeigt.

Technische Felder

Im oberen Teil der Übersicht stehen Ihnen die technischen Eigenschaften für Restriktionen zur Verfügung. Diese Felder sind unabhängig von der Dokumentart.

Dokumenten-Nummer: Dieses alphanumerische Feld steht für die **Zeichnungs-Nummer** (`zeich_nr`).

Dokument-ID: Die Dokument-ID ist ein eindeutiges Kennzeichen für ein Dokument im d.3 -Repository. Bei diesem Feld handelt es sich um ein alphanumerisches Feld.

Erstellt am: In diesem Feld können Sie bei einer Restriktion das Datum angeben, wann ein Dokument erstellt wurde. Es handelt sich bei diesem Feld um ein Datumsfeld und somit müssen die Restriktionen, wie zuvor beschrieben, angegeben werden.

Frei/Gesperrt: Diese Eigenschaft bezieht sich auf freigegebene Dokumente. Bei der Definition einer Dokumentklasse können Sie bei diesem Feld entweder "Freigegeben", "Gesperrt" oder nichts angeben.

Die Wertemenge mit "Freigegeben" und "Gesperrt" wird angeboten, wenn man auf die Combobox rechts außen klickt. Die Combobox erscheint auch, wenn man doppelt in das Restriktionsfeld klickt.

Angenommen, ein Anwender soll Zugriff auf alle freigegebenen Dokumente der Dokumentart "Dokumentation" erhalten, dann würde es ausreichen, für den Status den Wert "Freigabe" als Restriktion anzugeben. Somit hat der Anwender Zugriff auf alle freigegebenen Dokumente dieser Dokumentart, auch auf die gesperrten Dokumente. Damit der Anwender keinen Zugriff auf die gesperrten Dokumente erhält, müssen Sie für das Feld **Frei/Gesperrt** die Restriktion "Freigegeben" auswählen.

Anmerkung

Das Sperren eines freigegebenen Dokuments ist sinnvoll, wenn es sich als inhaltlich fehlerhaft herausstellen sollte, seine Gültigkeit verliert oder seine Gültigkeit erst zukünftig erlangt.

Plan/Geprüft: Dieses Feld bezieht sich auf den ersten Prüfschritt. Sie können für dieses Feld entweder "Ja", "Nein" oder nichts auswählen. Wenn Sie an dieser Stelle "Ja" auswählen, muss das entsprechende Dokument geprüft worden sein. Die Wertemenge mit "Ja" und "Nein" wird angeboten, wenn man auf die Combobox rechts außen klickt. Die Combobox erscheint auch, wenn man doppelt in das Restriktionsfeld klickt.

Status: Dieses Feld steht für den Status eines Dokumentes. Mögliche Werte sind "Bearbeitung", "Prüfung", "Freigabe", "Archiv" und nichts.

Anmerkung

Bei der Auswertung der Berechtigung wird immer auf den aktuellsten Status geprüft. D.h., tragen Sie hier als Restriktion "Freigabe" ein, werden nur die Dokumente bereit gestellt, die als aktuellsten Status den Status "Freigabe" haben. Alle Dokumente, die zusätzlich in "Bearbeitung" bzw. "Prüfung" sind, werden nicht berücksichtigt.

Um eine Restriktion "alle freigegebenen Dokumente" zu realisieren, lassen Sie diese Eigenschaft frei und tragen dafür bei **Frei/Gesperrt** "Freigegeben" ein.

Bearbeiter: Dieses Feld bezieht sich auf Dokumente im Status "Bearbeitung". Sie können für dieses Feld entweder einen Benutzernamen oder einen Gruppennamen aus der Auswahlliste wählen.

Denkbar sind an dieser Stelle auch die unten aufgeführten Makros, insbesondere die Makros @D3USER und @D3GROUP (siehe auch Kapitel [Makros](#)).

Diese Eigenschaft ist ein alphanumerisches Feld.

Ungeschützter Webzugriff: Es besteht die Möglichkeit, Dokumente für das Web zu veröffentlichen. Wenn ein Dokument für das Web veröffentlicht wurde, wird im d.3 smart explorer eine kleine Weltkugel angezeigt. Um einem Benutzer ausschließlich den Zugriff auf diese für das Web veröffentlichten Dokumente zu erteilen, müssen Sie aus der Auswahlliste den Wert **Web Veröffentlicht** auswählen. Um dem Anwender explizit den Zugriff auf die nicht veröffentlichten Dokumente zu erteilen, wählen Sie bitte **NICHT Web Veröffentlicht** aus. Die dritte Möglichkeit besteht in der Auswahl des Leereintrages. Dadurch hat die Eigenschaft **Web Veröffentlicht** keine Auswirkung auf die Bestimmung der Berechtigung.

Anmerkung

Ab der d.3 Version 6.3 heißt diese Eigenschaft **Ungeschützter Webzugriff**. Es stellt allerdings eine obsoleete Funktion bereit, da diese auf CGI-Skripten beruht und zukünftig der d.3 Web Publisher nicht mehr ausgeliefert wird.

Besitzer: In diesem Feld kann über den Besitzer eines Dokuments eine Restriktion erstellt werden. Der Besitzer ist die Benutzerkennung, unter der das Dokument importiert wurde.

Client-Kennung: Es besteht die Möglichkeit, eine Client-Kennung als Restriktion zu hinterlegen. Jede Anwendung wird mit einer internen Kennung versehen. Das ist ein dreistelliger Code, z.B. 200 bei d.3 smart explorer . So ist auch für zukünftige Zwecke gewährleistet, dass der Aufruf neuer oder auch externer Anwendungen über das Berechtigungskonzept erlaubt bzw. verboten werden kann. Diese Einstellungen werden momentan primär für kundenspezifische Lösungen verwendet. Beispielsweise werden d.3 smart explorer , d.3 import und d.3 view mit den Kennungen 200, 220 und 100 verwendet. Diese Kennungen werden auch bei jedem API-Call an den d.3 -Server übermittelt und können in d.3 logviewer eingesehen werden:



Dateierweiterung: Eine Restriktion über die Dateierweiterung ist ab der d.3 Version 6.3 verfügbar. Somit ist es möglich, Anwendern nur bestimmte Dateitypen zur Verfügung zu stellen.

Makros

Folgende Makros können Sie bei der Definition der Restriktionen verwenden:

@D3USER

Wenn Sie für ein Feld einer Dokumentklasse das Makro @D3USER als Restriktion angeben, wird beim Bestimmen der Berechtigungen für einen Benutzer dieses Makro durch den aktuellen d.3-Benutzernamen (den technischen Namen) ersetzt.

Angenommen, in Ihrem Repository existiert eine Dokumentart "E-Mail". Diese Dokumentart enthält ein Feld mit der Bezeichnung "Benutzer". Beim Importieren von Dokumenten wird dieses Feld automatisch mit dem d.3-Benutzernamen gefüllt. Alle Benutzer des d.3-Repository erhalten Zugriff auf diese Dokumentart. Der Zugriff auf diese Dokumentart wird über eine Dokumentklasse gesteuert. Diese Dokumentklasse enthält für das Feld "Benutzer" das Makro @D3USER als Restriktion. Wenn ein Anwender dann mittels d.3 smart explorer im d.3-Repository nach E-Mails sucht, sieht er nur diejenigen, die seinen d.3-Benutzernamen im Feld "Benutzer" enthalten.

@D3GROUP

Bei der Verwendung des Makros @D3GROUP wird zur Laufzeit geprüft, ob die entsprechende Eigenschaft einen d.3 -Gruppennamen enthält, in welcher der Anwender Mitglied ist. Wenn dies der Fall ist, erhält der Anwender Zugriff auf die Dokumente.

@D3USER_OPTFIELD_XX

Beim Ermitteln der Klassenzugehörigkeit eines Dokumentes kann man das Makro @D3USER_OPTFIELD_xx in einem Eigenschaftsfeld verwenden. Dies bewirkt, dass gegen das benutzerspezifische optionale Feld mit der Nummer xx (1 bis 10) des aktiven Benutzers aus der Benutzerverwaltung geprüft wird.

Wenn man beispielsweise für den Benutzer "Otto" im fünften benutzerspezifischen Feld in d.3 admin "23" angibt und dann eine Klasse erstellt, in der z.B. das Eigenschaftsfeld "Abteilungsnummer" mit @D3USER_OPTFIELD_05 besetzt wird, dann wird zur Laufzeit der Eigenschaftswert mit dem des 5. optionalen Feldes verglichen (also mit 23). Bei Übereinstimmung hat der Benutzer "Otto" Zugriff auf dieses Dokument.

@D3USER_LDAPDN

Das Dokumentklasse-Makro @D3USER_LDAPDN wird bei der Rechteermittlung auf Dokumente ersetzt durch den vollständigen Namen (Distinguished Name im LDAP) des d.3-Benutzers, der bei aktiviertem LDAP-Support zugewiesen ist.

Bei Benutzung von Microsoft Windows Active Directory Services (ADS) als LDAP-Server ist dies die ADS-GUID des entsprechenden Microsoft Windows-Benutzers.

Anmerkung

Bei der Auswertung des Makros wird eine bei einer ADS-GUID vorangestellte Zeichenkette "GUID=" entfernt.

@D3HOOK

Anmerkung

Mit der d.3 Version 6.2 wurde mit der Möglichkeit, Berechtigungsmengen zu definieren und zu verwalten eine Basis geschaffen, ohne den Aufruf von vielen kleinen Hook-Funktionen auszukommen. Bevor Sie eine Lösung mit Hook-Funktionen in Erwägung ziehen, prüfen Sie bitte immer, ob eine Berechtigungsmenge nicht bereits die Lösung bringt (siehe Kapitel [d.3 restriction set manager](#)).

Die Verwendung des Makros @D3HOOK ermöglicht die Erstellung einer Hook-Funktion zum Bestimmen der Berechtigung. Als Parameter erhält das Makro den Namen der Hook-Funktion, beispielsweise @D3HOOK (procedure). Beim Bestimmen der Berechtigung, also dem Aufruf dieser Hook-Funktion, wird der Funktion der Eigenschaftswert des Dokumentes übergeben. Wenn diese Hook-Funktion eine "1" (TRUE) zurückgibt, dann ist die Bedingung (Berechtigung) erfüllt. Liefert dieser Hook eine "0" (FALSE) zurück, dann ist die Bedingung nicht erfüllt und der Benutzer erhält keinen Zugriff auf das Dokument.

Anmerkung

Vergleich einer Lösung mit Hook-Funktion und Berechtigungsmenge:

Wie bereits oben bei den "Numerischen Feldern" beschrieben wurde, können Sie für numerische Felder nur die Restriktionen "VON-BIS", "-BIS" und "VON-" verwenden. Eine Prüfung auf mehrere Bereiche ist damit nicht möglich.

Angenommen, Sie möchten ein numerisches Feld überprüfen. Der Benutzer soll Zugriff auf das Dokument erhalten, wenn dieses numerische Feld, in diesem Beispiel die "Liefer_Nr", zwischen "1 und 10", genau 15 oder größer als 100 ist.

Lösung der Problemstellung mit einer Hook-Funktion

Eine Hook-Funktion für diese Aufgabe könnte wie folgt aussehen:

```
proc liefer_nr_klasse (liefer_nr)
{
  if ( liefer_nr >= 1 && liefer_nr <= 10 \
      || liefer_nr == 15 \
      || liefer_nr > 100 \
      )
    return (1)
  else
    return (0)
}
```

Das Makro müsste folgendermaßen angegeben werden: @D3HOOK(liefer_nr_klasse).

Lösung der Problemstellung mit einer Menge für numerische Werte, Name: lief_nr

1-10

15

100-

Lösung der Problemstellung mit einer Menge für alphanumerische Werte: lief_nr

1~10

15

>100

Voraussetzung in diesem Beispiel: Definition der Sonderzeichen für alphanumerische Suche (~ und >)

Aufruf der Menge in der Dokumentklassendefinition: @D3SET(lief_nr)

Anmerkung

Bevor Sie eigene Hook-Funktionen erstellen, sollten Sie unbedingt an einer d.3 hook -Schulung bei der d.velop AG teilnehmen.

@D3SET

Mit diesem Makro können Sie eine definierte Berechtigungsmenge einer Eigenschaft als Restriktion zuordnen. Über den Button ... können Sie auch aus den definierten Mengen auswählen. Achten Sie dabei unbedingt auf die Verträglichkeit der Datentypen.

Anschließend wird über das Makro ein Verweis auf die Restriktionsmenge erstellt. Wie Restriktionsmengen erstellt werden, erfahren Sie im Kapitel [d.3 restriction set manager](#).

@D3REGEXPR

Mit diesem Makro können reguläre Ausdrücke für die Restriktionen genutzt werden. Die mögliche Syntax hängt von der Wahl des "Interpreters" der regulären Ausdrücke ab (siehe hierzu die Erläuterungen zum Parameter `REGEX_SYNTAX`).

Damit lassen sich einfache Restriktionen ohne Einsatz einer HOOK-Funktion bzw. von Restriktionsmengen erstellen.

Beispiel für eine Beschränkung auf den Buchstabenbereich A-H.

```
@D3REGEXPR([A-H].*)
```

```
[A-H]
```

Genau ein Zeichen aus dem Intervall A bis H.

```
.
```

Beliebiges Zeichen.

```
*
```

Wiederholung des vorangehenden regulären Ausdrucks (hier: beliebiges Zeichen) 0 bis n Mal.

Weitere Informationen und Beispiele zu den regulären Ausdrücken finden Sie im Kapitel [Regulärer Ausdruck](#).

@D3USER_REALNAME

Dieses Makro wird durch den vollständigen Namen des angemeldeten Benutzers ersetzt.

@D3USER_LONG

Dieses Makro wird durch den Anmeldenamen des angemeldeten Benutzers ersetzt.

@D3SUP

Über dieses Makro wird geprüft, ob der aufrufende Benutzer der Vorgesetzte von dem Benutzer ist, der in diesem Eigenschaftsfeld hinterlegt ist.

@D3USER_EMAIL

Dieses Makro wird durch die Mail-Adresse des angemeldeten Benutzers ersetzt.

@D3IDPUSER

Wenn Sie für ein Feld einer Dokumentklasse das Makro `@D3IDPUSER` als Restriktion angeben, wird beim Bestimmen der Berechtigungen für einen Benutzer dieses Makro durch die aktuelle ID vom Identity Provider (IDP) ersetzt.

Angenommen, in Ihrem Repository existiert eine Dokumentart "E-Mail". Diese Dokumentart enthält ein Feld mit der Bezeichnung "Benutzer". Beim Importieren von Dokumenten wird dieses Feld automatisch mit der IDP-ID von Benutzern gefüllt. Alle Benutzer des d.3-Repository erhalten Zugriff auf diese Dokumentart. Der Zugriff auf diese Dokumentart wird über eine Dokumentklasse gesteuert. Diese Dokumentklasse enthält für das Feld "Benutzer" das Makro `@D3IDPUSER` als Restriktion. Wenn ein Anwender dann mittels d.3 smart explorer im d.3-Repository nach E-Mails sucht, sieht er nur diejenigen, die seine IDP-ID im Feld "Benutzer" enthalten.

Sie können dieses Makro nur dann nutzen, wenn Sie sich am d.3-System mittels Identity Provider anmelden.

@D3IDPGROUP

Bei der Verwendung des Makros @D3IDPGROUP wird zur Laufzeit geprüft, ob die entsprechende Eigenschaft eine IDP-ID einer Gruppe enthält, in welcher der Anwender Mitglied ist. Wenn dies der Fall ist, erhält der Anwender Zugriff auf die Dokumente.

Die Information, in welchen IDP-Gruppen ein Benutzer Mitglied ist, wird bei der Anmeldung ermittelt und mittels jStore gespeichert. Dieses gecachten Daten haben eine Gültigkeit von 30 Minuten (falls keine Anmeldeinformationen zu anderen d.ecs apps mittels DECS_SERVICE_USER eingestellt sind, beträgt die Gültigkeit 10 Tage).

Änderungen an den IDP-Gruppenmitgliedschaften eines Benutzers können vom Makro @D3IDPGROUP als nur dann erfasst werden, wenn

- wenn der IDP diese schon ausliefert (Achtung: Der Identity Provider stellt diese ggwf. aufgrund seines eigenen Caches nicht direkt zur Verfügung!)
- sich der Benutzer neu anmeldet
- oder, wenn die Ablaufzeit des jStore-Cache Eintrags erreicht ist

Dokumentart Unabhängige Klasse

Im Gegensatz dazu werden bei Auswahl von **Dokumentart Unabhängig** alle Datenbankfelder (dok_dat_feld_1 bis dok_dat_feld_89) unter den Namen "DB Position X" angezeigt. Die Restriktion, die hier vorgenommen wird, gilt also nicht logisch für eine Eigenschaft (z.B. Lieferantename), sondern physikalisch für ein Tabellenfeld.

Achten Sie deshalb bei der Planung darauf, dass für die beteiligten Dokumentklassen, auf die Sie eine dokumentartunabhängige Klasse anwenden wollen, die Datenbankpositionen immer gleich sind. Hier klärt sich vielleicht die Bezeichnung bevorzugte Position bei der Anlage von Eigenschaften.

Wählen Sie als Dokumentart **Dokumentart Unabhängig** aus, dann werden Ihnen alle möglichen Eigenschaftsfelder (DOK_DAT_FELDER) angezeigt.

Unter der Bezeichnung "DB Position 1" ist das DOK_DAT_FELD_1 zu verstehen. Auch bei diesen Eigenschaftsfeldern können Sie in Abhängigkeit des Datentyps eines Feldes die zuvor genannten Sonderzeichen in den Restriktionen verwenden. Dabei sind die

- Felder 1 bis 49 Textfelder,
- 50 bis 59 Datumsfelder,
- 60 bis 69 Mehrfacheigenschaftsfelder,
- 70 bis 79 Geldfelder (numerische Felder) und
- die Felder 80 bis 89 numerische Felder.

Die oben genannten Auswahlmöglichkeiten sind hier ebenfalls gegeben.

Gesamtübersicht der Dokumentklassen

Die Gesamtübersicht gibt eine Übersicht über alle Dokumentklassen. Wollen Sie die Gesamtübersicht speichern, gehen Sie folgendermaßen vor:

1. Klicken Sie dazu auf den Button **Speichern**.
2. Alternativ betätigen die Tastenkombination **STRG+S**.



Die Kennung (ID) einer Dokumentklasse (1. Spalte der Darstellung) wird ausschließlich von d.3 server vergeben. Sie haben keinen Einfluss auf die Nummerierung.

d.3 bietet die Möglichkeit der AdHoc-Vererbung von Dokumenten. Für die Umsetzung werden Dokumentklassen auf das entsprechende Dokument erstellt. Da diese Dokumentklassen nur temporär existie-

ren, werden diese in den normalen Dialogen nicht präsentiert. In der **Gesamtübersicht** werden diese jedoch speziell gekennzeichnet dargestellt.

Weitere Informationen finden Sie auch im Kapitel d.3 [inherit rights manager](#).

Verwendungsnachweis für Klassen

Über den Button **Verwendung** auf der Übersicht der Dokumentklassen können Sie bei einer gesetzten Auswahl im Filter sehen, in welchen Berechtigungsprofilen diese Dokumentklasse Verwendung findet.



Berechtigungsprofile

Berechtigungsprofile allgemein



Anmerkung

In früheren Versionen hießen Berechtigungsprofile noch Rollen. Zum Teil wird dieser Name auch noch intern genutzt.

Ein Berechtigungsprofil ist eine Zusammenfassung von Dokumentklassen und den Rechten darauf und kann einem oder mehreren Benutzer(n), aber auch Gruppen direkt für die Rechtevergabe zugeordnet werden.

Im d.3 Projekt wird für jeden Aufgabenbereich (Abteilungen, Zuständigkeiten, etc) erarbeitet, auf welche Dokumente/Akten die Mitarbeiter Zugriff haben müssen, damit sie in ihren Aufgabenbereichen gemäß der Stellenbeschreibung die nötigen Dokumente verfügbar haben.

Ein Berechtigungsprofil kann nun als Gegenstück im d.3 eingerichtet werden, sodass später das Berechtigungsprofil nur noch den Mitarbeitern der Abteilungen zugewiesen werden muss, z.B. "Auszubildender Einkauf" oder "Vertrieb Länderbüro Südeuropa".

Angenommen, in Ihrem Unternehmen existieren die Dokumentarten "Lieferschein", "Bestellung" und "Rechnung". Ihre Mitarbeiter im Einkauf sollen lesenden Zugriff auf diese Dokumentarten erhalten. Sie könnten nun für jede dieser drei Dokumentarten eine Dokumentklasse mit der Berechtigung zum Lesen erstellen.

Abschließend werden jedem Benutzer aus dem Einkauf diese drei Dokumentklassen zugeordnet (direkte Benutzer - Klassenzuordnung). Jetzt kann es vorkommen, dass einige Wochen später eine neue Dokumentart in Ihrem Unternehmen benötigt wird, und zwar die Dokumentart "Mahnbescheid". Sie müssten nun wieder eine Dokumentklasse für den Zugriff auf die Dokumentart "Mahnbescheid" anlegen und diese Dokumentklasse allen Benutzern aus dem Einkauf zuweisen. Das wäre recht zeitaufwändig.

Die bessere Vorgehensweise ist die Verwendung eines Berechtigungsprofils. Auch bei der Verwendung eines Berechtigungsprofils müssen Sie die Dokumentklassen für die drei erstgenannten Dokumentarten anlegen. Dann wird jedoch ein Berechtigungsprofil angelegt, welche diese drei Dokumentklassen enthält. Anschließend wird allen Benutzern aus dem Einkauf dieses Berechtigungsprofil zugewiesen (Benutzer - Berechtigungsprofil-Zuordnung). Wenn jetzt nach vier Wochen die neue Dokumentart "Mahnbescheid" angelegt wird, reicht es aus, die zugehörige Dokumentklasse in das zuvor angelegte Berechtigungsprofil mit aufzunehmen.



Warnung

Der Name eines Berechtigungsprofils darf nur die Sonderzeichen "+", "-" und "_" enthalten. Andere Sonderzeichen sind nicht erlaubt.

Auswahl von Dokumentklassen

Beim Erstellen eines Berechtigungsprofils besteht nach der Benennung der erste Schritt darin, die entsprechenden Dokumentklassen auszuwählen. Die Anzahl der Dokumentklassen, die in einem Berechtigungsprofil enthalten sein können, ist nicht beschränkt.



Aus der Liste der verfügbaren Dokumentklassen wählen Sie diejenigen aus, die für das Berechtigungsprofil bestimmt sind.

Da in den ausgewählten Dokumentklassen auch Dokumentart unabhängige enthalten sein können, haben Sie die Möglichkeit, diese übergreifende Restriktion nur auf dieses Profil zu beziehen.

Hintergrund ist die Tatsache, dass bei einer solchen übergreifenden Dokumentklasse die Datenbanktabelle nur entlang einer Datenbankspalte ausgewertet wird. Wird diese Datenbankspalte aber in anderen Dokumentarten für andere Werte genutzt, würde eine falsche Interpretation erfolgen.

Das kann z.B. gegeben sein, wenn Sie Mitarbeitern mehrere Profile zuordnen. Die Dokumentart unabhängige Klasse würde über alle in den Profilen enthaltenen Dokumentklassen als "Schablone" gelegt.

Rechtevergabe



Hier lässt sich die Vielfalt der Möglichkeiten der Rechtevergabe einsehen. Sie sind z.B. in der Lage, über Profile bzw. Dokumentklassen Benutzern das Erstellen von Notizen oder Redlining-Elementen zu verbieten oder den manuellen Wechsel in den Status "Archiv" nicht zu erlauben.

Die Schaltflächen unterhalb der Rechteübersicht haben folgende Funktion:

Recht erteilen: Die Berechtigung wird grundsätzlich für das ausgewählte Recht vergeben.

Recht verweigern: Die Berechtigung wird grundsätzlich für das ausgewählte Recht nicht erteilt.

Recht ignorieren: Die Berechtigung wird an dieser Stelle weder erteilt noch verweigert. Das System prüft, ob die Berechtigung in einem anderen Berechtigungsprofil, welches dem Benutzer zugeordnet ist, erteilt wird. Ist dies nicht der Fall, gilt die Berechtigung als nicht erteilt.

Auf der rechten Seite können Sie auch mehrere Einträge auf einmal markieren. Alternativ können Sie die Berechtigungen auch per Tastenkombination setzen:

- **STRG+1:** Recht erteilen
- **STRG+2:** Recht verweigern
- **STRG+3:** Recht ignorieren

Anmerkung

Wenn Sie mehrere Einträge auf einmal auswählen und für diese ein Recht setzen möchten, dann nutzen Sie dafür diese Tastenkombinationen. Die Schaltflächen ignorieren eine Mehrfachauswahl. Die Tastenkombinationen funktionieren nur über die Nummernleiste oben auf der Tastatur, nicht über den Nummernblock.

Lesen

Sie vergeben hier die Leseerlaubnis für die jeweilige Dokumentklasse.

Anmerkung

"Lesen Bearbeitung" meint in diesem Fall auch, dass das Recht erteilt werden kann, Dokumente als Gruppenmitglied bereits im Status Bearbeitung lesen zu können.

Über "Lesen versteckter Attribute" kann hier gesteuert werden, ob die ausblendbar markierten Eigenschaften dem Benutzer angezeigt werden oder nicht (Recht verweigert).

Folgende Übersicht soll die Berechtigungen genauer erläutern:

Export abhängiges Dokument: Export des abhängigen Dokuments.

Export Original: Export des Originaldokuments.

Lesen Aktivitäten: Ansicht der Aktivitäten.

Lesen Archiv: Lesen von Dokumenten im Status Archiv.

Lesen Attribute: Wenn kein Leserecht auf Dokumente vorhanden ist, können in d.3 smart explorer zumindest die Eigenschaften angezeigt werden; das Dokument selbst kann aber nicht visualisiert werden.

Lesen Bearbeitung: Lesen von Dokumenten im Status Bearbeitung; gilt auch oder erst recht, wenn sich das Dokument NICHT in der eigenen Bearbeitung befindet.

Lesen Freigabe: Lesen von Dokument im Status Freigabe.

Lesen Gesperrt: Lesen von gesperrten Dokumenten.

Lesen Prüfung: Lesen von Dokument im Status Prüfung. Dabei sind sowohl die ungeprüften, als auch die geprüften Dokumente gemeint.

Lesen versteckter Attribute: Einblenden versteckter Eigenschaften (als ausblendbar markierte Eigenschaft). Das Recht kann nur für alle als ausblendbar markierte Eigenschaften der Dokumentklasse vergeben werden.

Anzeigen mit Wasserzeichen: Bei der Visualisierung eines Dokumentes wird ein Wasserzeichen eingezeichnet und angezeigt.

Schreiben

Sie vergeben hier die Schreiberlaubnis für die jeweilige Dokumentklasse. Hier können Sie nun auch Einfluss auf die Erstellung von Notizen oder Redlinings nehmen.

Achten Sie auf sinnvolle Kombinationen zwischen Leserecht und Schreibrecht. So ist das Recht **Ändern versteckter Attribute** nur in dem Zusammenhang sinnvoll, dass auch das Lesen dieser Eigenschaften erlaubt ist.

Folgende Übersicht soll die Berechtigungen genauer erläutern:

Ändern Attribute Bearbeitung/Prüfung: Ändern der Eigenschaften von Dokumenten im Status "Bearbeitung" und "Prüfung".

Ändern Attribute Freigabe: Ändern der Eigenschaften von Dokumenten im Status "Freigabe". Dieses Recht steht nur dann zur Verfügung, wenn der Parameter **ATTRIB_SUPPORT_MODIFY_RELEASE** eingeschaltet wurde.

Ändern geschützter Attribute: Recht, Eigenschaften zu ändern, auch wenn für die Eigenschaft die nachträgliche Modifizierung verneint wurde (siehe [modifizierbar](#)).

Ändern versteckter Attribute: Ändern von Eigenschaften, die in der Dokumentart als versteckte Eigenschaften gekennzeichnet sind.

Dokument aktualisieren: Recht, ein Dokument zu ändern (Anlegen einer neuen Version). Das Dokument muss sich dabei in der eigenen Bearbeitung befinden, bzw. das Dokument muss im Status "Bearbeitung" einer Gruppe zugeordnet sein, in der man Mitglied ist.

Dokument importieren: Recht auf Dokumentenimport

Dokumentart ändern: Recht, eine Dokumentart zu ändern. Hierdurch können erweiterte Eigenschaften geändert werden, nicht jedoch die Kategorie.

Erstellung abhängiger Dokumente: Recht zur Erstellung von abhängigen Dokumenten beim Neuimport oder bei der Dokumenten-Aktualisierung; dieses Recht bezieht sich nicht auf abhängige Signaturdateien.

Erstellung/Änderung Notizen: Recht zur Erstellung oder Änderung von Notizen zu einem Dokument.

Erstellung/Änderung Redlining: Recht zur Erstellung oder Änderung von Redlinings zu einem Dokument.

Farbmarkierung ändern: Recht, die Farb-Markierungen für die Darstellung in d.3 smart explorer zu erstellen oder zu ändern.

Löschen Archiv: Löschen von Dokumenten im Status "Archiv". Dieses Recht steht nur dann zur Verfügung, wenn der Schalter **ALLOW_DELETE_FROM_RELEASE** eingeschaltet wurde.

Löschen Bearbeitung: Löschen von Dokumenten im Status "Bearbeitung". Das Dokument muss sich dabei in der eigenen Bearbeitung oder der Bearbeitung einer Gruppe zugeordnet sein, in der man Mitglied ist.

Löschen Freigabe: Löschen von Dokumenten im Status "Freigabe". Dieses Recht steht nur dann zur Verfügung, wenn der Schalter **ALLOW_DELETE_FROM_RELEASE** eingeschaltet wurde.

Löschen Prüfung: Löschen von Dokumenten im Status "Prüfung". Zusätzlich benötigt man das Recht **Statuswechsel Prüfung** auf das Dokument.

Statustransfer

Der Dokumentstatuswechsel wird über ein Profil geregelt. Sie sehen die Verfeinerungen deutlich.

Anmerkung

Denken Sie bei der Planung daran, dass die verschiedenen Mitarbeiter entsprechende Rechte erhalten, sodass auch der manuelle Workflow weiterhin realisiert werden kann.

Das Recht, einem anderen Benutzer die Bearbeitung zu entziehen, wird oft Key-Usern bzw. Fachverantwortlichen erteilt, damit man z.B. auf die Krankheit eines Mitarbeiters reagieren kann, der wichtige Dokumente in seiner Bearbeitung hält.

Folgende Übersicht soll die Berechtigungen genauer erläutern:

Statustransfer Archiv: Statustransfer eines Dokumentes in den Status "Archiv".

Statustransfer Bearbeitung: Statustransfer eines Dokumentes in die "Bearbeitung".

Statustransfer Bearbeitung entziehen: Einem anderen Benutzer die Bearbeitung eines Dokumentes entziehen.

Statustransfer Freigabe: Freigeben eines Dokumentes.

Statustransfer Prüfen: Prüfen eines Dokumentes, Prüfung abschließen.

Statustransfer Prüfung: Statustransfer eines Dokumentes in die Prüfung, zur Prüfung.

Statustransfer Sperren: Sperren eines Dokumentes, Freigabe gesperrt.

Verknüpfungen

Dokumente können manuell verknüpft werden, einfach per Drag & Drop. Damit eine Verknüpfung "gesteuert" vorgenommen werden muss, legen Sie hier fest, was bzw. auf was verknüpft werden kann.

Folgende Übersicht soll die Berechtigungen genauer erläutern:

Verknüpfung erstellen (übergeordnetes Dokument): Recht, Dokumente der Dokumentklasse als Ziel einer Verknüpfung auszuwählen. Eine Verknüpfung zwischen zwei Dokumenten kann nur über die Kombination der Rechte **Verknüpfung erstellen (übergeordnetes Dokument)** und **Verknüpfung erstellen (untergeordnetes Dokument)** erstellt werden.

Verknüpfung erstellen (untergeordnetes Dokument): Recht, Dokumente der Dokumentklasse als Quelle einer Verknüpfung zu verwenden. Eine Verknüpfung zwischen zwei Dokumenten kann nur über die Kombination der Rechte **Verknüpfung erstellen (übergeordnetes Dokument)** und **Verknüpfung erstellen (untergeordnetes Dokument)** erstellt werden.

Verknüpfung lösen (übergeordnetes Dokument): Recht, eine Verknüpfung zwischen zwei Dokumenten zu lösen, wobei Dokumente der Dokumentklasse das Ziel der Verknüpfung sind. Eine Verknüpfung zwischen zwei Dokumenten kann nur über die Kombination der Rechte **Verknüpfung lösen (übergeordnetes Dokument)** und **Verknüpfung lösen (untergeordnetes Dokument)** gelöst werden.

Verknüpfung lösen (untergeordnetes Dokument): Recht, eine Verknüpfung zwischen zwei Dokumenten zu lösen, wobei Dokumente der Dokumentklasse die Quelle der Verknüpfung sind. Eine Verknüpfung zwischen zwei Dokumenten kann nur über die Kombination der Rechte **Verknüpfung lösen (übergeordnetes Dokument)** und **Verknüpfung lösen (untergeordnetes Dokument)** gelöst werden.

Um Verknüpfungen also gezielt zu erlauben, müssen Sie zwei Einträge machen:

Zum einen müssen Sie in dem untergeordneten Element das Recht erteilen, Verknüpfungen (als Quelle) zu erstellen, zum anderen müssen Sie auch in dem übergeordneten Element (Ziel) das Recht erteilen.

Aktivitäten

Über die Aktivitäten

Über die Aktivitäten in d.3 erfährt der Anwender, wie der Lebenszyklus eines Dokuments oder eine Akte konkret aussieht. Alle Benutzerhandlungen und Ereignisse wie z.B. der Import eines neuen Dokuments, einer neuen Version, Eigenschaftsänderungen, Workflows oder neue Kommentare können nachvollzogen werden und sind in einem chronologischen Verlauf aufgeführt. Es ist ersichtlich, wann welche Aktivität durch welchen Benutzer oder das System stattgefunden haben. Hierdurch kann bspw. ein Projektleiter auf einen Blick erfahren, was ist letzter Zeit in einer bestimmten Projektakte passiert ist.

Der Aktivitätsstrom eines Dokuments oder einer Akte wird über eine HTML-Oberfläche angezeigt, die von d.3 server bereitgestellt wird. Der Anwender sieht dann auf einer Registerkarte der Detailansicht nun den Verlauf der Änderungen seines Dokuments oder in seiner Akte. Hierbei kann er zwischen zwei Detaillierungsgraden wählen: **Kompakt** bedeutet, es werden nur die wichtigsten Aktivitäten angezeigt, während bei **Erweitert** alle Aktivitäten angezeigt werden.

Zur Aktivierung der Anzeige ist eine entsprechende, gesonderte Rechtevergabe erforderlich:

Die Anzeige der Aktivitäten zu Dokumenten kann mittels des Dokumentklassenrechtes **Lesen Aktivitäten** gesteuert werden. Dies ist standardmäßig nicht aktiv und muss manuell im Berechtigungsprofil eingeschaltet werden. Falls die Funktion generell erwünscht ist, kann separat das Script **set_activity-stream_rights.jsp** zum Setzen des Rechts genutzt werden, so dass bei bestehendem Leserecht auch der Aktivitätsstrom zum Dokument/zur Akte angezeigt werden.

Einrichten der HTTP-Schnittstelle

d.3-Konfiguration

Die HTTP-Schnittstelle von d.3 server ist im Standard aktiviert. Um diese komplett zu deaktivieren, kann in d.3 admin in der d.3-Konfiguration der Schalter **ENABLE_HTTP** auf **Nein** gesetzt werden. Dadurch können keine neuen Features genutzt werden, die diese Schnittstelle benötigen. Das betrifft aktuell:

- Die Ansicht für Aktivitäten in jeder Form (dokumentbezogen, benutzerbezogen, systemweit)
- Die Home-Seite

Einrichtung des Reverse-Proxy

d.3 server kommuniziert normalerweise über d.3 gateway mit den d.3-Anwendungen. Wenn die HTTP-Schnittstelle verwendet wird, dann verwendet d.3 gateway zusätzlich d.3 presentation server gateway als Reverse-Proxy. Die dazu notwendigen Schritte können den Hinweisen zur Inbetriebnahme am Ende des Setups der Version 8.0 entnommen werden.

Setzen der Berechtigung

Im Standard hat kein Benutzer das Recht, die Aktivitäten zu sehen.

Einzelne Rechtevergabe

Das Recht zur Anzeige der Aktivitäten heißt **Lesen Aktivitäten**. Es kann in d.3 admin in einem Berechtigungsprofil vergeben oder verweigert werden.



Globale Rechtevergabe

Alternativ kann allen Benutzern, die Leseberechtigung auf ein Dokument haben, das Recht zum Lesen der Aktivitäten erteilt werden. Dazu kann das externe JPL-Skript **set_activitystream_rights.jpl** (zu finden im d.3-Installationsverzeichnis `\d3\d3server.prg\ext_jpl`) verwendet werden. Folgen Sie dazu den Anweisungen im Skript.

Einrichten der Home-Seite

Auf der Home-Seite wird eine kundenspezifische Webseite sowie optional zwei Ansichten für Aktivitäten angezeigt. Über die Tabs **Meine Aktivitäten** und **Alle Aktivitäten** kann zwischen den verschiedenen Ansichten gewechselt werden.



Aktivieren der Aktivitäten-Ansicht

Es gibt zwei Ansichten für Aktivitäten auf der Home-Seite

- Aktivitäten des aktuellen Benutzers
- Aktivitäten im gesamten System

Aus Datenschutzgründen sind beide Ansichten im Standard deaktiviert. Um diese zu aktivieren, müssen in d.3 admin in der d.3-Konfiguration folgende Einstellungen vorgenommen werden.

- Aktueller Benutzer: **HOME_ENABLE_OWN_ACTIVITIES = Ja**
- Gesamtes System: **HOME_ENABLE_ALL_ACTIVITIES = Ja**



Der Schalter **DETAILVIEW_ENABLE_ACTIVITIES** aktiviert die dokumentbezogenen Aktivitäten für alle Benutzer.

Aktivitäten-Ansicht in d.3 smart explorer

Aktivitäten zeigt die letzten Aktivitäten des Benutzers oder auch im gesamten System an. Diese Anzeige ist standardmäßig durch oben gesetzte Schalter aktiv und kann über folgende Einstellung für bspw. bestimmte Gruppen deaktiviert werden:

d.3-Anwendungsprofil: **d.3 admin > Systemeinstellungen > d.3 client config > d.3 smart explorer > Main Window > Activities (navigation)**

Aktivitätsverlauf eines Dokuments als Anwender verfolgen

Im Fenster Verlauf werden alle Änderungen an einem Dokument als zeitlicher Verlauf dargestellt, bei Akten auch alle Änderungen innerhalb dieser.

Die Anzeige des Aktivitätsverlaufes zu Dokumenten kann mittels des Rechtes **Lesen Aktivitäten** zur Dokumentklasse gesteuert und wieder für einzelne Gruppen deaktiviert werden:

d.3-Anwendungsprofil: **d.3 admin > Systemeinstellungen > d.3 client config > d.3 smart explorer > Main Window > Drop down menu > View > Activities**

Hinterlegen einer kundenspezifischen Webseite

Im Installationsverzeichnis von d.3 server kann unter dem Ordner **html/events/home** eine kundenspezifische Webseite hinterlegt werden. Diese wird dann linksbündig auf der Home-Seite angezeigt. Im Standard ist hier ein Platzhalter hinterlegt. Die Webseite muss sich in der Datei **welcome.html** befinden. Ggf. referenzierte Dateien können in dem Ordner ebenfalls hinterlegt werden.

Berechtigungsprofil-Zuordnung

In dieser Übersicht können Sie ermitteln, welche Berechtigungsprofile einem Benutzer direkt zugeordnet sind.

Nachdem Sie einen Benutzer oder eine Gruppe ausgewählt haben, werden die Berechtigungsprofile in der Übersicht angezeigt.



Über die Checkboxen kann die Übersicht gefiltert werden.

Vollständiger Name: der vollständige Name des Benutzers kombiniert mit dem technischen Namen

d.3 Verteiler Gruppe: Verteilung von Dokumenten an alle Mitglieder der Gruppe

d.3 Strukturierungsgruppe: keine Verteilung, die Gruppe fasst nur Mitarbeiter zusammen

d.3 Tätigkeitsprofile: Verteilung an ein Mitglied der Gruppe (Lastverteiler)

Sind einem Benutzer oder der Gruppe keine Berechtigungsprofile zugeordnet, dann ist die Übersicht leer. Um ausführliche Informationen über ein dem Benutzer/der Gruppe zugeordnetes Berechtigungsprofil zu erhalten, klicken Sie doppelt auf ein Berechtigungsprofil in der Übersicht.

Im Detail-Fenster werden alle Klassen dieses Berechtigungsprofils dargestellt.

Neue Berechtigungsprofil-Zuordnung

Sie können folgendermaßen eine neue Zuordnung erstellen:





1. Klicken Sie auf **Neu**.
2. Wählen Sie im ersten Dialog zunächst alle Profile aus, die Sie zuordnen wollen.



Benutzerzuordnung

Wählen Sie alle Benutzer, Gruppen oder Tätigkeitsprofile für diese Zuordnung aus.

Über die vorangestellten Symbole kann man zwischen den folgenden Möglichkeiten unterscheiden:

- Benutzern 
- Gruppen (ohne Postkorb) 
- Gruppen (mit Postkorb) 
- Tätigkeitsprofile (Lastverteilung) 



Löschen/Bearbeiten eines Profils

1. Um eine Zuordnung von Profilen zum Benutzer zu entfernen, markieren Sie diese Berechtigungsprofile in der Übersicht mit der Maus.
2. Anschließend klicken Sie auf **Entfernen**.

Um bestehende Zuordnungen zu verändern, klicken Sie auf **Bearbeiten**.

Diese Änderungen beziehen sich jeweils nur auf den aktuell ausgewählten Benutzer.

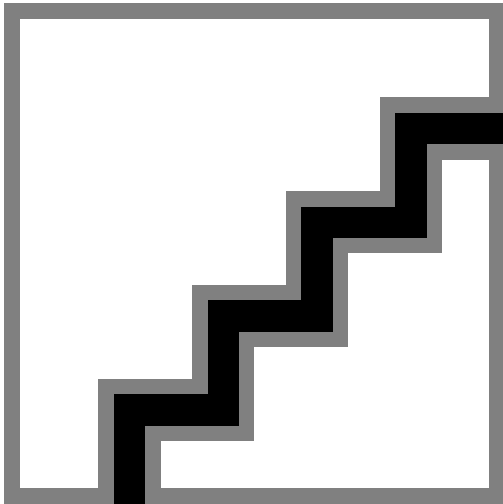
Wollen Sie mehreren Benutzern zusätzliche Profile zuordnen, gehen Sie wie bei einer neuen Zuordnung von Profilen vor.

Wenn Sie auf diese Weise dem Benutzer "USER" die Berechtigungsprofile "Profil1" und "Profil2" zuweisen, dieser Benutzer jedoch zuvor schon in der Rolle "Profil3" war, dann sind dem Benutzer am Ende drei Berechtigungsprofile zugeordnet.

Es ist nicht möglich, mehreren Benutzern gleichzeitig Berechtigungsprofile zu entziehen.

Gesamtübersicht Berechtigungsprofile


Die Übersicht zeigt, welche Berechtigungsprofile welchem Benutzer bzw. welcher Gruppe zugeordnet sind.



Es wird eine Gesamtübersicht der Berechtigungsprofile und der zugehörigen Benutzer/Gruppen dargestellt.

Auch hier erfahren Sie über die vorangestellten Symbole den Typ der Zuordnung.

 Benutzer

 Postkorbversand ohne Lastverteiler

 Postkorbversand über Lastverteiler

 kein Postkorbversand, nur Gruppierung

Möchten Sie die Übersicht speichern, betätigen Sie den **Speichern**-Button oder verwenden Sie die Tastenkombination **STRG+S**.

Benutzer-/Dokumentklassen-Zuordnung

Werden einem Benutzer (direkt oder über die verschiedenen Gruppen) Berechtigungsprofile zugeordnet, spricht man von einer impliziten Rechtevergabe, denn mit dem Berechtigungsprofil sind eine oder mehrere Dokumentklassen verbunden, welche den Zugriff auf die Dokumente steuern. Im Gegensatz dazu können Sie einem Benutzer auch explizit eine Dokumentklasse zuordnen. Die effektiven Rechte bilden sich dann aus den impliziten und den expliziten Zuordnungen.

Eine direkte (implizite) Zuordnung kann nur bei einem Benutzer vorgenommen werden.



Die **Übersicht der Benutzer- und Klassen-Zuordnungen** bezieht sich immer auf einen Benutzer. Wenn Sie einen Benutzer in der Auswahlbox auswählen, dann werden in der Übersicht die dem Benutzer direkt zugewiesenen Dokumentklassen angezeigt. In dieser Übersicht werden die Bezeichnungen der einzelnen Dokumentklassen und die Berechtigungen angezeigt.

Um diese Zuordnungen zu erstellen oder zu ändern, gehen Sie so vor:

1. Wählen Sie zuerst einen Benutzer aus.
2. Betätigen Sie dann den Schalter **Bearbeiten**.

Sie gelangen in den Zuordnungs-Dialog (Details finden Sie unter [Zuordnung der Berechtigungen](#)).

Sie können in dem daraufhin angezeigten Dialog die Zuordnungen erstellen oder auch entfernen.

Temporäre Dokumentklassen

Mit der d.3 Version 6.3 wird die AdHoc-Vererbung von Rechten auf Dokumente eingeführt. Dadurch entsteht eine differenzierte Möglichkeit der Rechtevergabe über Dokumentklassen.

Die sogenannten temporären, von d.3 server zugewiesenen Dokumentklassen, werden losgelöst von den permanenten, über d.3 admin zugewiesenen, unterschieden.

Anmerkung

Die Adhoc-Rechtevererbung funktioniert nur, wenn der Empfänger die betreffende Dokumentart in seinen Berechtigungsprofilen hat.

Unter den **Permanenten Dokumentklassen** sind die "normalen" Dokumentklassen aufgeführt. Unter den **Temporären Dokumentklassen** werden die aufgrund einer Vererbung zugewiesenen Dokumentklassen gelistet. Diese vererbten Dokumentklassen können vom d.3- Administrator NICHT manipuliert, z. B. die Berechtigungen verändert werden.

Wird der Benutzer "bearbeitet", werden die temporären Dokumentklassen in der Auswahlübersicht nicht gelistet.

Verfügt der Benutzer jedoch über geerbte Dokumentklassen, erhalten Sie einen entsprechenden Dialog.

Der d.3-Administrator hat hier die Möglichkeit, die durch Vererbung zugewiesenen Dokumentklassen zu entfernen.

Warnung

Sie greifen damit in laufende Prozesse ein. Die Aktion muss daher ein weiteres Mal bestätigt werden.

Sub-Administration

Die Sub-Administration ermöglicht es, weitere d.3-Benutzer administrative Rechte zu vergeben. Dabei lässt sich einstellen, dass der entsprechende Benutzer nur bestimmte Rechte erhält bzw. nur bestimmte Punkte in d.3 admin sehen und Zugriff darauf hat.



Anmerkung

Ein Administrator kann jeden Benutzer zum Sub-Administrator machen. Ein Sub-Administrator kann keine weiteren Sub-Administratoren anlegen oder seine eigenen Rechte als Sub-Administrator ändern.

Außerdem kann ein Sub-Administrator keine Projekte/Meilensteine importieren oder exportieren, da unkontrolliertes Importieren von Projekten/Meilensteinen in das Produktivsystem zu schweren Inkonsistenzen führen könnte und dies ein Sicherheitsproblem für das Produktivsystem darstellt.

Benutzer als Sub-Administrator hinzufügen

Sie haben zwei Möglichkeiten einen Sub-Administrator zu ernennen:

- Legen Sie einen neuen Benutzer direkt mit allen gewünschten Rechten an.
- Fügen Sie einen vorhandenen Benutzer zum Sub-Administrator hinzu weisen Sie im Sub-Administrator-Dialog die Rechte zu.

Anmerkung

Prinzipielles Rechtssystem:

Das Leserecht bewirkt, dass der Sub-Administrator den Menüpunkt überhaupt erst sehen kann.

Das Schreibrecht bewirkt, dass der Sub-Administrator nach dem Wechseln in den Bearbeitungsmodus auch noch das Modul öffnen kann. Wenn das Schreibrecht nicht gesetzt ist, so ist der Menüpunkt ausgegraut.

Schreibrechte implizieren Leserechte und überschreiben Sie. Wenn das Schreibrecht gesetzt ist, ist automatisch das Leserecht vorhanden.

Um einen bereits existierenden Benutzer als Sub-Administrator hinzuzufügen, gehen Sie folgendermaßen vor:

1. Wählen Sie den gewünschten Benutzer in der Übersicht der Benutzer über **Berechtigungen | Benutzer** aus.
2. Öffnen Sie die **Eigenschaften** des Benutzers.
3. Wechseln Sie dort zu den **erweiterten Eigenschaften**.
4. Weisen Sie in den Rechtebereichen unter **Benutzer | d.3 | Benutzerkonto** in der Objektübersicht rechts dann die **Sub-Administrator-Berechtigung** zu.



5. Wechseln Sie dann über den Menüpunkt **Berechtigungen** in die **Sub-Administration**.
6. Wählen Sie im Dialog Übersicht der Sub-Administratoren den gewünschten und nun unter Sub-Administratoren aufgeführten Benutzer aus.
7. Anschließend rechts in den Rechtebereichen den gewünschten Menüpunkt von d.3 admin unterhalb **d.3 Administration**.
8. Darunter befindet sich die Rechteübersicht, wo Sie dann das entsprechende Recht per Klick in die Spalte Zuweisung oder über die darunter befindlichen Schaltflächen **Zuweisen**, **Entziehen**, **Ignorieren** setzen.
9. Speichern Sie die Änderungen mit **OK**.

Die folgende Abbildung zeigt beispielhaft, dass ein Benutzer ein Leserecht für die Übersicht der Benutzer erhält, aber dort keine Änderungen vornehmen darf.



Anmerkung

Wie kann ein Sub-Administrator angelegt werden, der nur das Kennwort von Nutzern ändern kann?

Wenn Sie einen Sub-Administrator anlegen und das Leserecht auf Benutzer vergeben, reicht dieses Leserecht aus, um in Benutzerdialog das Kennwort zu ändern.

Unterhalb **Berechtigungen | Sub-Administration** finden Sie nun den vorher ausgewählten Benutzer in der Übersicht der Sub-Administratoren. Auch hier lassen sich noch Rechte zuweisen oder wieder entziehen.



Anmerkung

Die Sub-Administration ist ebenfalls über Gruppen möglich. Allen Gruppen können prinzipiell ebenfalls die Sub-Administrationsberechtigungen gegeben werden. Die User der Gruppe erhalten dann die Rechte, da die Sub-Administration auf Basis der effektiven Benutzerrechte funktioniert. Woher der Sub-Administrator seine Berechtigung(en) hat, kann durch die [Berechtigungsanalyse](#) nachgesehen werden.

Auch LDAP-User können Sub-Administratoren werden.

Berechtigungsanalyse

Die Berechtigungsanalyse soll Ihnen einen Überblick der effektiven Rechte eines Benutzers auf Dokumente, Dokumentklassen und Policies verschaffen.

1. Wählen Sie zunächst eine Benutzerkennung aus, für die Sie Berechtigungsinformationen erlangen wollen.
2. Für diesen Benutzer wählen Sie anschließend den gewünschten Rechte-Typ (Benutzer oder Dokumentklasse) aus.



Rechtstyp Benutzer

In der Darstellung zum Rechtstyp Benutzer werden die erweiterten Berechtigungen (Policies) im rechten unteren Bereich präsentiert. Die Baumstruktur links besteht aus einem Hauptknoten und ggf. mehreren Unterknoten. Hier wählen Sie aus, für welche Ebene Ihnen die Policies dargestellt werden sollen. Zusätzliche Informationen erhalten Sie auch immer in der Statuszeile des Fensters.

Über die Ebene des Hauptknotens erhalten Sie die effektiven Rechte des Benutzers. Daher sind alle Berechtigungen im rechten unteren Bereich mit **Ja** oder **Nein** bestimmt. Ob die Verweigerung des Rechts (**Nein**) über die direkte Zuordnung **Recht verweigert** resultiert oder über ein durchgereichtes **Recht ignoriert** resultiert, kann man auf der Ebene der effektiven Rechte nicht ersehen. Markieren Sie allerdings einen Unterknoten, wobei Benutzer, Gruppe oder Organisationseinheit auswählbar sind, erhalten Sie die Rechte angezeigt, die auf dieser Ebene zugewiesen wurden.



Über die Auswahl im rechten, oberen Bereich können Sie die Darstellung weiter filtern.

Anmerkung

Beachten Sie, dass auf dieser Ebene ein leerer Eintrag **Recht ignoriert** bedeutet. Erst bei der Ermittlung des effektiven Rechts im Hauptknoten wird daraus ggf. ein **Nein**.

Rechtstyp Dokumentklasse

Interessieren Sie sich für die Berechtigungen eines Benutzers bezogen auf Dokumentklassen, wählen Sie als Rechtstyp **Dokumentklasse** aus.



Im linken Fenster werden alle Dokumentklassen, die dem Benutzer zugeordnet sind, gelistet, im rechten oberen Fenster werden die Dokumentklassenrechte als Filter angeboten.

Allgemeine Rechte auf die Dokumentart

Wählen Sie eine Akten- oder Dokumentart aus, erhalten Sie zunächst eine Übersicht aller Dokument- und Aktenarten des ausgewählten Benutzers. Für die jeweils markierte Dokumentart erhalten Sie im unteren, rechten Fenster die allgemeinen Rechte angezeigt.

Anmerkung

Besonderheit: Die Rechte auf versteckte Eigenschaften (**Lesen versteckter Eigenschaften** , **Schreiben versteckter Eigenschaften**) werden hier unter dem Aspekt der Darstellung in d.3 smart explorer bzw. d.3 import angezeigt.

Damit ist gemeint, dass die Information geliefert wird, ob diese Felder in den Anwendungen verfügbar oder nicht verfügbar sind.



Effektive Rechte auf Dokumentklasse

Markieren Sie unterhalb des Baums zu einer Dokumentart eine Dokumentklasse, werden die effektiven Rechte der Dokumentklasse dargestellt.

Ja: Das Recht wurde erteilt.

Verweigert: Das Recht wurde verweigert.

Nein: Das Recht wurde ignoriert und es gilt standardmäßig **Nein**.




Zugewiesene Rechte über Benutzer, Gruppen oder Organisationseinheiten

Öffnen Sie in der linken Baumstruktur die unterste(n) Ebene(n) und wählen einen Eintrag aus.


Sie erhalten Sie die Rechte, die über dieses Element vergeben wurden.



Dabei bedeuten die Symbole und Beschriftungen:

 direkte Zuordnung einer Dokumentklasse oder eines Berechtigungsprofils zum Benutzer.

Ob es sich um eine direkte Zuordnung einer Dokumentklasse oder eines Berechtigungsprofils handelt, ist in dieser Darstellung nicht zu erkennen. Vergeben Sie also immer aussagekräftige Bezeichnungen für Dokumentklassen und Berechtigungsprofile.

 Zuordnung der Dokumentklasse über ein Profil (Bezeichnung bis zu Klammern).

Das Profil wurde über die Gruppe (Bezeichnung in Klammern) zugeordnet.

Der Typ der Gruppe (Lastverteilung, keine Lastverteilung, Gruppe ohne Postkorb) lässt sich nicht ablesen, hat aber für die Berechtigungen auch keine Bedeutung.

Berechtigung zu einem Dokument

Über die Eingabe einer Dokument-ID können Sie ermitteln, welche Berechtigungen der ausgewählte Mitarbeiter auf ein Dokument hat. Geben Sie hierfür im Feld **Dokument-ID** die konkrete Dokument-ID ein.



In der Darstellung wird zum einen die Dokumentart bzw. Aktenart fett hervorgehoben, zu der die Dokument-ID gehört, zum anderen wird in der Baumstruktur auch die Dokumentklasse hervorgehoben, über die der Mitarbeiter die Berechtigungen erhalten hat. Die konkreten Berechtigungen auf die Dokumentklasse bezogen lassen sich wie vorher beschrieben ansehen und filtern.

Die Eigenschaften des Dokuments lassen sich über die Drucktaste **Eigenschaften** abrufen.

Effektive Berechtigungen zu einem Dokument

Für die Anzeige der effektiven Rechte zu einem Dokument, das Sie über die Dokument-ID gefunden haben, klicken Sie auf die Schaltfläche **Rechte**.

Sie erhalten anschließend eine Übersicht.

Über die Auswahl einer entsprechenden Ebene im rechten, oberen Fenster werden die gefilterten Rechte angezeigt.

d.3 organizational structure

Mit dem Aufruf des d.3 admin PlugIns **d.3 organizational structure** erscheint die Organisationsstruktur.

Über die Organisationsstruktur ist es möglich, eine Hierarchie der Mitarbeiter eines Unternehmens abzubilden.

Diese Struktur ist Grundlage der Vertreterregelung inkl. des Lastverteilmechanismus (siehe hierzu: [Vertreterregelung](#)). Über diese hinterlegte Struktur erhält der Vorgesetzte die Möglichkeit, die Abwesenheitssteuerung seiner Mitarbeiter zu übernehmen, z. B. bei Krankheit. Stellvertreter und auch Leiter eines Bereichs werden bei der Gruppeneinstellung bestimmt.



Im linken Fenster wird die erzeugte Struktur baumartig dargestellt. Die einzelnen Ebenen lassen sich nach Bedarf öffnen. Zum ausgewählten Knoten werden im unteren rechten Fenster die Mitglieder der Gruppe angezeigt.

Im rechten, oberen Fenster werden alle Gruppen, die in der Organisationsstruktur noch nicht zugeordnet sind, zur Auswahl angezeigt. Über die vorangestellten Symbole kann auch der Typ der Gruppe einfach unterschieden werden.

Im unteren, rechten Fenster werden immer die Mitglieder der markierten Gruppe angezeigt. Sie können also auch im rechten, oberen Fenster eine Gruppe markieren. Mitglieder können neben Benutzern auch wiederum Gruppen sein.

Hinzufügen einer Organisationseinheit

Um eine neue Organisationseinheit anzulegen, gehen Sie folgendermaßen vor:

1. Markieren Sie zunächst den Knoten, unterhalb dem die neue Einheit eingefügt werden soll.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Tragen Sie in dem erscheinenden Fenster die Bezeichnung der neuen Organisationseinheit ein.

Im Dialog wird immer die übergeordnete Ebene angezeigt, sodass Sie noch einmal die Hierarchie kontrollieren können.

Anschließend wird die neue Ebene in der Baumstruktur angezeigt und Sie können nun Gruppen zuordnen.

Gruppe(n) der Organisationseinheit zuordnen

Die Zuordnung von Gruppen zu einer Organisationseinheit erfolgt über Drag&Drop. "Greifen" Sie also die Gruppe im rechten Auswahlfenster mit der linken Maustaste und Sie ziehen diese auf die Organisationseinheit, zu der diese Gruppe gehören soll.

Für die Zuordnung ist es hilfreich, dass zur jeweils markierten Gruppe immer die Mitglieder im unteren rechten Fenster angezeigt werden.

Über Drag&Drop können Sie auch bereits erstellte Zuordnungen verändern. Ziehen Sie dann die Gruppe einfach in die andere Organisationseinheit.

Zuordnung löschen

Wollen Sie eine Zuordnung wieder löschen, z. B. eine Gruppe aus der Organisationseinheit entfernen, haben Sie folgende Möglichkeiten:

Markieren Sie die Gruppe und betätigen die Drucktaste **Entfernen**.

Oder:

Wählen Sie im Kontextmenü den Eintrag **Entfernen** aus.

Oder:

Ziehen Sie die Gruppe einfach wieder in das Auswahlfenster rechts, oben zurück.

Nach Bestätigung der Sicherheitsabfrage ist die Zuordnung gelöscht und die Gruppe wieder in der Auswahl verfügbar.

Anmerkung

Löschen Sie eine Organisationseinheit, die Gruppenzuordnungen enthält, werden diese Gruppen automatisch der nächsthöheren Ebene zugeordnet.

Leitung definieren

Sie haben die Möglichkeit, über das Kontextmenü eine Gruppe als Leitung der Organisationseinheit zu definieren.

Damit werden alle Mitglieder dieser Gruppe zu Leitern der Organisationseinheit. Dabei ist aber zu beachten, dass mindestens eine weitere Gruppe als Mitglied der Organisationseinheit angegeben wird. Dann können alle Mitglieder dieser Leitungsgruppe die Abwesenheitssteuerung übernehmen.

Alternativ können Sie natürlich für jede Gruppe die Leitung der Gruppe definieren (siehe hierzu [Gruppe anlegen](#); [Lastverteilung](#)).

Benutzer in Organisationseinheiten

Wenn Sie erfahren wollen, in welchen Organisationsebenen ein Mitarbeiter zu finden ist, wählen Sie in der Auswahlliste **Benutzer** einen Namen aus.

Anschließend werden alle Ebenen, in denen der Mitarbeiter enthalten ist, unterstrichen dargestellt.



IDP-Unterstützung

d.ecs identity provider (kurz IDP) authentifiziert Benutzer über verschiedene Authentifizierungsverfahren wie z.B. die Windows-Authentifizierung (Kerberos) mit Benutzername und Passwort gegen unterschiedliche Systeme zur Benutzerverwaltung wie z.B. Active Directory (AD) und stellt hierüber die erforderlichen Benutzerinformationen für die Nutzung durch andere Apps bereit.

Der Sinn der d.3-IDP-Unterstützung ist, dass Sie nur IDP als führendes System zur Benutzerverwaltung haben. Sie ersparen sich so, Benutzer auf Fremdsystemen wie Microsoft Windows sowie auf d.3-Ebene doppelt zu verwalten.

Ab d.3-Version 8.2 ist die IDP-Unterstützung in d.3 admin integriert. Sie bietet die Möglichkeit, Benutzergruppen von IDP mit d.3-Benutzergruppen sowie d.3-Berechtigungsprofilen zu koppeln und somit Benutzern Rechte auf d.3-Objekte zu erteilen.

Systemvoraussetzungen

Für die IDP-Unterstützung eines d.3-Systems muss d.ecs infrastructure setup mindestens in der Version 1.2.2 installiert sein.

In d.ecs http gateway muss das d.3-System als App d3 registriert sein.

Im d.3-Repository ist der Parameter **ENABLE_HTTP** standardmäßig aktiviert.

Aktivieren der IDP-Unterstützung

Über den d.3-Konfigurationsparameter **AUTH_SYSTEM** wird das Authentifizierungssystem für den Zugriff auf das d.3-System eingestellt. Stellen Sie hier den Wert des Parameters auf IDP. Sie finden diesen Parameter in d.3 config unter **d.ecs infrastructure**.

Zusätzlich müssen Sie noch über die Parameter **DECS_SERVICE_USER** und **DECS_SERVICE_USER_PWD** die Daten eines Service-Benutzer für den Zugriff auf IDP einstellen.

Speichern Sie anschließend die Konfiguration und beenden Sie d.3 admin. Starten Sie alle d.3-Prozesse in d.3 process manager neu, damit die neue Konfiguration wirksam wird. Starten Sie anschließend d.3 admin neu.

Sobald die Benutzersteuerung über die IDP-Verknüpfung aktiviert ist, ist der IDP das führende System gegen das Berechtigungen überprüft werden. Ist die IDP-Authentifizierung fehlgeschlagen und ist eine Anmeldung an IDP nicht möglich, prüft d.3, ob es sich um einen lokalen Benutzer handelt und führt gegebenenfalls damit die Anmeldung durch.

Theoretisch können sich alle Benutzer am d.3-System anmelden, die über IDP definiert sind und mit den IDP-Zuordnungen von d.3 ausgelesen werden. Dies ist aber nur möglich, wenn diesem auch über die Berechtigungszuweisung im d.3-IDP-Dialog entsprechende Berechtigungen zugeordnet wurden.

Mit der ersten Anmeldung wird ein d.3-Benutzer angelegt, der auch in d.3 admin gepflegt werden kann. Änderungen an dem zugehörigen d.3-Benutzer haben keine Auswirkungen, da IDP immer das führende System ist und die über den d.3-IDP-Dialog zugeordneten Berechtigungen jeweils neu eingelesen werden. Die Konfiguration bezüglich grundsätzlicher Berechtigungen (soweit möglich) muss im d.3-IDP-Dialog erfolgen.

Bei jeder d.3-Anmeldung werden die Daten an IDP übergeben. Die Anmeldung und das Kennwort werden über IDP verifiziert.

In Verbindung mit IDP sind Benutzer dem d.3-System erst bekannt, nachdem sie sich mindestens einmal angemeldet haben.

Folgende weitere Parameter können in diesem Zusammenhang zusätzlich gesetzt werden:

AUTH_SYSTEM_NEW_USER_ONLY_MODE: "Nur neue Benutzer" Modus für die Übernahme von Benutzern aus Fremdsystemen.

Wird dieser Modus aktiviert, so werden nur noch neue Benutzer aus Fremdsystemen nach d.3 übernommen, aber keine Änderungen mehr an bestehenden Benutzern vorgenommen. Dieser Modus kann genutzt werden, wenn die Benutzer per d.3 admin gepflegt und verändert werden sollen.

Die Änderungen werden nicht von der IDP-Schnittstelle übersteuert. Die per d.3-IDP-Dialog vorgenommenen Eigenschaften- und Rechtezuweisungen greifen hier nur für die initiale Übernahme eines externen Benutzers nach d.3.

Standardeinstellung = 0 (deaktiviert):

Alle Änderungen in der IDP-Konfiguration oder an den Daten im Directory Service werden nach d.3 übernommen.

AUTH_SYSTEM_SYNC_TIME: Zeitangabe für Synchronisierung aller Benutzer aus Fremdsystemen.

Wird hier eine Uhrzeit (Format: "hh:mm") angegeben, so wird jeden Tag zu dieser Zeit eine Synchronisierung der d.3-Benutzerverwaltung mit der über das IDP-Administrationsmodul konfigurierten IDP-d.3-Verbindungen durchgeführt.

Dabei werden neue Benutzer sowie geänderte Benutzereinstellungen vorhandener Benutzer nach d.3 übernommen.

Erstellen und verwalten von IDP-Zuordnungen

Öffnen Sie den Dialog zur Erstellung und Verwaltung von IDP-Zuordnungen unter **IDP-Unterstützung**.

Die Zuordnung von IDP-Daten gliedert sich in die Bereiche **Hinweise**, **Gruppen** und **Benutzer Informationen**.

Alle Änderungen an den Daten, die Sie in diesem Dialog vornehmen, werden zunächst intern vorgemerkt. Erst wenn Sie auf **Speichern** klicken, werden die Daten zum Server übertragen und gültig.

Mit **Neu laden** können Sie die Daten erneut vom Server abrufen. Dabei gehen alle vorgemerkten, noch nicht gespeicherten Informationen verloren.

Aktivieren Sie die Option **LDAP-IDP-Konvertierungsvorschläge**, um Vorschläge zur Konvertierung der bisherigen LDAP-Konfiguration zu erhalten.

Bitte beachten Sie:

- Diese Option ist nur verfügbar, wenn Sie das IDP-Authentifizierungssystem noch nicht aktiviert haben.
- Wenn Sie diese Option aktivieren bzw. deaktivieren, wird der Dialog neu geladen. Dabei gehen alle vorgemerkten, noch nicht gespeicherten Informationen verloren.
- Die Vorschläge werden, zusammen mit den bereits definierten Zuordnungen, unter **Gruppen und Benutzer Informationen** im Bereich **IDP-Zuordnungen** dargestellt. Die Vorschläge sind blau, die Bestandsdaten schwarz.

IDP-Hinweise

Wenn Sie die Option **LDAP-IDP-Konvertierungsvorschläge** aktiviert haben, werden bei der Ermittlung der Vorschläge ggf. auch Hinweise generiert. Sie erhalten beispielsweise Hinweise, dass LDAP-Einstellungen nicht direkt auf IDP-Einstellungen abbildbar sind. Sie erhalten diese Hinweise als Liste unter **Hinweise**.

IDP-Gruppenzuordnung

Unter **Gruppen** konfigurieren Sie, welche IDP-Gruppen welchen d.3-Benutzergruppen oder d.3-Berechtigungsprofilen zugeordnet werden sollen.

Erstellen von IDP-Gruppenzuordnungen

Sie möchten eine neue IDP-Zuordnung erstellen. Sie können d.3-Objekte mehreren IDP-Gruppen zuordnen. Sie können entweder eine d.3-Benutzergruppe oder ein d.3-Berechtigungsprofil zuordnen.

So geht's

1. Wählen Sie unter **IDP-Gruppen** einen Eintrag aus der Auswahlliste aus.
2. Wählen Sie unter **Objekttyp** den Zuordnungstyp aus (Benutzergruppe oder Berechtigungsprofil).
3. Wählen Sie unter **d.3 Objekte** einen Eintrag aus der Auswahlliste aus.
4. Klicken Sie auf **Hinzufügen**, um die Auswahl zu bestätigen.

Sie haben einen neuen Eintrag unter **IDP-Zuordnungen** erstellt. Der Eintrag wird grün dargestellt.

Löschen von IDP-Gruppenzuordnungen

Sie möchten eine bestehende IDP-Zuordnung löschen.

So geht's

1. Markieren Sie die zu entfernende IDP-Zuordnung.
2. Klicken Sie auf **Löschen**. Beachten Sie beim Löschen Folgendes:
 - Handelt es sich bei dem gewählten Eintrag um ein untergeordnetes Element in der Liste, wird nur diese IDP-Zuordnung gelöscht.
 - Handelt es sich bei dem gewählten Eintrag um ein übergeordnetes Element auf der Hauptebene, werden alle zugehörigen untergeordneten IDP-Zuordnungen gelöscht.

Die gelöschten Einträge werden intern zur Löschung vorgemerkt und rot und durchgestrichen dargestellt.

Akzeptieren von IDP-Gruppenzuordnungen

Sie möchten eine automatisch vorgeschlagene IDP-Gruppenzuordnung akzeptieren.

So geht's

1. Wählen Sie den entsprechenden Eintrag (blau dargestellt) im Bereich **IDP-Zuordnungen** aus.
2. Klicken Sie auf **Akzeptieren**. Beachten Sie beim Akzeptieren Folgendes:
 - Handelt es sich bei dem gewählten Eintrag um ein untergeordnetes Element in der Liste, wird nur dieser Vorschlag übernommen.
 - Handelt es sich bei dem gewählten Eintrag um ein übergeordnetes Element auf der Hauptebene, werden alle zugehörigen untergeordneten Vorschläge übernommen.

Die akzeptierten Vorschläge werden intern zur Übernahme vorgemerkt und grün dargestellt.

Ablehnen von IDP-Gruppenzuordnungen

Sie möchten eine automatisch vorgeschlagene IDP-Gruppenzuordnung ablehnen.

So geht's

1. Wählen Sie den entsprechenden Eintrag (blau dargestellt) im Bereich **IDP-Zuordnungen** aus.
2. Klicken Sie auf **Ablehnen**. Beachten Sie beim Ablehnen Folgendes:
 - Handelt es sich bei dem gewählten Eintrag um ein untergeordnetes Element in der Liste, wird nur dieser Vorschlag verworfen.
 - Handelt es sich bei dem gewählten Eintrag um ein übergeordnetes Element auf der Hauptebene, werden alle zugehörigen untergeordneten Vorschläge verworfen.

Die abgelehnten Vorschläge werden intern vermerkt und blau und durchgestrichen dargestellt.

IDP Benutzer Informationen

Unter **Benutzer Informationen** legen Sie fest, welche Benutzerinformationfelder die Benutzerverwaltung (IDP) welchen d.3-Benutzerfeldern zugeordnet werden.

Erstellen von IDP-Feldzuordnungen

Sie möchten eine neue IDP-Feldzuordnung erstellen. Wenn Sie einen LDAP-Server als User Provider in Ihrer Benutzerverwaltung (IDP) definiert haben, können Sie die Benutzereigenschaftsfelder von diesem LDAP-Server als d.3-Benutzereigenschaften definieren.

Beispiel: Wenn in Ihrem LDAP-Server für den Straßennamen das Feld **streetAddress** definiert ist, können Sie diese Eigenschaft dem d.3-Feld **Option 1** zuweisen. In d.3 wird im Feld **Option 1** anschließend der jeweilige Straßename des Benutzers angezeigt.

So geht's

1. Wählen Sie im Bereich **IDP-Zuordnungen** ein d.3-Benutzerfeld aus.
2. Geben Sie unter **Feldname** den Name der IDP-Eigenschaft an, die dem d.3-Feld zugeordnet werden soll. Den Namen der IDP-Eigenschaft können Sie in Ihrem LDAP-Server ermitteln.
3. Klicken Sie auf **Hinzufügen**.

Sie haben einen neuen Eintrag unter **IDP-Zuordnungen** erstellt. Der Eintrag wird grün dargestellt.

Löschen von IDP-Feldzuordnungen

Sie möchten eine bestehende IDP-Zuordnung löschen.

So geht's

1. Markieren Sie die IDP-Zuordnung unter **IDP-Zuordnungen**.
2. Klicken Sie auf **Löschen**. Beachten Sie hierbei Folgendes:
 - Handelt es sich bei dem gewählten Eintrag um ein untergeordnetes Element in der Liste, wird nur diese Zuordnung gelöscht.
 - Handelt es sich bei dem gewählten Eintrag um ein übergeordnetes Element auf der Hauptebene, werden alle zugehörigen untergeordneten Zuordnungen gelöscht.

Die gelöschten Einträge werden intern zur Löschung vorgemerkt und rot und durchgestrichen dargestellt.

Akzeptieren von IDP-Feldzuordnungen

Sie möchten eine automatisch vorgeschlagene IDP-Feldzuordnung akzeptieren.

So geht's

1. Wählen Sie den entsprechenden Eintrag (blau dargestellt) im Bereich **IDP-Zuordnungen** aus.
2. Klicken Sie auf **Akzeptieren**. Beachten Sie beim Akzeptieren Folgendes:
 - Handelt es sich bei dem gewählten Eintrag um ein untergeordnetes Element in der Liste, wird nur dieser Vorschlag übernommen.
 - Handelt es sich bei dem gewählten Eintrag um ein übergeordnetes Element auf der Hauptebene, werden alle zugehörigen untergeordneten Vorschläge übernommen.

Die akzeptierten Vorschläge werden intern zur Übernahme vorgemerkt und grün dargestellt.

Ablehnen von IDP-Feldzuordnungen

Sie möchten eine automatisch vorgeschlagene IDP-Feldzuordnung ablehnen.

So geht's

1. Wählen Sie den entsprechenden Eintrag (blau dargestellt) im Bereich **IDP-Zuordnungen** aus.
2. Klicken Sie auf **Ablehnen**. Beachten Sie beim Ablehnen Folgendes:
 - Handelt es sich bei dem gewählten Eintrag um ein untergeordnetes Element in der Liste, wird nur dieser Vorschlag verworfen.
 - Handelt es sich bei dem gewählten Eintrag um ein übergeordnetes Element auf der Hauptebene, werden alle zugehörigen untergeordneten Vorschläge verworfen.

Die abgelehnten Vorschläge werden intern vermerkt und in blau und durchgestrichen dargestellt.

LDAP-Unterstützung

Informationen zur LDAP-Unterstützung finden Sie in der Dokumentation d.3 admin ldap.

d.3 policy manager

d.3 policy manager erlaubt die Vergabe von erweiterten Rechten an Benutzer, Gruppen und Organisationseinheiten. Die Rechte sind in drei Bereiche aufgeteilt:

- Benutzerkonto
- Anwendungen
- Dokumentenrechte



Anmerkung

Wird ein Recht einmal verweigert, egal ob direkt beim Benutzer oder aber z. B. bei einer Gruppe, wird das Recht für den jeweiligen Benutzer immer verweigert. Steht ein Recht für einen Benutzer in der Summe auf **Ignoriert**, wird dieses in der Regel verweigert. Sollte es Ausnahmen dazu geben, werden diese im Folgenden aufgeführt.

Benutzer-Rechte oder "Policies" sind Rechte bzw. Eigenschaften, die Benutzern, aber auch Gruppen oder Organisationseinheiten, zugewiesen werden können. Das bedeutet, dass ein Recht für einen Benutzer auch aus der Mitgliedschaft in einer Gruppe bestimmt werden kann.

Anwendungen

Web-Zugriff: Benutzer mit dieser Berechtigung können die Web-Recherche- und Import-Komponenten verwenden. Legt man einen neuen Benutzer an, muss dieses Recht explizit erteilt werden.

Workflow hochladen: Mit diesem Recht erhält ein Benutzer die Berechtigung, Leitwege zum Server hochzuladen. Bei deaktivierten erweiterten Berechtigungen haben noch alle Benutzer diese Berechtigung. Aktiviert man die erweiterten Rechte, haben die Benutzer nicht mehr dieses Recht. Ebenso muss man neu angelegten Benutzern diese Berechtigung explizit erteilen.

Workflow freigeben: Mit diesem Recht erhält ein Benutzer die Berechtigung, Leitwege freizugeben. Bei deaktivierten erweiterten Berechtigungen haben noch alle Benutzer diese Berechtigung. Aktiviert man die erweiterten Rechte, haben die Benutzer nicht mehr dieses Recht. Ebenso muss man neu angelegten Benutzern diese Berechtigung explizit erteilen.

Workflow deaktivieren: Mit diesem Recht erhält ein Benutzer die Berechtigung, Leitwege zu deaktivieren. Bei deaktivierten erweiterten Berechtigungen haben noch alle Benutzer diese Berechtigung. Aktiviert man die erweiterten Rechte, haben die Benutzer nicht mehr dieses Recht. Ebenso muss man neu angelegten Benutzern diese Berechtigung explizit erteilen.

Workflow beaufsichtigen: Mit diesem Recht erhält ein Benutzer die Berechtigung sich am d.3 flow inspector anzumelden und dort Workflows zu beaufsichtigen und zu administrieren. Dies beinhaltet das Recht Dokumente aus einem ausgewählten Workflow zu entfernen oder innerhalb des Workflows zu verschieben.

Anzeigen des Audit-Trails (alles): Mit diesem Recht erhält ein Benutzer die Berechtigung, alle Protokolle einsehen zu dürfen.

Postkörbe anderer Benutzer sichten: Hier wird bestimmt, wer Postkörbe anderer Benutzer einsehen darf. Voraussetzung hierfür ist die konfigurierte Organisationsstruktur, in der die Hierarchie festgelegt wurde. Beachten Sie auch die Konfiguration zu den [Gruppen](#), in denen Sie die Vertreterregelungen festlegen können.

Zugriff auf JPL-Skripte: JPL-Skripte benutzerabhängig ausführen (für internen Gebrauch, Projekt bezogen)

Nicht vollständig signierte Dokumente freigeben: Auch wenn nicht alle Signaturen vorliegen, kann das Dokument dennoch freigegeben werden.

Ändern der E-Mail-Benachrichtigungen: Mit der Option **E-Mail-Benachrichtigung** in d.3 smart explorer können d.3-Anwender angeben, ob sie per E-Mail Benachrichtigungen für Nachrichten oder Workflowaufgaben erhalten möchten.

Als d.3-Administrator müssen Sie Folgendes tun, damit Ihre d.3-Anwender die Funktion **E-Mail-Benachrichtigung** nutzen können:

- In d.3 admin müssen Sie den E-Mail-Versand aktivieren.
- Die d.3-Anwender müssen darüber hinaus die Berechtigung besitzen, die Einstellungen ändern zu dürfen. Wenn Sie den Anwendern keine Berechtigung zum Ändern zuweisen, werden ihnen global definierte Werte aus d.3 admin angezeigt. Folglich können die Anwender die Einstellungen lediglich aufrufen und ansehen, jedoch nichts ändern.

Anmerkung

Die Rechte für Workflow-Funktionen und E-Mail-Benachrichtigungen können im LDAP-Plugin nicht direkt zugewiesen werden. Stattdessen müssen diese in d.3 policy manager einer Gruppe zugewiesen werden. Dieser Gruppe kann dann ein Berechtigungsprofil zugeordnet werden, auf das Mitarbeiter dann aus dem LDAP-Baum gemappt werden.

Benutzerkonto

Kann Kennwort nicht ändern: Der Benutzer, dem dieses Recht zugewiesen wurde, kann sein Kennwort nicht ändern.

Kennwort läuft nie ab: Bei Erteilung des Rechts läuft das Kennwort des Benutzers niemals ab. Dieses Recht überschreibt die d.3-Server-Einstellung **PASSWORT_EXPIRE_DAYS**.

Dialoganmeldung: Der Benutzer bekommt das Recht, sich über d.3 login manager an einem d.3 -Repository anzumelden.

Im Folgenden werden die erweiterten Rechte des Benutzerkontos genauer erläutert.

Anmerkung

Bei der Neuanlage eines Benutzers wird dieses Recht automatisch erteilt. Sollten Sie bei der Benutzeranmeldung die Fehlermeldung „Diesem Benutzer ist keine Dialoganmeldung gestattet“ (Fehlernummer 5) erhalten, überprüfen Sie, ob dem entsprechenden Benutzer das Recht zur Dialoganmeldung in d.3 admin zugewiesen ist.

Konto ist gesperrt: Ist diese Eigenschaft erteilt bzw. zugewiesen, kann der Benutzer keinen API-Call mehr absetzen. Der Benutzer ist aber immer noch im Repository „aktiv“ und wird z. B. in d.3 smart explorer in der Liste der Benutzer bei der Dokumentenversendung aufgeführt.

Die Sperre kann u.a. durch die Überschreitung der Anzahl erlaubter Anmeldeversuche aktiviert werden.

Konto ist deaktiviert: Ist diese Eigenschaft zugewiesen, kann der Benutzer keinen API-Call mehr absetzen. Der Benutzer ist im Archiv nicht mehr „aktiv“ und wird z.B. in d.3 smart explorer in der Liste der Benutzer bei der Dokumentenversendung nicht mehr aufgeführt. Ein Benutzer kann nur dann deaktiviert werden, wenn dieser keine Dokumente mehr in seiner Bearbeitung und in seinem Postkorb hat.

Konto ist ausgeblendet: Ist diese Eigenschaft erteilt bzw. zugewiesen, gilt für den Benutzer folgendes:

- Die Authentifizierung wird vorgenommen, und eine Anmeldung für den Benutzer über d.3 login manager ist möglich.

- Dem Benutzer ist eine Dialoganmeldung gestattet.
- Der Benutzer erscheint nicht in der Empfängerliste beim Dokumentversand (Senden an d.3 Postkorb).
- Der Benutzer kann nicht als Adhoc-Vertreter ausgewählt werden.
- Der Benutzer wird nicht über die vordefinierten dynamischen Wertemengen zurückgegeben.
- Bei einer Postkorb-Versendung des Benutzers werden keine Einträge unter "Gesendet" gespeichert

Administrator-Berechtigung: Der Benutzer erhält die Berechtigung, sich an d.3 admin anzumelden. Mit dieser Berechtigung hat der Benutzer die Möglichkeit, alle administrativen Tätigkeiten durchzuführen.

Service Benutzer: Diese Benutzer werden für Dienste angelegt, die sich an das d.3 anbinden müssen, z. B. d.3 abo service oder d.3 iTrieve server.

Folgendes gilt für den Benutzer:

- Die Authentifizierung wird vorgenommen, aber für diese Benutzer ist eine Anmeldung über d.3 login manager nicht mehr möglich.
- Dem Benutzer ist keine Dialoganmeldung mehr gestattet (implizite Verweigerung). **ValidatePasswordForUser** funktioniert trotzdem.
- Das Kennwort dieses Benutzers läuft nicht ab.
- Dieser Benutzer erscheint nicht in der Empfängerliste beim Dokumentversand (Senden an d.3 Postkorb).
- Der Benutzer wird nicht über die vordefinierten dynamischen Wertemengen zurückgegeben.
- Der Benutzer kann nicht als Adhoc-Vertreter ausgewählt werden.

Authentifizierung delegieren: Dieses Recht bewirkt, dass dieser Benutzer berechtigt ist, als Aufrufer einer Benutzeranmeldung dem übergebenen Benutzer zu vertrauen. Dieses Recht dient dazu, in Zusammenhang mit Diensten die selber bereits eine Benutzer-Authentifizierung durchführen und auf d.3 zugreifen, eine doppelte Authentifizierung und damit auch die Konfiguration von Vertrauensstellungen zwischen den Diensten zu ersparen.

Funktionsaufrufe delegieren: Ruft der Benutzer API-Funktionen auf, können diese unter einer anderen Benutzerkennung ausgeführt werden. Die Benutzerkennung wird dabei über den Importparameter **vice_user** bei jeder API-Funktion angegeben.

Sub-Administrator-Berechtigung: Der Benutzer erhält die Berechtigung, sich an d.3 admin anzumelden. Mit dieser Berechtigung hat der Benutzer die Möglichkeit, ausgewählte, administrative Tätigkeiten durchzuführen. Dafür muss der Benutzer jedoch von einem Administrator die erforderlichen Sub-Administrator-Berechtigungen erhalten.

Dokumentenrechte

Rechte vererben: Gibt einem Benutzer das Recht, beim Versenden eines Dokuments in den Postkorb eines anderen Benutzers das Recht auf das Dokument zu vererben, falls der Empfänger über Dokumentklassen kein Recht auf das Dokument hat.

Das Recht kann für die Dauer der Ablage im Postkorb oder zeitbezogen vergeben werden.

Der Dokumentation zu d.3 smart explorer entnehmen Sie weitere Informationen.

Mit dem d.3 smart explorer- PlugIn ist es auch möglich, komplette Aktenstrukturen zu vererben.

Privilegiert Löschen: Wird die "Privileged Delete"-Funktionalität eines Stagesystems unterstützt, kann dieses Recht zugeordnet werden.

Mit d.3 inherit rights manager können Sie eine Übersicht über vererbte Dokumente abrufen und bei Bedarf auch die Vererbung lösen, d.h. den Zugriff auf ausgewählte Dokumente zurücknehmen.

d.3-Administration

Unterhalb **d.3 Administration** können Sie noch gezielt für von Ihnen ausgewählte Benutzer Lese- und Schreibrechte auf die einzelnen Optionen und Funktionen in d.3 admin setzen.

Policies vergeben

Erweiterte Eigenschaften über Policies vergeben Sie nach Auswahl des Rechts an Benutzer, Gruppen oder Organisationseinheiten.

Über Filtermöglichkeiten können Sie die Liste der Adressaten bequem reduzieren.



Für die ausgewählten Einträge können Sie anschließend die Rechte vergeben, wobei Sie immer daran denken müssen, dass auch hier die Standardeinstellung (Recht ignoriert) einem "Nein" entspricht, wenn in der Summe aller Zuordnungen ein explizites "Ja" nicht erteilt ist.



Nutzen Sie hierfür die Buttons **Zuweisen**, **Entziehen**, **Ignorieren** oder das Kontextmenü.

Ein einmal festgelegtes "Nein" lässt sich auch hier, genau wie bei den Dokumentklassen, nicht mehr mit einem "Ja" übersteuern.

Denken Sie ferner daran, dass Sie hier Rechte sowohl auf Benutzer, als auch auf Gruppen bzw. Organisationseinheiten-Ebene vergeben können und Sie ggf. Rechte implizit vergeben.

Planen Sie also die Vergabe der Policies gründlich und dokumentieren Sie diese.

Mit dem d.3 Administrations Plugin [Berechtigungsanalyse](#) können Sie sich immer einen Überblick über die effektiv vergebenen Rechte verschaffen. Das ersetzt allerdings niemals die gründliche Planung.

d.3 inherit rights manager

Mit Hilfe von d.3 inherit rights manager kann eine Übersicht der vererbten Dokumente abgerufen werden. Das Plugin zeigt an, wer ein Dokument an wen vererbt hat. Es bietet zusätzlich die Möglichkeit, die Vererbung zu löschen und somit den Zugriff auf das Dokument oder die Akte zu entziehen. Den Einsprung finden Sie unter den d.3 Komponenten. Wählen Sie d.3 inherit rights manager.



Zunächst werden alle Dokumente gelistet. Sie können über die Dropdownlisten aber auch nach einem Rechteerteiler, einem Rechteempfänger oder nach beidem die Liste erstellen lassen.

In der Übersicht erhalten Sie diese Informationen:

- Das Dokument (**Titel** oder **Dokument-ID**)
- Der **Rechteerteiler**, den **Rechteempfänger**
- Das **Ablaufdatum**, falls ein Zeitstempel vergeben wurde.

Zusätzlich wird noch die **Art der Vererbung** mitgeteilt, ob nur **Leserecht** oder auch **Schreibrecht** erteilt wurde.

Wenn Sie Zuordnungen löschen wollen, markieren Sie die Zuordnungen und klicken Sie auf **Löschen**.

d.3 inherit rights manager steht den Benutzern, denen die Vererbung von Dokumentrechten erlaubt wurde, auch als Plugin in d.3 smart explorer zur Verfügung. Allerdings kann dann nur nach den von diesem Benutzer vererbten Dokumenten gesucht werden, d.h. der Rechteerteiler ist nicht änderbar.

Über das vorangestellte Symbol erkennt man schnell, ob sich die Vererbung auf eine Akte oder ein Dokument bezieht. Da es bei der Vererbung von Akten möglich ist, auch die direkte Ebene unterhalb der Akte zu vererben, wird über die Checkbox **rekursiv** diese Vererbungsart angezeigt.

Wollen Sie statt des Titelfeldes die Dokument-ID in der Übersicht sehen, aktivieren Sie die Checkbox unten links (Anzeigen der Dokument-ID).

d.3 restriction set manager

Im folgenden erfahren Sie, was Sie mit d.3 restriction set manager tun können.

Berechtigungs mengen allgemein

Mit dem Einsatz der Berechtigungs mengen können viele Einzelwerte für eine Dokumentklasse als Werteliste hinterlegt werden.

Hier können verschiedene Wertekombinationen gesammelt werden und über das Makro @D3SET in der Definition der Restriktion zugeordnet werden. Der Vorteil liegt in der Reduzierung von Hook-Funktionen für die Berechtigungssteuerung, die immer dann nötig wurden, wenn sich die Restriktion für eine Eigenschaft aus verschiedenen Werten ergab, z. B. Auflistungen von Standorten, Filialen, oder verschiedene Datumswerte.

Der Begriff der Berechtigungs menge charakterisiert folgendes:

- Eine Menge definiert ein oder mehrere Filterkriterien zu einer Eigenschaft einer Dokumentklasse.
- Eine Menge kann einem Benutzer, einer Gruppe, einem Tätigkeitsprofil oder einer Organisationseinheit zugeordnet werden.
- Eine Menge wird über ein Makro (@D3SET(mengen_name)) als Filter für ein Eigenschaftsfeld in einer Dokumentklasse verwendet.
- Zur Laufzeit werden bei der Auswertung der Dokumentklassen über den Mengennamen alle Mengen zugeordnet. Die Mengen, die einem Benutzer über die direkte Benutzerzuordnung und über die Mitgliedschaft in Gruppen zugeordnet sind, werden zu einer Vereinigungsmenge zusammengefasst. Diese ermittelt die Berechtigung auf Dokumente.
- Mengen können per Sub-Administration von verschiedenen Benutzern erstellt oder geändert werden. Hierfür wird eine Erweiterung für d.3 smart explorer (Plugin: **d3setmgr.dxp**) zur Verfügung gestellt.

Die Verwendung des bisherigen Berechtigungskonzeptes (bis d.3 Version 6.1) stieß immer wieder an gewisse Grenzen.

Vielfach war die Erstellung von Dokumentklassen zu umständlich oder es wurden zur Flexibilisierung Hook-Funktionen eingesetzt, die bei der Ermittlung von Berechtigungen sehr rechenintensiv sein können.

Anmerkung

Bei der Definition der Dokumentklassen wurden häufig Eigenschaft-Einschränkungen in Form von

- Bereichen (Kostenstelle 100-200) oder
- einer Oder-Suche (Kostenstelle 100 oder 200 oder 300 oder ... oder ...)

benötigt.

Dies war bis zur d.3 Version 6.1 nicht möglich (mal abgesehen von der Bereichsangabe bei numerischen Feldern), sodass man mehrere Dokumentklassen anlegen musste.

Mit Hilfe von Berechtigungsmengen ist folgendes ab der d.3 Version 6.2 ermöglicht worden:

- Erstellung von flexibleren Filterkriterien für Eigenschaften in Dokumentklassen.
- Dynamische Zusammenstellung des Eigenschaft-Filters einer Dokumentklasse durch Vereinigung mehrerer Mengen zur Laufzeit.
- Administration von Mengen durch Sub-Administratoren, z. B. Abteilungsleitern oder KeyUsers.

Anwendungsfälle

Nachfolgend finden Sie ein paar Anwendungsbeispiele.

Beispiel 1: Zugriffsbeschränkung auf Dokumentarten

Die Dokumentart „Rechnung“ enthält ein Feld „Kostenstelle“. Dieses Feld kann Werte von „100“ bis „999“ enthalten. Anhand dieses Feldes sollen in d.3 Berechtigungen aufgebaut werden.

Dazu wird eine Dokumentklasse „Rechnungszugriff über Kostenstelle“ erstellt.

Für das Feld „Kostenstelle“ wird als Filter die Menge „Kostenstelle“ über das Makro @D3SET(Kostenstelle) angegeben.

Im d.3-System wurde die Menge „Kostenstelle“ angelegt.

Einem Benutzer „user1“ wird die Dokumentklasse „Rechnungszugriff über Kostenstelle“ über Berechtigungsprofile oder über eine direkte Zuordnung zur Dokumentklasse zugewiesen. Zusätzlich ist dieser Mitglied der Gruppe „Abteilung1“.

Solange diese Menge keine Filterkriterien enthält, kann „user1“ entsprechend seiner anderen Berechtigungen (Gruppenzugehörigkeit, Zuweisung von Dokumentklassen/Berechtigungsprofilen) ganz normal auf die Dokumente von „Rechnung“ zugreifen.

Im ersten Schritt weist man jetzt der Gruppe „Abteilung1“ die Menge „Kostenstelle“ zu und definiert dort die Filterkriterien „100;200-400“. Mitglieder der Gruppe „Abteilung1“ haben jetzt nur noch Zugriff auf die Rechnungen mit den Kostenstellen 100 und 200 bis 400.

Wenn jetzt ein Benutzer, der Mitglied der Gruppe „Abteilung1“ ist, auf Dokumente der Dokumentart „Rechnung“ zugreifen möchte, wird dieser nur die Dokumente sehen, bei denen das Eigenschaftsfeld „Kostenstelle“ die Werte 100 oder 200-400 enthält.

Im nächsten Schritt weist man dem Benutzer „user1“ direkt die Menge „Kostenstelle“ zu, und zwar mit den Filterkriterien „!300;500“. Es wird also eine 2. Wertezuordnung zur Menge erstellt.

Anmerkung

Das "!" (NICHT) muss in der d.3- Konfiguration unter Retrieval_Verhalten definiert sein.

Möchte der Benutzer „user1“ jetzt auf Dokumente der Dokumentart „Rechnung“ zugreifen, wird über die Dokumentklasse „Rechnungszugriff über Kostenstelle“ eine Vereinigungsmenge über alle Mengen mit dem Namen „Kostenstelle“ gebildet.

Der Benutzer „user1“ bekommt also nur Zugriff auf Rechnungen mit den Kostenstellen 100, 200-400 und 500, aber nicht auf Rechnungen mit der Kostenstelle 300.

Beispiel 2: Berechtigungsverwaltung über Mengen

Im Beispiel 1 können Sie sehen, dass man die Berechtigungen für Benutzer gezielt durch Zuordnungen von Mengen erteilen oder verweigern kann.

Durch den Einsatz von Mengen ist es möglich, solche Berechtigungen durch berechtigte Benutzer über den d.3 smart explorer zu erstellen bzw. Benutzern zuzuweisen.

Das könnte so aussehen:

Man definiert eine Dokumentklasse „Verwaltung der Menge Kostenstelle“, die auf der Dokumentart aufbaut, in der die Mengen gespeichert werden. Diese Dokumentart enthält als Eigenschaft unter anderem den Namen der Menge und das Objekt (z. B. Benutzername, Gruppenname), dem diese Menge zugeordnet ist. Als Filter der Dokumentklasse gibt man z. B. den Mengennamen „Kostenstelle“ an. Für das Objekt kann man entweder einen Benutzernamen, oder auch wieder eine andere Menge per @D3SET(...) angeben, die dann mehrere Benutzernamen enthält.

Somit lassen sich Berechtigungen auf die Erstellung oder Änderung von Mengen geben, die dann benutzt werden können, um Benutzern Rechte zu erteilen oder zu verweigern.

Beispiel 3: Anwendung von Restriktionsmengen

Ein weiteres Beispiel für die Anwendung von Restriktionsmengen finden Sie im Anhang unter [Beispiel für Berechtigungsmengen](#).

Speicherung von Mengen

Die Berechtigungsmengen werden in Form von Dokumenten in der Dokumentart \$Restrictionset\$ gespeichert. Dadurch wird ein einfacher Aufbau eines Berechtigungskonzepts für die Bearbeitung von Mengen ermöglicht, da über Dokumentklassen und Berechtigungsprofile Rechte auf diese Dokumente vergeben werden können.

Eine Auflistung der Mengen im System wird in der Datenbank gehalten, wobei dort zusätzlich, sprachabhängig, noch ein beschreibender Text zu der Menge abgelegt ist.

Bei den Restriktionsmengen gibt es keine Versionierung in Form der Nutzdateien (da es keine Nutzdateien gibt), sondern nur seitens der Eigenschaften, die in der Eigenschaftshistorie oder im Audit-Trail eingesehen werden können.

Anlegen von Mengen

1. Über die Auswahl des Plugins d.3 restriction set manager öffnen Sie den Dialog zur Erstellung und Verwaltung von Berechtigungsmengen.
2. Über den Button **Anlegen** erstellen Sie zunächst die Menge, indem Sie einen sprechenden Namen vergeben. Sie können eine Erläuterung zur Menge hinterlegen.



3. Tragen Sie einen eindeutigen Namen sowie erklärende Hinweise ein:



Betrachten Sie diese angelegte Menge als Container für Werte gegen die später zur Laufzeit der Eigenschaftswert geprüft werden soll.

Diese angelegten Mengen können nun in der [Dokumentklassendefinition](#) über das Makro @D3SET (im Beispiel: PLZ 48000 - 49000) genutzt werden.

Werte der Menge zuordnen

Im rechten Bereich **Mengen-Zuordnungen** kann über den Button **Anlegen** eine Zuordnung erstellt werden.



Zugeordnet: Hier ordnen Sie den Filter, also die Menge der erlaubten und nicht erlaubten Werte, einer der gelisteten Ebenen zu. Je nach Zuordnungsebene wird diese Berechtigungsmenge nur in die Ermittlung der realen Berechtigung einfließen, wenn der Benutzer:

- in der **Gruppe** oder
- in der **Organisationseinheit** Mitglied ist oder
- ihm der Filter direkt zugeordnet wurde.

Wählen Sie den Punkt **Keine Zuordnung**, wenn Sie die Kriterien allgemein - als Basiswerte - nutzen wollen.

Filter: Hier sammeln Sie alle erlaubten oder nicht erlaubten Werte. Für die Auflistung stehen Ihnen die von Ihnen zu definierenden Sonderzeichen (siehe Kapitel [d.3-Retrieval-Verhalten](#)) zur Verfügung.

Sie können eine Negation immer über das intern vergebene Zeichen "!" erstellen. Da erst zur Laufzeit eine Liste aller Vergleichs-Werte ermittelt wird, ist die Positionierung des negierten Eintrags freigestellt. Es gilt aber: ein negierter Wert lässt sich nicht durch mehrere positive Zuordnungen übersteuern.

Sie können die Ausdrücke zeilenweise erfassen oder das von Ihnen definierte ODER-Zeichen nutzen. Insgesamt können Sie 150.000 Zeichen für Ihre Filterkriterien nutzen.

Erst mit der Zuordnung der Klasse (implizit zum Benutzer oder explizit über ein Berechtigungsprofil) wird die konkrete Berechtigung festgelegt. Die tatsächliche Berechtigung hängt also entscheidend davon ab, in welcher Gruppe oder Organisationseinheit ein Mitarbeiter enthalten ist, oder ob eine Werteauflistung einem Benutzer direkt zugeordnet wurde.

Makros bei Mengen

Bei der Erstellung der Filter für Mengen können Sie folgende Makros einsetzen, die Sie auch bei den Dokumentklassen nutzen können:

@D3USER

@D3GROUP

@D3USER_OPTFIELD_XX

@D3USER_LDAPDN

@D3REGEXPR

@D3SET (Vorsicht)

@D3USER_REALNAME

@D3USER_LONG

Erstellung bzw. Aktualisierung von Mengen über den Hostimport

Mit der d.3 Version 6.3 von d.3 server können Restriktionsmengen auch über den Hostimport erstellt werden.

Konfiguration

Mit dem Parameter **D3SET_IMPORT_PATH** wird ein Verzeichnis für den Hostimport-Prozess definiert, aus dem die Mengen-Definitions-Dateien eingelesen werden. Dieser Parameter kann über d.3 config in d.3 admin gesetzt werden. Als Dateierweiterung für solche Filter-Dateien wird dabei automatisch `TEXT` verwendet.

Bereitstellung der Import-Dateien

Wie bei einem normalen Hostimport-Ablauf werden auch hier eine JPL-Datei und eine Nutzdatei benötigt. Die Nutzdatei bekommt dabei die Dateierweiterung TXT (siehe oben).

Folgende Parameter sind in der JPL-Datei zu setzen:

set_name

enthält dabei den Kurznamen der Restriktionsmenge und ist ein Pflichtparameter

set_object

enthält das Objekt, dem die Mengenfilter zugeordnet werden sollen. Dabei kann folgendes angegeben werden:

- ein Benutzername
- ein Gruppenname
- ein Tätigkeitsprofilname oder
- ein Organisationseinheitsname

Der Parameter kann auf Leerstring gesetzt werden oder auch weggelassen werden. In diesem Fall wird eine Menge ohne direkte Objektzuordnung erstellt bzw. geändert.

Die TXT-Datei enthält die Filterkriterien, die entweder durch ein „;“ voneinander getrennt werden oder jeweils in einer neuen Zeile stehen.

Anmerkung

Bestehende Mengen-Filter werden beim Hostimport überschrieben. Es muss also immer der komplette Filter in der TXT -Datei angegeben werden.

Restriktionsmengen, die es noch **nicht** gibt, werden nicht angelegt. Der Parameter **set_name** muss also immer den Namen der schon existierenden Menge enthalten.

Verwaltung von Mengen durch andere Personen

Die erstellten Restriktionsmengen können von berechtigten Personen administriert werden, d.h. es können Werte hinzugefügt oder gelöscht/korrigiert werden. Dies kann z. B. eine Aufgabe eines Abteilungsleiters oder Bereichsleiters sein, der die Aufgaben eines Mitarbeiters oder einer Gruppe kurzzeitig, bzw. auch langfristig anpassen möchte. Eine Restriktionsmenge kann grundsätzlich auch leer angelegt und erst vom Verantwortlichen mit konkreten Einträgen den Aufgaben entsprechend versorgt werden.

Für diese Tätigkeit ist eine Dokumentklasse mit entsprechenden Zuordnungen und Rechten zu erstellen.

Erstellen einer Dokumentklasse für die Administration von Mengen

Zunächst legen Sie eine neue Dokumentklasse für die Systemdokumentart \$RestrictionSet\$ wie gewohnt an.

Warnung

Die System- und Standardklassen stehen nur bei ausgeschaltetem Flag zur Verfügung.

Die Eigenschaften der System-Dokumentart \$Restriction Set\$ haben die folgende Bedeutung:

- \$Set_Name\$: Name der Restriktionsmenge(n) (z. B. PLZ 48000 - 48999), für die die externe Administration erfolgen soll.
- \$Object\$: Objekt, auf das der Zugriff über diese Klasse erfolgen soll, z. B. die Menge(n) des Benutzers cc, der Gruppe Einkauf oder Organisationseinheit Abt. Buchhaltung (wie in den Beispielen weiter oben). Hier können Sie ebenfalls eine definierte Restriktionsmenge angeben, die alle Benutzer, Gruppen, Organisationseinheiten etc. enthält, auf die eine Sub-Administration ermöglicht werden soll.

- `$Object-Class$`: der Zuordnungsbereich der Menge

0: keine Zuordnung

1: Benutzer

2: Gruppe

4: Organisationseinheit

Anmerkung

Bei einem Update des d.3- Repository auf die neue Version wird der Wert "3" für ein Tätigkeitsprofil (vor d.3 Version 7) automatisch auf den Wert "2" umgesetzt.

Der Datentyp `$Object-Class$` ist numerisch, sodass auch eine Bereichsangabe möglich ist (1-3, -2, 2-).

Sie können direkt kombinieren, so wie Sie es von den „normalen“ Dokumentarten her kennen. Es werden nur die eingetragenen Werte den Restriktionen zugeordnet.

Im obigen Beispiel wird der Zugriff auf die Restriktionsmenge "PLZ 48000 - 48999" definiert, allerdings nur die Mengen der Benutzer.

Beispiele für weitere Zuordnungen:

Tragen Sie als Wert für `$Object-Class$` nur den Wert "2" ein und lassen alle weiteren Felder leer, kann die berechnete Person, der diese Dokumentklasse später zugeordnet wird, auf alle Mengen, die Gruppen zugeordnet sind, zugreifen bzw. eben nicht. Denken Sie daran, dass hier nur die Vergleichswerte erfasst werden, die Berechtigung aber erst in der Zuordnung der Dokumentklasse vergeben oder verweigert wird.

Die Zuordnung des Zugriffs kann auch über eine Menge gesteuert werden. Hierzu kann eine Menge, z. B. "Meine Mitarbeiter" angelegt werden.

Ob der Zugriff nun gestattet oder verboten wird, wird nach wie vor erst in der Rechtezuordnung (Berechtigungsprofil bzw. Dokumentklassen-Zuordnung) getroffen ("Recht erteilt"/"Recht verweigert"/"Recht ignoriert").

Die Menge wird dann in der Dokumentklassen-Restriktion ausgewählt und zugeordnet.

Die Dokumentklasse zur Mengenverwaltung wird über die üblichen Mechanismen entweder über ein Profil oder eine direkte Zuordnung einem Mitarbeiter zugeordnet und mit entsprechenden Rechten versehen (Lesen, Schreiben).

Anmerkung

Es ist sogar möglich, eine Restriktionsmenge zu erstellen, in der die Namen von Restriktionsmengen stehen. Diese kann dann als Wert im Feld `$Set-Name$` über das Makro `@D3SET(xxxxxx)` referenziert werden. Eine Schachtelung von Restriktionsmengen ist somit bedingt möglich.

Mengenadministration über d.3 smart explorer Plugin

Für d.3 smart explorer muss das DXP `d3setmgr.dxp` (zu finden unter `...\d3client.prg\DXP`) über die Clientverteilung bereitgestellt werden. Unter dem Menüpunkt **Werkzeuge** kann dann für berechnete Personen die Restriktionsmengenverwaltung aufgerufen werden.

Über das installierte Plugin von d.3 smart explorer können die berechtigten Personen allerdings dann nur die ihnen zugeordneten Restriktionsmengen verwalten.

Der angemeldete Benutzer kann also die Mengen für die Benutzer oder Gruppen abändern und den entsprechenden Aufgaben anpassen.

Er kann aber keine neue Menge anlegen.

Wasserzeichen

Seit Version 8.1.0 unterstützt d.3 server das Anzeigen von Dokumenten mit einem automatisch aufgerollten Wasserzeichen. Die gleichzeitige Nutzung von d.ecs sign und Wasserzeichen in d.3 ist derzeit noch nicht unterstützt.

Es können dabei mehrere Wasserzeichen definiert und Dokumentklassen zugewiesen werden. Dadurch werden bei der Anzeige eines Dokumentes die Wasserzeichen anhand der Zugehörigkeit eines Dokumentes zu Dokumentklassen mit der Nutzdatei verrechnet.

Beachten Sie Folgendes beim Einsatz von der Erweiterung **hashcheck.dxp**:

Wenn mithilfe der Wasserzeichenfunktionalität in d.3 server auf das Dokument ein Wasserzeichen hinzugefügt wird, stellt das **hashcheck.dxp** eine Änderung fest und gibt eine entsprechende Meldung aus.

Aktivierung der Wasserzeichenunterstützung

Über den d.3-Konfigurationsparameter **WATERMARK_SUPPORT** kann die allgemeine Unterstützung für die Anzeige mit Wasserzeichen aktiviert werden.

Man findet diesen Parameter in d.3 config unter **Sonstige Parameter**.

Mit dem Aktivieren des Parameters können Sie Benutzern mittels des Dokumentklassenrechtes "Anzeige mit Wasserzeichen" die Eigenschaft zuweisen, dass diese Benutzer nur Dokumente mit Wasserzeichen anschauen dürfen.

Anmerkung

- Eine Installation von d.ecs pdf extension Version 1.4.2 oder höher ist erforderlich.
- Es wird die zentrale Installation empfohlen.
- Nach Neuinstallation wird ein Neustart des Rechners empfohlen, damit die d.3-Prozesse wieder erfolgreich starten.
- Die Anzeige mit Wasserzeichen funktioniert nur mit dem deaktivierten Schalter **V8RunningUpdateBackComp**.
- Die Anzeige mit Wasserzeichen gilt nur für Dokumente, die im PDF-Format abgelegt sind.

Warnung

Wenn der Parameter **WATERMARK_SUPPORT** aktiviert aber d.ces pdf extension nicht installiert wurde oder in einer Version kleiner als 1.4.2 vorliegt, können die d.3-Prozesse nicht mehr gestartet werden!

Anzeige von Dokumenten mit Wasserzeichen

Wenn bei der Rechteprüfung für den Benutzer festgestellt wird, dass das Recht "Anzeigen mit Wasserzeichen" erteilt ist und die Datei, die zur Anzeige gebracht werden soll, eine PDF-Datei ist (Nutzdatei ist PDF oder abhängige Datei ist P1), wird bei der Anforderung der Datei über das d.3 gateway eine Routine zur Aufbringung von Wasserzeichen durchlaufen.

Dabei werden alle Dokumentklassen ermittelt, die das Dokument treffen. Daraus folgt dann eine Liste der Wasserzeichen, die diesen Dokumentklassen zugeordnet sind.

Anmerkung

Ein Anwender, der das Bearbeitungsrecht auf der Dokumentklasse besitzt, bekommt im Status Bearbeitung immer das Original-Dokument ohne Wasserzeichen angezeigt, da nur dieses verändert werden darf. Diese Anwender bekommen auch in den anderen Status das Original ohne Wasserzeichen angezeigt, wenn es kein PDF ist und die asynchrone Erzeugung der abhängigen P1-Datei noch nicht abgeschlossen ist.

Als Folge daraus muss Anwendern, die das Dokument nie ohne Wasserzeichen sehen dürfen, das Bearbeitungsrecht auf der Dokumentklasse entzogen werden. In diesem Fall ist eine Anzeige des Dokuments nicht möglich, wenn es selbst keine PDF-Datei ist und die Erzeugung der abhängigen P1-Datei noch nicht abgeschlossen ist.

Wenn keine Wasserzeichen-Zuordnung gefunden wurde, werden automatisch 2 Standard-Wasserzeichen generiert, so dass immer sichergestellt ist, dass ein Wasserzeichen aufgetragen wird.

Nach der Aufbringung der Wasserzeichen wird die generierte Datei in einem temporären Bereich des d.3-Dokumentenbaumes abgelegt und bereitgestellt. Diese Datei ist für 15 Minuten gültig. Wenn also ein weiterer Download des Dokumentes innerhalb von 15 Minuten nach der Generierung stattfinden soll, kann das Dokument direkt bereitgestellt werden. Ansonsten wird die Wasserzeichen-Generierung erneut ausgeführt.

Der Master-Async löscht automatisch die temporären Wasserzeichen-Datei, die in den letzten 5 Tagen erzeugt wurden.

Einschränkung bei der Nutzung von Wasserzeichen mit d.3 mobile

Folgende Einschränkungen sind in d.3 mobile im Offline-Bereich bei der Nutzung von Dokumenten mit Wasserzeichen zu beachten:

1. Offline gespeicherte Dokumente mit Wasserzeichen, wobei ein Zeitstempel des Download-Zeitpunktes als Wasserzeichen aufgebracht wird, werden nicht mehr aktualisiert.
Über den Aufruf "**Jetzt bereitstellen**" in der d.3 mobile App wird dieser Zeitstempel auf dem Dokument nicht aktualisiert, weil das Dokument nicht erneut heruntergeladen wird.
2. Bei Änderungen von Benutzer-Eigenschaften, welche mit einem Wasserzeichen aufgebracht wurden, werden als offline bereitgestelltes Dokument nicht aktualisiert.
Über den Aufruf "**Jetzt bereitstellen**" in der d.3 mobile App wird keine Änderung einer Benutzer-Eigenschaft angezeigt, weil das Dokument nicht erneut heruntergeladen wird.
3. Bei einer Änderung an der Wasserzeichen-Konfiguration werden offline bereitgestellte Dokumente mit Wasserzeichen nicht aktualisiert.
Die Änderung wird im Offline-Bereich nicht angezeigt. Auch der Aufruf "**Jetzt bereitstellen**" in d.3 mobile führt nicht dazu, dass diese Änderung sichtbar wird, weil das Dokument nicht erneut heruntergeladen wird.

Workaround in der d.3 mobile App:

Um für diese Dokumente im Offline-Bereich ein aktuelles Wasserzeichen zu erhalten, ist es notwendig das Dokument aus dem Offline-Bereich zu entfernen und wieder hinzuzufügen.

Dazu kann wie folgt vorgegangen werden:

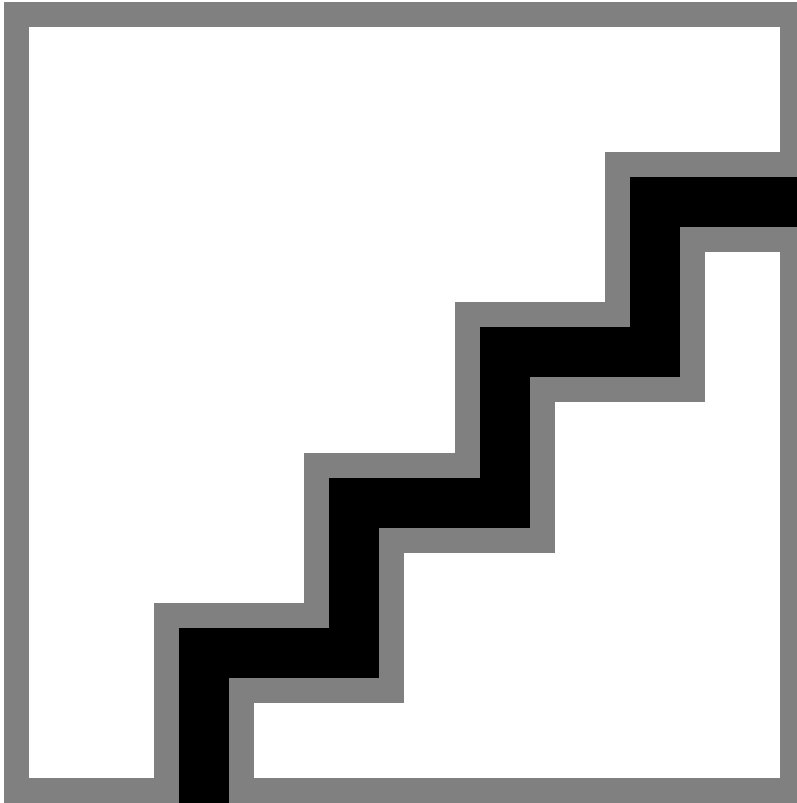
1. Das zu aktualisierende Dokument/die Akte im Offline-Bereich identifizieren und z.B. die Dokument-ID merken.
2. Im Offline-Bereich für das Dokument/die Akte den Menüpunkt "**vom Gerät entfernen**" aufrufen.
3. Das Dokument/die Akte über die Suche nach der Dokument-ID wiederfinden und erneut offline verfügbar machen.

Warnung

Vorausgesetzt wird der Einsatz der Softwareversionen d.3 mobile 1.6.0 und d.3 document render service 1.3.0.

Erstellen und Verwalten von Wasserzeichen

Öffnen Sie den Dialog zur Erstellung und Verwaltung von Wasserzeichen über die Auswahl des Plugins **Wasserzeichen**.



Wasserzeichen erstellen

Um ein neues Wasserzeichen zu erstellen, betätigen Sie die Schaltfläche **Neu** in der Übersicht.

Allgemeine Einstellungen

Über die Kategorie **Allgemein** werden Grundeinstellungen des Wasserzeichens festgelegt. Diese Kategorie öffnet sich automatisch, wenn **Neu** gedrückt wurde.



Geben Sie einen **Namen** zum Wasserzeichen ein. Diese Information hat nur administrativen Charakter und wird außerhalb von d.3 admin nicht angezeigt. Der Name kann maximal 50 Zeichen lang sein.

Im **Text**-Feld müssen die Bestandteile des Textes für die Anzeige des Wasserzeichens definiert werden.

Dabei wird die Open-Source Template Sprache "Liquid" unterstützt. Näheres dazu kann man den Seiten <https://shopify.github.io/liquid/> oder <https://github.com/shopify/liquid/wiki/Liquid-for-Designers> entnehmen. Es können auch Eigenschaften des d.3-Dokumentes oder des d.3-Benutzers in den Text aufgenommen werden. Diese Eigenschaften müssen innerhalb der Zeichenkette `{{...}}` eingetragen werden.

Mögliche Eigenschaften für ein Dokument sind:

Eigenschaft	Beschreibung	Syntax
doc_id	Dokument-ID	{{doc.doc_id}}
number	Dokumentnummer	{{doc.number}}
current_status	aktueller Status des Dokumentes	{{doc.current_status}}
file_id_current_vers	aktuelle Dateiversion des Dokumentes	{{doc.file_id_current_vers}}
current_version_id	aktuelle Versionsnummer des Dokumentes	{{doc.current_version_id}}
editor	Bearbeiter des Dokumentes	{{doc.editor}}
field[...]	Eigenschaftsfelder 1-59 und 70-89	{{doc.field[15]}}
field[6].[...]	Mehrfacheigenschaftsfelder 60-69	{{doc.field[60][15]}}

Mögliche Eigenschaften für einen Benutzer sind:

Eigenschaft	Beschreibung	Syntax
id	Benutzerkennung in d.3	{{user.id}}
long_name	Anmeldename in d.3	{{user.long_name}}
name	vollständiger Name des Benutzers	{{user.name}}
plant	Abteilung	{{user.plant}}
department	Organisation	{{user.department}}
opt_field[...]	optionales Feld des Benutzers	{{user.opt_field[1]}}

Beispiele:

{{doc.field[1]}} zeigt den Wert des d.3-Dokumentes aus dem Eigenschaftsfeld an der Datenbank-Position 1 an.

{{user.name}} zeigt den vollständigen Namen des d.3-Benutzers an.

Mit Aktivierung der Option **Fallback-Wasserzeichen** können Sie einstellen, dass dieses Wasserzeichen dann angezeigt wird, wenn für das Dokument kein anderes Wasserzeichen ermittelt werden konnte.

Bei Aktivierung der Option **Wasserzeichen immer anzeigen** wird dieses Wasserzeichen in jedem Fall verrechnet und zur Anzeige gebracht, auch wenn schon andere Wasserzeichen auf das Dokument aufgebracht werden.

Textoptionen

In der Kategorie **Textoptionen** tätigen Sie Einstellungen zum Wasserzeichentext:



Folgende Optionen stehen dabei zur Verfügung:

Farbe: Hiermit wird die Farbe des Wasserzeichens festgelegt. Folgende Farben sind möglich:

- 0: Schwarz
- 1: Rot
- 2: Grün
- 3: Blau

Deckkraft: Hiermit wird die Deckkraft bzw. Transparenz des Wasserzeichens festgelegt. Die Angabe erfolgt in Prozent. Je höher der Wert, desto kräftiger wird das Wasserzeichen dargestellt. Der Wert 0 führt dann zu einer transparenten und der Wert 100 zu einer deckenden Darstellung.

Skalierung: Hiermit wird die prozentuale Größe des Wasserzeichens im Verhältnis zur Seite gesteuert. Mit dem Wert 100 erstreckt sich das Wasserzeichen über die gesamte Breite bzw. Länge des Dokumentes.

Ausrichtung

In der Kategorie **Ausrichtung** positionieren Sie den Text des Wasserzeichens.



Über **Position** legen Sie die horizontale und vertikale Position des Textes fest. Dabei stehen 9 Ankerpunkte zur Verfügung.

Über die horizontale Position gelten folgende Regeln:

- Links: Der Text beginnt am linken Rand des Dokuments.
- Mitte: Die Mitte des Textes befindet sich in der Mitte des Dokuments.
- Rechts: Der Text endet am rechten Rand des Dokuments.

Über die vertikale Position gelten folgende Regeln:

- Oben: Der Text beginnt oder endet am oberen Rand des Dokuments (abhängig von der konfigurierten Rotation).
- Mitte: Die Mitte des Textes befindet sich in der Mitte des Dokuments.
- Unten: Der Text beginnt oder endet am unteren Rand des Dokuments (abhängig von der konfigurierten Rotation).

In der Sektion **Verschiebung** wird die Position des Wasserzeichens prozentual zur Seitenbreite bzw. Seitenhöhe festgelegt.

Horizontal: Dieser Parameter legt die horizontale Verschiebung der Position des Wasserzeichens prozentual zur Seitenbreite fest.

Mit einem negativen Wert wird die Position nach links und mit einem positiven Wert nach rechts verschoben.

Anmerkung

Negative Werte können den Text oder Teile des Textes nach links, positive Werte nach rechts aus dem Dokument herausrücken!

Vertikal: Dieser Parameter legt die vertikale Verschiebung der Position des Wasserzeichens prozentual zur Seitenhöhe fest.

Mit einem negativen Wert wird die Position nach oben und mit einem positiven Wert nach unten verschoben.

Anmerkung

Negative Werte können den Text oder Teile des Textes nach oben, positive Werte nach unten aus dem Dokument herausrücken!

Über **Rotation** wird die Drehung des Wasserzeichens gegen den Uhrzeigersinn gesteuert. Die Angabe erfolgt in Grad. Mit dem Wert 0 erscheint das Wasserzeichen waagrecht, mit dem Wert 90 senkrecht.

Dokumentklassen

In der Kategorie **Dokumentklassen** legen Sie fest, für welche Dokumentklassen das Wasserzeichen angezeigt werden soll. Näheres dazu können Sie dem Kapitel [Anzeige von Dokumenten mit Wasserzeichen](#) entnehmen.



Die Übersicht zeigt die ausgewählten Dokumentklassen an.

Über **Hinzufügen** können neue Dokumentklassen ausgewählt oder bestehende entfernt werden. Folgendes Fenster erscheint dabei:



Über **Entfernen** können Dokumentklassen auch direkt abgewählt werden. Dabei ist eine Mehrfachauswahl möglich.

Änderungen übernehmen oder zurücksetzen

Wenn Änderungen vorgenommen wurden, werden automatisch die Knöpfe Übernehmen und Zurücksetzen freigegeben.

Mit Übernehmen werden die Änderungen gesichert aber noch nicht zum d.3-Server gesendet. In der Übersicht erscheint der Name des Wasserzeichen in kursiv und fett, wenn ein bestehendes Wasserzeichen geändert wurde und in **fett**, wenn ein Wasserzeichen neu erstellt wurde.

Mit Zurücksetzen werden die Änderungen rückgängig gemacht und auf den Stand vom Start des Plugins bzw. auf den Stand nach der letzten Speicherung der Änderungen gebracht.

Änderungen speichern

Um alle Änderungen an den Wasserzeichen dauerhaft zu sichern, betätigt man die Schaltfläche Speichern.

Wasserzeichen ändern

Um ein bestehendes Wasserzeichen zu ändern, markieren Sie dieses in der Übersicht.

Über **Suchen nach** können auch gezielt Wasserzeichen anhand des Namens gesucht werden.

Dabei wird die Liste per Volltextsuche case insensitive auf die Ergebnisse zusammengeschrumpft.

Markieren Sie ein Wasserzeichen, öffnet sich automatisch die Kategorie **Textoptionen**.

Das weitere Vorgehen ist dann genauso, wie im Kapitel [Wasserzeichen erstellen](#) beschrieben.

Wasserzeichen löschen

Um ein bestehendes Wasserzeichen zu löschen, markieren Sie dieses in der Übersicht und betätigen Sie die Schaltfläche **Entfernen**.

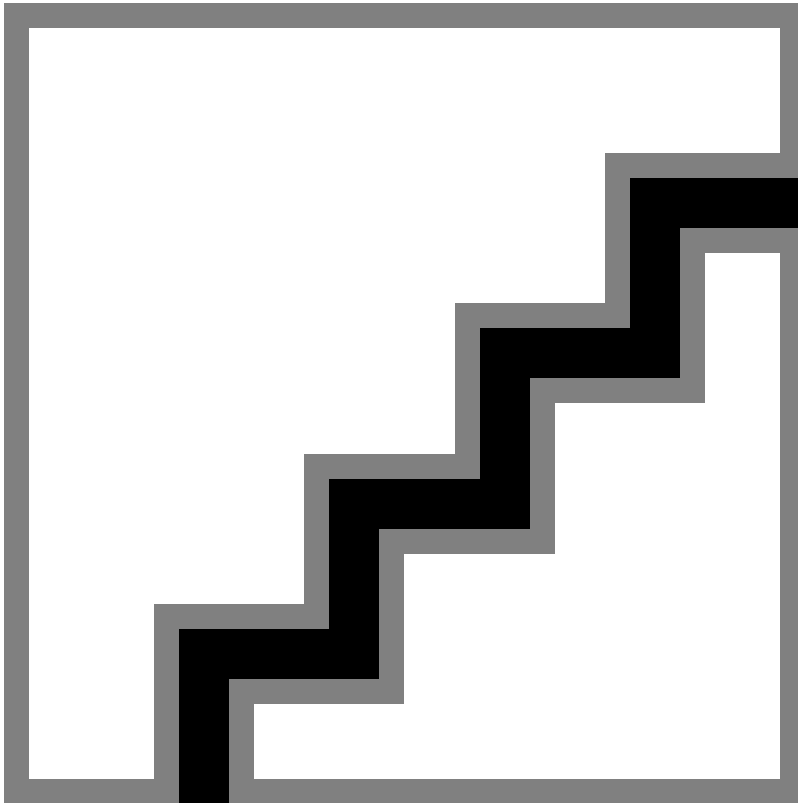
Das Wasserzeichen wird daraufhin nur zum Löschen markiert und erscheint durchgestrichen.

Erst, wenn Sie die **Speichern**-Schaltfläche betätigen, wird das Wasserzeichen dauerhaft gelöscht.

Solange Sie die Schaltfläche **Speichern** noch nicht gedrückt haben, können Sie den Löschvorgang per **Zurücksetzen** widerrufen. Ein Wasserzeichen, welches zum Startzeitpunkt noch nicht existierte, wird allerdings aus der Liste entfernt und steht somit nicht mehr zur Verfügung.

Vorschau

Um Einstellungen an Wasserzeichen besser prüfen zu können, können Sie die Vorschaufunktion des Plugins nutzen.



Diese befindet sich im oberen rechten Bereich des Plugins und kann mittels der Schaltfläche **Vorschau** verwendet werden. Die Vorschau kann nur dann verwendet werden, wenn Sie ein Wasserzeichen in der Übersicht ausgewählt haben.

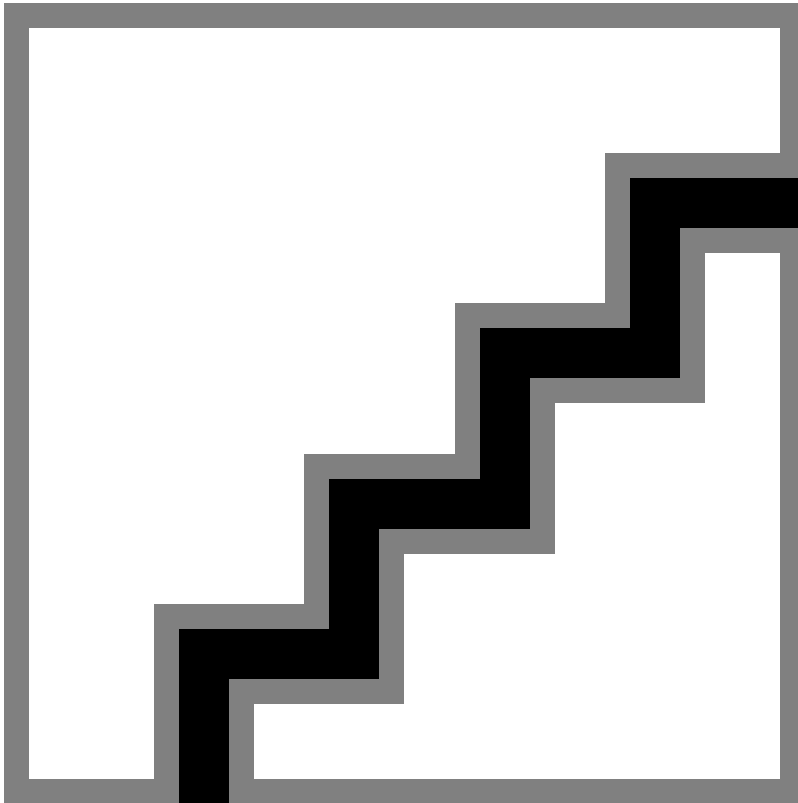
Die Vorschau kann nur für im d.3-System befindliche Dokumente ausgeführt werden. Suchen Sie sich also zunächst PDF-Dokumente mittels der Dokument-ID aus dem d.3-System aus, an denen Sie die Wasserzeichen ausprobieren wollen.

Die d.3-Dokument-ID muss in das Feld **Dokument** eingegeben werden.

Im Feld **Benutzer** tragen Sie die ID eines d.3-Benutzers ein, in dessen Namen Sie das Wasserzeichen verrechnen wollen.

Über das Optionsfeld **Simulation** können Sie zusätzlich zum ausgewählten Wasserzeichen noch die schon im d.3-System gespeicherten Wasserzeichen mit verrechnen lassen. Dabei werden die Dokumentklassen des angegebenen d.3-Dokumentes ermittelt und die diesen zugeordneten Wasserzeichen eingerechnet.

Durch betätigen des Knopfes **Vorschau** wird eine Anfrage zur Erstellung des Vorschaudokumentes zum d.3-Server gesendet und nach erfolgreicher Verarbeitung das Dokument heruntergeladen und im Vorschaubereich angezeigt.



Im Vorschaufenster können Sie das Dokument vergrößern, im Dokument blättern oder das Dokument auf Vollbild vergrößern.

1.4.4. Systemeinstellungen

Verzeichnisstruktur

Dokumente im d.3 -Repository können in verschiedenen Verzeichnissen auf dem d.3- Server liegen. Dieses Kapitel beschreibt die Unterschiede.

Anmerkung

Die Verzeichnisnamen sind aus der Sicht des d.3- Servers zu betrachten. Damit ist der Rechner gemeint, auf welchem die d.3- Serverprozesse (hostimp, d3async und d3server) aktiv sind.

Wenn also als Verzeichnis C:\D3\D3.DOK\..... angezeigt wird, dann ist dies das Laufwerk C:\ auf dem d.3-Server. Somit machen die Schalter zum Auswählen eines Verzeichnisses auch nur Sinn, wenn d.3 admin auf dem d.3-Server gestartet wurde.

Verzeichnisse



Anmerkung

Mit der d.3 Version 8.0 wurde die Verzeichnisstruktur bzw. die Struktur des Dokumentbaums geändert, damit Dateikopiervorgänge minimiert werden. So ist nun ein "lebenslang" stabiler Ablageort gegeben und es finden keine Dateioperationen mehr beim Statustransfer statt. Alle 100 Dokument-IDs wird ein neues Unterverzeichnis erstellt. Der Dateiaufbau lautet: doc_id.file_id+abh. Erweiterung. Die file_id entspricht dabei nicht jeder Dokumentversion 1:1, d.h. es kann Lücken bei den Nummern im Dateisystem geben.

Grundsätzlich landen **Dokumente** standardmäßig im Verzeichnis C:\d3\D3P.dok\docs.

Dokumente im Zwischenspeicher sind unter C:\d3\D3P.dok\cached_docs zu finden.

Geteilte Dateien liegen im Verzeichnis C:\d3\D3P.dok\share.

Der **Sekundärspeicher** befindet sich unter C:\d3\D3P.dok\Jukebox.

Anmerkung

Die Verzeichnisse lassen sich durch manueller Eingabe im Adressfeld oder durch einen Klick auf das jeweilige Symbol rechts davon ändern.

Alte Verzeichnisse

Die nachfolgenden Verzeichnisse wurden in früheren Versionen von d.3 (vor 8.0) genutzt.



Bearbeitung

Jeder Benutzer und jede Gruppe erhält ein eigenes Bearbeitungsverzeichnis.

Archivieren Sie beispielsweise die Datei TEST.DOC in die Bearbeitung des Benutzers USER, dann wird das Dokument auf dem Fileserver in dem Verzeichnis F:\d3\d3.dok\bearbeit\user als A0000001.DOC abgelegt.

Angenommen, das Dokument hat beim Ablegen die Dokumenten ID F0000001 erhalten und Ihre d.3-Verzeichnisstruktur befindet sich unter F:\d3\d3.dok.

(DIESE ANNAHME WIRD AUCH WEITER VERWENDET).

Ebenso verhält sich der Vorgang, wenn Sie das Dokument in die Bearbeitung einer Gruppe archivieren (z.B. F:\d3\d3.dok\bearbeit\gruppe).

Prüfung

Wird das zuvor archivierte Dokument mit d.3 smart explorer nun in den Status "Prüfung" verschoben, dann wird auch das Dokument in das entsprechende Verzeichnis verschoben.

Das Dokument finden Sie dann unter F:\d3\d3.dok\pruefung.

Freigabe

Ist dieses Dokument nun geprüft und kann in die Freigabe verschoben worden, wird das Dokument in das Verzeichnis F:\d3\d3.dok\public\A000 transferiert.

Wie Sie erkennen können, wird das Dokument nicht direkt in das **PUBLIC**-Verzeichnis verschoben, sondern dort in das Unterverzeichnis **A000**.

Diese Unterverzeichnisse werden vom d.3-System automatisch angelegt. Der Grund für das Verwenden von Unterverzeichnissen liegt in der Performance. Unter Microsoft Windows Betriebssystemen und

Novell Netware kann es zu erheblichen Problemen kommen, wenn sich in einem Verzeichnis beispielsweise 500.000 Dateien befinden.

Für diesen Status existiert ein zusätzliches Verzeichnis unterhalb von **jukebox**. Dieses Verzeichnis wird für das Auslagern auf den Sekundärspeicher benötigt.

Archiv

Nach einem weiteren Statustransfer in den Status "Archiv" wird das Dokument dann in dem Verzeichnis F:\d3\d3.dok\archiv als A0000001.1 abgelegt. Auch für diesen Status existiert ein zusätzliches Verzeichnis unterhalb von **jukebox**. Auch dieses wird für das Auslagern auf den Sekundärspeicher benötigt.

Sekundärspeicher

Dieses Verzeichnis wird für die Kommunikation mit dem Sekundärspeicher-System benötigt. Dieses Verzeichnis enthält zwei weitere Unterverzeichnisse **public** und **archiv**.

Wenn ein Dokument im Status "Freigabe" auf das Sekundärspeicher-System ausgelagert werden soll, wird dieses Dokument in das Unterverzeichnis **public** kopiert. In unserer Annahme wäre dieses somit F:\d3\d3X.dok\jukebox\public.

Für den Status "Archiv" wäre dies das Verzeichnis F:\d3\d3X.dok\jukebox\archiv.

Anfragen für das Retrieval von Dokumenten vom Sekundärspeicher werden direkt in dem Verzeichnis **jukebox** abgelegt.

Notizen

In diesem Unterverzeichnis werden die Notizen zu Dokumenten aufbewahrt.

Hätte man zu dem in unserem Beispiel archivierten Dokument eine Notiz angelegt, würde in dem Verzeichnis F:\d3\d3.dok\notizen die Datei A0000001.NOT angelegt werden.

Workflow

In diesem Unterverzeichnis werden die Definitionen der regelbasierten Leitwege abgelegt. Unterhalb dieses Verzeichnisses befindet sich ein Unterverzeichnis mit den Namen **Protokoll**. In diesem Verzeichnis wird zu jedem Dokument, welches durch einen Leitweg läuft, das entsprechende Protokoll des Durchlaufs durch den Leitweg abgelegt.

OCR

In diesem Unterverzeichnis werden die OCR-Dateien abgelegt.

Datensicherung

Sie können über eine automatische Sicherung den aktuellen Stand der Stammdaten des d.3-Repositorys speichern. Die so erstellten Backup-Dateien werden im d.3-Dokumentenbaum im Verzeichnis \D3P.dok\config\d3client\d3admin\mdbbackup abgelegt. Mit diesen Dateien kann man entweder das Bestandssystem in einen früheren Stand zurückversetzen, oder aber ein komplett neues System aufbauen.

Die Datensicherung kann so eingerichtet werden, dass diese täglich (zu einer bestimmten Zeit), wöchentlich (immer montags) oder monatlich (an einem bestimmten Tag) ausgeführt wird. Bei Fehlern oder bei jeder Datensicherung können Sie sich per E-Mail über den Durchlauf informieren lassen.

Es ist auch möglich, per expliziten Exportieren den aktuellen Stand zu sichern. Auch hier wird die Backup-Datei ebenfalls im d.3-Dokumentenbaum abgelegt.

Anmerkung

Die Backup-Datei enthält alle Daten, die auch bei der Aufzeichnung über Projekte und Meilensteine gesammelt werden. Zusätzlich werden auch die Benutzerdaten inklusive der Gruppenmitgliedschaften und Rechtezuweisungen gesichert. Mit diesen Daten können Sie dann das Bestandssystem auf einen älteren Stand zurücksetzen, oder aber ein neues System aufbauen.



Soll die Sicherung automatisch erfolgen, gehen Sie so vor:

1. Aktivieren Sie zunächst die Option **Automatische Sicherung aller Stamm-/ und Statusdaten auf dem d.3 Server**.
2. Legen Sie dann fest, wie oft (**täglich, wöchentlich, monatlich**) und um welche Uhrzeit (**Startzeit**) die Sicherung erfolgen soll.

Eine automatische Datensicherung in Form eines Snapshots findet bei jedem Import-Vorgang einer Transportdatei statt. Dabei wird ein neuer Meilenstein im Snapshot-Projekt angelegt und die aktuellen Daten dort abgelegt.

Sie haben zudem die Möglichkeit, sich per E-Mail über die Datensicherung - immer oder bei Fehlern - informieren zu lassen.

1. Aktivieren Sie die **E-Mail Benachrichtigung**.
2. Wählen zwischen **Benachrichtigung immer** oder **Benachrichtigung bei Fehler**.
3. Tragen Ihre **E-Mail-Adresse** im entsprechenden Feld ein.
4. Klicken auf **Übernehmen**.

Für einen manuellen Export aller Stamm-/ und Statusdaten klicken Sie auf die Schaltfläche **Export**.

d.3 client config

Bei dem Modul d.3 client config handelt es sich um ein Plugin für d.3 admin, das bei der Installation des der d.3-Anwendung (ab Version 5.5) automatisch eingerichtet wird. Weitere Informationen entnehmen Sie bitte der Dokumentation d.3 admin client config.

d.3 config

Jedes d.3 -Repository besitzt fünf Konfigurationsdateien, die sich normalerweise unterhalb des d.3- Server-Verzeichnisses (**d3server.prg**) in einem Unterverzeichnis befinden, das das Kürzel des d.3 -Repository trägt (z. B. **d3server.prg\D3FU**, wobei "FU" das Kürzel des d.3-Repository ist). In diesem Verzeichnis finden Sie dann die Dateien

- **d3admin.ini**
- **d3fixed.ini**
- **d3config.ini**
- **d3addon.ini**
- **aktplan.ini** (obsolet)

Die Aktenbildungsdefinitionen werden ab der d.3 Version 7 in der Datenbank verwaltet. Die **aktplan.ini** wird durch das Update-Skript einmalig umgesetzt.

Die Konfigurationsdateien **d3fixed.ini**, **d3config.ini** und **d3addon.ini** werden nacheinander beim Start der d.3-Prozesse (d3server, hostimp, d3async) in dieser Reihenfolge geladen. Dabei werden Einstellungen, die in mehreren Konfigurationsdateien vorkommen, jeweils durch die zuletzt geladene Datei überschrieben (die zuletzt vom d.3-Server geladene Datei ist **d3addon.ini**).

Um das d.3-Repository Ihren Bedürfnissen anzupassen, können Sie Veränderungen an den Konfigurationsdateien vornehmen. Die Datei **d3config.ini** wird über d.3 admin gepflegt. Spezielle Einstellungen können Sie in der **d3addon.ini** vornehmen.

Hier finden Sie nach der Repositoryinstallation immer den Pfad auf die Suchvorlagen-Dateien und die Profile, die Sie über das d.3 admin Plugin **d.3 client config** erstellen können.

Beispiel: Für das neu erstellte Repository "FU" sieht der Eintrag unter Microsoft Windows folgendermaßen aus:

```
CONFIG_PATH_D3CLIENT = „C:\d3\D3FU.dok\config\d3client“
```

Für ein Linux System ist folgender Eintrag denkbar:

```
CONFIG_PATH_D3CLIENT = „/opt/d3/D3FU.dok/config/d3client“
```

Warnung

Ändern Sie niemals die Datei **d3fixed.ini**. In diesem Fall kann es zu Fehlern in Ihrem d.3-Repository kommen.

Alle Änderungen müssen in der Datei **d3config.ini** oder **d3addon.ini** vorgenommen werden.

Die Datei **d3fixed.ini** enthält alle Parameter, mit denen das d.3 -Repository konfiguriert werden kann, bzw. mit denen das Repository im Standardverhalten erstellt wird. Wenn Sie also einen Parameter benötigen, können Sie sich in der **d3fixed.ini** über seine Verwendung informieren.

Anmerkung

Haben Sie Änderungen an der **d3addon.ini** vorgenommen, müssen Sie die d.3- Prozesse im d.3 process manager stoppen und anschließend neu starten, damit die neue Konfiguration wirksam wird.

Konfigurationsdialog

Die unten gelisteten und beschriebenen Parameter können über das Plugin **d.3 config** von d.3 admin unterhalb der **Systemeinstellungen** bequem eingelesen und ggf. auch angepasst werden.

Die Parameter sind zu logischen Gruppen zusammengefasst. Zu jedem Parameter erhalten Sie Hinweise, ggf. den Standardwert und den aktuell gesetzten Wert angezeigt.



1. Wählen Sie zunächst immer die logische Gruppe/Sektion aus, der der Parameter zugeordnet ist.
2. Anschließend wählen Sie den Parameter über seinen beschreibenden Namen aus (der technische Name ist i.d.R. nicht direkt aussagekräftig).



Nachdem Sie den betreffenden Parameter aktiviert haben, können Sie über eine Zeilenauswahl in der Wertetabelle rechts in den Änderungsdialog des Parameters gelangen.

Zum Teil können Sie hier über eine Wertemenge den neuen Wert auswählen, bei einigen Werten ist eine Eingabe erforderlich. Werden Verzeichnispfade erwartet, können Sie einen Auswahldialog öffnen.



Anmerkung

Die Änderungen an Werten und Parametern werden erst nach Bestätigung via **OK/Übernehmen** bzw. **Speichern** wirksam.

Konfigurierbare Parameter

Nachfolgend werden die Parameter aufgeführt, die direkt im Plugin **d.3 config** bearbeitet werden können.

Gespeichert werden diese in der Datei **d3config.ini** im Konfigurationsverzeichnis des Repository unterhalb von **d3server.prg**.

d.3 Dokumentenserver (Nutzdaten)

Protokoll über jeden Dokumentzugriff

LOG EVERY DOCUMENT ACCESS

Es wird ein Protokoll über jeden Dokumentzugriff und die Art des Zugriffs erstellt. Dieses Protokoll kann für Abrechnungszwecke (Accounting) verwendet werden. Die Sicherung erfolgt in einer Datenbank-Tabelle mit Namen zugriffs_protokoll.

Sobald dieser Schalter aktiviert ist, wird anschließend in der Tabelle zugriffs_protokoll jede Visualisierung (streng genommen sogar jede Aktion) eines Dokumentes eingetragen. Zunächst werden 100 Zugriffe gecached und anschließend gesammelt in die Tabelle eingetragen, um die Datenbanklast zu minimieren.

aktion	Diese Spalte enthält das Aktionskürzel der Änderung. Jedes Änderungs-Aktion (Import, AttributUpdate, Löschen) hat ein eigenes Kürzel. Eine Auflistung der Kürzel finden Sie weiter unten.
tstamp_aktion	Datum und Uhrzeit der Änderungsaktion
aktion_id	In dieser Spalte werden die Änderungsaktionen für jedes Dokument fortlaufend eindeutig durchnummeriert. Die aktion_id wird benötigt für die Verknüpfung (Join) mit anderen Tabellen insbesondere mit der Tabelle firm_spez_mul_hist.
aktion_user	Zu jeder Änderungs-Aktion wird in dieser Spalte der d.3-User gespeichert, der die Aktion durchgeführt hat.
aktion_text	Diese Spalte enthält einen Klartext zur Änderungsaktion. Bei Löschaktionen kann der User selber einen Klartext eingeben.

Aktionskürzel:

aktion	aktion_text
INV001	ImportNewVersion
UPD001	Aufruf von UpdateAttributes
DEL001	Benutzer-eigener Text

Der Schalter greift nur, wenn zusätzlich auch der Schalter LOG_CHANGES_IN_DB gesetzt ist.

Standardwert: Nein

Werte in der Spalte art_zugriff:

1	View/Download
21	ImportNewVersion
22	UpdateAttributes
31	Gelöscht im Dialog
32	Automatisch gelöscht inkl. Nutzfile
41	Verknüpft
42	Verknüpfung gelöst
51	Statustransfer
52	Geprüft
53	Freigegeben
61	Löschen eines Redlinings

Diese Tabelle kann mit den Zusatzprodukten Qlikview und d.link for Qlikview ausgewertet werden.

Spalte aktion_id:

In dieser Spalte werden die Änderungsaktionen für jedes Dokument fortlaufend eindeutig durchnummeriert.

Die aktion_id wird benötigt für die Verknüpfung (Join) mit anderen Tabellen insbesondere mit der Tabelle firm_spez_mul_hist.

Sichern der Kenndaten in der Datenbank**SAVE_CHANGES_IN_DB**

Bei

- Änderungen an den Kenndaten eines Dokumentes
- beim Löschen eines Dokumentes
- dem Anlegen einer Verknüpfung

oder

- Lösen einer Verknüpfung

werden die alten Werte in der Datenbank gesichert.

Standardwert: Ja

Eigenschaften sichern beim manuellen Ändern von Dokument-/Aktenverknüpfungen

<p>SAVE_USR_CHANGES_LINK_DOC</p> <p>Beim manuellen Anlegen oder Löschen einer Dokument-/Aktenverknüpfung werden die Änderungen in der Datenbank (Historientabellen) protokolliert.</p> <p>Standardwert: Ja</p>
<p>Eigenschaften sichern beim automatischen Ändern an Dokument-/Aktenverknüpfungen (Aktenplan)</p>
<p>SAVE_SRV_CHANGES_LINK_DOC</p> <p>Beim automatischen Anlegen oder Löschen einer Dokument-/Aktenverknüpfung werden die Änderungen in der Datenbank (Historientabellen) protokolliert.</p> <p>Standardwert: Nein</p>
<p>Eigenschaften sichern beim manuellen Ändern von Dokumenteigenschaften</p>
<p>SAVE_USR_CHANGES_ATTRIBUTES</p> <p>Die alten Eigenschaftswerte werden beim manuellen Ändern von Dokumenteigenschaften in der Datenbank (Historientabellen) protokolliert.</p> <p>Standardwert: Ja</p>
<p>Eigenschaften sichern beim automatischen Ändern an Dokumenteigenschaften</p>
<p>SAVE_SRV_CHANGES_ATTRIBUTES</p> <p>Die alten Eigenschaftswerte werden beim automatischen Ändern von Dokumenteigenschaften in der Datenbank (Historientabellen) protokolliert.</p> <p>Standardwert: Nein</p>
<p>Eigenschaften sichern beim Ersetzen der Nutzdatei</p>
<p>SAVE_SRV_CHANGES_REPLACE_USEFILE</p> <p>Die alten Eigenschaftswerte werden beim Ersetzen der Nutzdatei eines Dokuments (z.B. durch TIFF oder PDF) in der Datenbank (Historientabellen) protokolliert.</p> <p>Standardwert: Ja</p>
<p>Eigenschaften sichern beim manuellen Import neuer Dokumentversion</p>
<p>SAVE_USR_CHANGES_NEW_DOC_VERSION</p> <p>Die alten Eigenschaftswerte werden beim manuellen Import neuer Dokumentversionen in der Datenbank (Historientabellen) protokolliert.</p> <p>Standardwert: Ja</p>
<p>Eigenschaften sichern beim Import neuer Dokumentversion über hostimp</p>
<p>SAVE_SRV_CHANGES_NEW_DOC_VERSION</p> <p>Wenn diese Option aktiviert wurde, werden die alten Eigenschaftswerte beim Import einer neuer Dokumentversionen über den d.3 hostimp in der Datenbank (Historientabellen) protokolliert.</p> <p>Standardwert: Nein</p>
<p>Sichern von tätigkeitsprofil-basierten Wiedervorlage-Einträgen</p>
<p>SAVE_DISTRIBUTION_BASED_HOLD_FILE_ENTRIES</p>
<p>Sichern von nicht tätigkeitsprofil-basierten Wiedervorlage-Einträgen</p>
<p>SAVE_NON_DISTRIBUTION_BASES_HOLD_FILE_ENTRIES</p> <p>Informationen zu d.3 Postkorb-Einträgen, die über ein Tätigkeitsprofil liefern, werden in der Datenbank (Historientabellen) protokolliert.</p> <p>Standardwert: Nein</p>
<p>Protokoll über Kenndatenänderungen</p>
<p>LOG_CHANGES_IN_DB</p> <p>Änderungen an den Kenndaten eines Dokumentes, das Löschen eines Dokumentes das Anlegen oder Lösen einer Verknüpfung in der Datenbank werden protokolliert.</p> <p>Standardwert: Nein</p>

d.3-Datenbankserver (Kenndaten)

Database Management System

db_server

Die folgenden DBMS stehen zur Auswahl:

ORAC	Oracle 7.3 oder höher
MSQL	Microsoft SQL Server 6.5 oder höher
INFO	Informix 9.3 oder höher (wird mit Version 7.2 nicht mehr unterstützt)
DB 2	DB2 8.1 oder höher
DB2-400	iSeries Datenbank

d.3-Repositorys**Database**

Liste der Datenbanknamen (ODBC-Datenquellename; DSN), die in der Login-Maske für die Prozesse 'd3_server', 'd3_async', 'hostimp' u.a. zur Verfügung stehen..

d.3 SMTP-Unterstützung**Aktiviere SMTP Unterstützung****SMTP_SUPPORT**

d.3 kann zusätzlich zur internen d.3-Wiedervorlagefunktion eine E-Mail an den Adressaten senden. Bei Aktivierung dieses Parameters werden die dazu benötigten Treiber geladen.

Standardwert: Nein

Aktiviere SMTP für die Wiedervorlage**SMTP_MAIL_ON_HOLDFILE**

Bei der Wiedervorlage eines Dokuments wird der betreffende Benutzer per Mail darüber informiert.

Standardwert: Nein

Aktiviere SMTP für die Workflow-Wiedervorlage**SMTP_MAIL_ON_WORKFLOW**

Bei Workflow-Benachrichtigungen wird der betreffende Benutzer per Mail darüber informiert.

Standardwert: Nein

Mail-Versand inklusive Dokumenten-Referenz**SMTP_MAIL_INCLUDE_DOC**

Wenn d.3 eine Mail versendet, hängt es auch eine Referenz auf das Dokument an. Neue d.3 smart explorer-Versionen können diese d3l-Verweisdatei dann aus dem d.3-Repository öffnen.

Standardwert: Ja

SMTP Gateway**SMTP_GATEWAY**

SMTP Gateway, das die E-Mail weiterleitet.

SMTP Betreffzeile**SMTP_SUBJECT**

Betreffzeile für die automatisch generierte E-Mail-Nachricht.

Standardwert: d.3 neue Nachricht ::betreff_text

Mail-Versand an sich selber**SMTP_MAIL_ON_OWN_HOLDFILE**

Bei Aktivierung wird auch dann eine E-Mail versendet, wenn Absender und Empfänger identisch sind.

Standardwert: Nein

Administrativer SMTP-Benutzer**SMTP_ADM_MAILBOX_USER**

Dieses Benutzerkonto wird für das Senden von d.3 -E-Mails verwendet, wenn die E-Mails von Systembenutzern wie z. B. vom d.3 async versendet werden.

Diesem Parameter darf keine Domäne vorangestellt werden.

Administrative SMTP-Adresse

SMTP_ADM_MAILBOX_ADDRESS

E-Mail Adresse des administrativen SMTP-Benutzers. Einige SMTP-Server erlauben es nicht, dass anonyme E-Mails versendet werden. Dies kann dann der Fall sein, wenn d.3- Systembenutzer aus d.3 heraus E-Mails versenden. Für diese Fälle kann hier eine E-Mail-Adresse für die Systembenutzer eingetragen werden.

SMTP_MAIL_WITH_URL_ON_HOLDFILE

Bei der Wiedervorlage eines Dokuments wird in der E-Mail ein Link zur Dokumentenanzeige in d.velop documents angezeigt.

SMTP_MAIL_WITH_URL_ON_WORKFLOW

Bei einer Workflowbenachrichtigung wird in der E-Mail ein Link zur Dokumentenbearbeitung in d.velop documents angezeigt.

d.3-Retrieval-Verhalten**Warnung**

Beachten Sie, dass Änderungen am Retrieval-Verhalten sich nicht nur auf die Suche nach Dokumenten sondern auch auf die in Dokumentklassen verwendeten Funktionen auswirken.

Prüfen Sie also vor solchen Änderungen, ob Sie den zu verändernden Mechanismus ggf. bislang in Ihren Dokumentklassen verwendet haben und passen Sie diese entsprechend an.

Verwenden Sie keine Buchstaben für die Anpassungen.

SQL-Jokerersatz für %**WILDCARD_JOKER_1**

Das %-Zeichen, das als Platzhalter für eine unbekannte Anzahl von unbekanntem Zeichen bei einer Suchanfrage steht, wird in der SQL-Abfrage durch dieses Zeichen ersetzt.

Standardwert: *

SQL-Jokerersatz für _**WILDCARD_JOKER_2**

Das _-Zeichen, das als Platzhalter für genau ein unbekanntes Zeichen bei einer Suchanfrage steht, wird in der SQL-Abfrage durch dieses Zeichen ersetzt.

Standardwert: ?

Schlüsselzeichen für Alternativsuche**SEPARATE_OR_SEARCH_CHAR**

Um innerhalb eines Eigenschaftsfeldes nach mehreren Eigenschaftswerten suchen zu können (Alternativsuche), kann hier ein Schlüsselzeichen definiert werden, welches als Trenner fungieren soll.

Beispiel:

SEPARATE_OR_SEARCH_CHAR = '|'

Eingabe im d.3 smart explorer : wert1|wert2

-> Suche wird durchgeführt über "wert1" oder "wert2"

Anmerkung

Nicht zulässige Zeichen sind: Minus- und Pluszeichen, Doppelpunkt, Schrägstrich und Komma ('+', '-', ':', '/', ',').

Schlüsselzeichen für Ausschlussuche

SEPARATE_NOT_SEARCH_CHAR

Um bei der Suche Eigenschaftswerte auszuschliessen (Ausschlusssuche), kann hier ein Zeichen definiert werden, welches als Schlüssel für den Ausschluss fungieren soll.

Die Ausschlusssuche über den Parameter **SEPARATE_NOT_SEARCH_CHAR** ist ermöglicht für die folgenden Systemattributfelder:

Besitzer (besitzer)

Dokumentnummer (zeich_nr)

Bearbeiter (bearbeiter)

Dateiname

Dateierweiterung (datei_erw)

Bemerkungstext (text)

Beispiel:

SEPARATE_NOT_SEARCH_CHAR = '!

Eingabe im d.3 smart explorer: !wert3

-> Suche alles außer "wert3"

Anmerkung

Nicht zulässige Zeichen sind: Minus- und Pluszeichen, Doppelpunkt, Schrägstrich und Komma ('+', '-', ':', '/', ',')

Schlüsselzeichen für die Suche über leere Eigenschaften**SEPARATE_EMPTY_SEARCH_CHAR**

Um nach Eigenschaftsfeldern ohne Eintrag zu suchen, kann das hier konfigurierte Zeichen als Suchbegriff eingegeben werden.

Beispiel:

SEPARATE_EMPTY_SEARCH_CHAR = '\$'

Eingabe im d.3 smart explorer: \$

-> Suche über Eigenschaften ohne Inhalt

Schlüsselzeichen für Bereichssuche in alphanumerischen Feldern**SEPARATE_SPAN_SEARCH_CHAR**

Definiert ein Schlüsselzeichen, welches für eine Bereichssuche in alphanumerischen Eigenschaftsfeldern (1-49, 60-69) verwendet werden kann. Für Dokumentklassendefinitionen kann dieses Schlüsselzeichen bei alphanumerischen Feldern analog verwendet werden.

Beispiel:

SEPARATE_SPAN_SEARCH_CHAR = '~'

Eine Suche mit "A~Z" findet alle Begriffe, alphabetisch nach A und vor Z, z. B. "Apfel" oder "Wolf".

Eine Suche mit "Mann~" findet alle Begriffe, alphabetisch gleich oder nach "Mann", z.B. "Mann", "Maus" oder "Wolf".

Eine Suche mit "~Maus" findet alle Begriffe, alphabetisch vor und gleich "Maus", z.B. "Apfel" oder "Mann".

Schlüsselzeichen für Kleiner-Als Suche in alphanumerischen Feldern**SEPARATE_LESS_SEARCH_CHAR**

Definiert ein Schlüsselzeichen, welches für eine Kleiner-Als-Suche in alphanumerischen Eigenschaftsfeldern (1-49, 60-69) verwendet werden kann. Für Dokumentklassendefinitionen kann dieses Schlüsselzeichen bei alphanumerischen Feldern analog verwendet werden.

Beispiel:

SEPARATE_LESS_SEARCH_CHAR = '<'

Eine Suche mit "<M" findet alle Begriffe, alphabetisch vor "M", z. B. das Wort "Land", aber nicht "Maus"!

Schlüsselzeichen für Grösser-Als Suche in alphanumerischen Feldern

SEPARATE_GREATER_SEARCH_CHAR

Definiert ein Schlüsselzeichen, welches für eine Größer-Als-Suche in alphanumerischen Eigenschaftsfeldern (1-49, 60-69) verwendet werden kann. Für Dokumentklassendefinitionen kann dieses Schlüsselzeichen bei alphanumerischen Feldern analog verwendet werden.

Beispiel:

SEPARATE_GREATER_SEARCH_CHAR = '>'

Eine Suche mit ">Mann" findet alle Begriffe, alphabetisch nach "Mann", z.B. "Maus".

Schlüsselzeichen für paarige Suche bei Mehrfacheigenschaftsfeldern**SEPARATE_PAIR_SEARCH_60X_CHAR**

Um bei der Suche über mehrere Mehrfacheigenschaftsfelder Treffer zu erhalten, bei denen die Eigenschaftswerte in der gleichen Zeile stehen (paarige Suche), kann hier ein Zeichen definiert werden, welches als Schlüssel für die Eigenschaftsfelder fungieren soll, die bei dieser Suche kombiniert werden sollen.

Beispiel:

SEPARATE_PAIR_SEARCH_60X_CHAR = '\$'

Eingabe im d.3 smart explorer :

Feld60: \$name1

Feld61: \$wert1

Ergebnis: alle Treffer, die in den Feldern 60 und 61 in der gleichen Zeile "name1" und "wert1" enthalten.

Schlüsselzeichen für Kombinations-Suche bei Mehrfacheigenschaftsfeldern**SEPARATE_AND_SEARCH_60X_CHAR**

Um bei der Suche über Mehrfacheigenschaftsfelder Treffer zu erhalten, bei denen mehrere Eigenschaftswerte im gleichen Mehrfacheigenschaftsfeld enthalten sind, kann hier ein Zeichen definiert werden, welches als Schlüssel für die Suche fungieren soll.

Beispiel:

SEPARATE_AND_SEARCH_60X_CHAR = "#"

Eingabe im d.3 smart explorer Feld60: name1#name2

Ergebnis: Treffer, bei denen in den Zeilen des Feldes 60 sowohl "name1" als auch "name2" vorkommen.

Suche nach dem Dokumentstatus**SEARCH_STATUS_CURRENT**

Dieser Parameter steuert das Suchverhalten bei der Suche nach dem Dokumentstatus.

Wenn der Parameter aktiviert ist (Ja), werden alle Dokumente geliefert, deren aktuellster Status dem gesuchten entspricht.

Ist der Parameter nicht aktiviert (Nein), werden alle Dokumente geliefert, die eine Version in dem gesuchten Status haben.

Standardwert: Ja

Maximale Anzahl von Mehrfacheigenschaftsfeldern für eine Suche**SEARCH_MAX_COUNT_60X_FIELD**

Gibt die Anzahl der Mehrfacheigenschaftsfelder an, die maximal bei einer Suche verwendet werden dürfen. Eine Suche über mehrere Mehrfacheigenschaftsfelder kann zu Performance-Problemen führen, so dass diese, wenn möglich, vermieden werden sollte. Dieser Schalter greift nur für die Suche in d.3 smart explorer.

Standardwert: 2

Suche über mehrere Dokumentarten

DOC_TYPE_MULTI

Ähnlich wie bei der Dummy-Dokumentart können hier Dokumentarten definiert werden, bei denen die Suche über mehrere Dokumentarten ausgeführt wird.

Beispiel:

MUL1: Kürzel einer virtuellen Dokumentart

ART1, ART2, ... ,ART10: normale Dokumentarten

DOKUART_MULTI[1] = "MUL1,ART1,ART7,ART9"

Setzt man jetzt eine Suche über die Dokumentart "MUL1" ab, wird zusätzlich zur Dokumentart "MUL1" auch in den Dokumentarten "ART1", "ART7" und "ART9" gesucht.

Anmerkung

Die erste Dokumentart, die hier eingetragen wird, fungiert dabei als Dummy-Dokumentart mit der Konsequenz, dass diese Dokumentart nicht im Import-Client angezeigt wird. Mit dem Schalter **ENABLE_DUMMY_WRITE_ACCESS** lässt sich das Verhalten beeinflussen.

Kürzel der Dummy Dokumentart**DOCTYPE_SHORT_TEMPLATE**

Angabe des Kürzels einer Dokumentart, die als Schablone für eine dokumentartübergreifende Suche benutzt werden soll.

Anmerkung

Dummy Dokumentarten werden bei neuen Repositories nicht mehr als schreibberechtigt vom Server zurückgeliefert. Das hat dann zur Folge, dass diese Dokumentarten nicht im d.3 import angezeigt werden. Mit dem Schalter **ENABLE_DUMMY_WRITE_ACCESS** lässt sich das Verhalten beeinflussen.

Schreibzugriff auf Dummy Dokumentarten**ENABLE_DUMMY_WRITE_ACCESS**

Mit Aktivierung des Schalters werden Dummy-Dokumentarten, bei erteiltem Schreibrecht, auch im d.3 import angezeigt.

Standardwert: Ja

Maximal zu scannende Dokumente**SEARCH_FETCH_LIMIT**

Gibt die Anzahl von Dokumenten an, die bei einer interaktiven Suche maximal gelesen werden.

Hintergrund: Bei der Suche greift die Rechteprüfung/Nachfilterung. Dies führt dazu, dass es nötig sein kann,

deutlich mehr Dokumente zu prüfen, als effektiv an den Benutzer ausgeliefert werden sollen.

Rückgabe der Mehrfacheigenschaftsfeldern bei der Suche als Tabelle**SHOW_60X_AS_TABLE**

Mit Aktivierung des Schalters werden die Werte verschiedener Mehrfacheigenschaftsfelder als zusammenhängende Tabelle interpretiert, wobei die Rückgabe immer mit der ersten Zeile beginnt.

d.3-Dokumentablage**Dateierweiterung der Notizdateien****NOTE_FILE_EXT**

Suffix für die Dateinamen der Notizdateien.

Standardwert: NOT

Beispiel: "NOT" => Zu dem Dokument mit der Dokument-ID "IP004711" erhält eine dazu erzeugte Notizdatei den Dateinamen "IP004711.NOT"

Hochzählen der Variantennummer beim Import

AUTO_VAR_NR_INCREMENT

Falls zur vorgegebenen Dokumentnummer und Dokumentart bereits ein Dokument existiert, kann beim Import eines neuen Dokuments die Variantenummer automatisch hochgezählt werden (es wird die nächste freie Variantenummer erzeugt), um einen eindeutigen Schlüssel zu vergeben. Dies funktioniert aber nur, wenn nicht ausdrücklich eine Variantenummer vorgegeben wird. Vormerken aller neu importierten Dokumente, um sie später mit bestimmten Verfahren weiter verarbeiten zu können. Z. B. sollen alle neu importierten Dokumente zur Verteilung an andere Werke direkt wieder exportiert werden.

Standardwert: Nein

Automatische zeich_nr**AUTO_DOC_NR_ASSIGN_DIALOG**

Sofern beim Importieren von Dokumenten keine "zeich_nr" vorgegeben wurde, wird automatisch die Dokument-ID als "zeich_nr" übernommen.

Standardwert: Ja

Zusätzliche Serverkürzel**server_archive_ID_array**

Bis zu 50 zusätzliche Serverkürzel können den Dokumentarten zugeordnet werden.

In Abhängigkeit des Serverkürzels in der Dokument-ID können die Dokumente in unterschiedliche Repositories auf ein Sekundärmedium gespeichert werden.

Löschen von Dokumenten aus Freigabe oder Archiv**ALLOW_DELETE_FROM_RELEASE**

Hiermit kann das Löschen von Dokumenten aus der Freigabe erlaubt werden. Bis zu fünf zusätzliche Serverkürzel können den Dokumentarten zugeordnet werden. In Abhängigkeit des Serverkürzels in der Dokument-ID können die Dokumente in unterschiedlichen Repositories (Pools) auf dem Sekundärspeicher gespeichert werden.

Standardwert: Nein

Warnung

Dabei ist allerdings folgendes zu beachten: Zum einen muss der Benutzer, der in d.3 smart explorer ein Dokument aus der Freigabe löschen will, die nötigen Rechte haben. Des Weiteren wird das Dokument auch nicht physikalisch gelöscht, es wird in der Datenbank nur kenntlich gemacht, dass dieses Dokument nicht mehr in Ergebnissen angezeigt wird.

Eigenschaftsänderung von Dokumenten in Freigabe**ATTRIB_SUPPORT_MODIFY_RELEASE**

Wenn aktiviert, dürfen Benutzer Eigenschaften eines Dokumentes ändern, wenn es sich im Status Freigabe befindet und das Recht "Ändern Eigenschaften Freigabe" erteilt ist.

Standardwert: Nein

Änderungstext bei direktem Statustransfer von Bearbeitung in Freigabe**ALTERATION_TEXT_B_TO_F**

Wenn aktiviert, müssen Benutzer bei einem Statustransfer von Bearbeitung direkt in die Freigabe einen Änderungstext eingeben.

Keine Plausibilitätsprüfung der Eigenschaften beim HOST-Import**NO_ATTRIBUTE_CHECK_ON_BATCH**

Beim Massenimportverfahren HOSTIMP wird nicht auf Gültigkeit der Eigenschaften, bezogen auf die Definition für allgemeine Eigenschaften (Wertemengen, Regular-Expressions, Min-Max-Bereiche) und bezogen auf die Definition innerhalb der Dokumentart (Pflichtfeld, usw.), geprüft.

Standardwert: Nein

Validierung von numerischen Eigenschaftsfeldern**VALIDATE_NUMERIC_FIELDS**

Beim Validieren von numerischen Feldern, bei denen man einen nicht numerischen Inhalt eingetragen hat, blieb nur noch der numerische Teil über und es wurde kein Syntaxfehler zurückgegeben (Panther Standardverhalten). Mittels Aktivierung dieses Schalters kann das Verhalten geändert werden. Bei neuen Repositories ist der Schalter automatisch aktiviert.

Standardwert: Nein

Dateinamenserweiterungen für abhängige Dokumente

view_dep_ext_default

Definiert die Dateinamenserweiterungen, die für die abhängigen Dokumente unterstützt werden.

Dabei kommen den bereits vordefinierten folgende Bedeutung zu:

or	Original
t1 t2 t3	Tiff
a1 a2	ASCII (also Textdatei)
n5	Lotus Notes Datei (E-Mail-Archivierung)
p1	PDF
r1	Redlining
s1	Signatur
o1	für Tausche Original - Tiff-Dokument

Dateierweiterungen für die Anzeige von abhängigen Dokumenten**view_dep_ext_type**

Definiert den genauen Dateityp der von d.3 unterstützten abhängigen Dateierweiterungen.

Diese können dann für die Bestimmung des Anzeigeprogrammes der abhängigen Dokumente verwendet werden.

Länge der Dokument-ID**DOC_ID_LENGTH**

Länge der Dokument-ID in Anzahl Zeichen für neu in d.3 abgelegte Dokumente.

Möglich sind 8 oder 10 Repositories, die bisher mit 8-stelligen Dokument-IDs gearbeitet haben, können auf 10-stellige Dokument-IDs umgestellt werden, sofern das Datenbankmodell mit 10 Zeichen Länge für die Dokument-ID definiert ist.

Mit einer 10-stelligen Dokument-ID und einem einstelligen Vorspann für das Repository/d.Link können 999.999.999 Dokumente in d.3 verwaltet werden. (Default: 8)

Änderung der Dateierweiterung**SUPPORT_MODIFY_FILE_EXT**

Bei Aktivierung ist es möglich, die Dateierweiterung in der Lebenszeit von Dokumenten zu ändern. Für jede Dokumentversion wird dabei die Dateierweiterung getrennt gespeichert, sodass jede Version mit der ursprünglichen Applikation geöffnet werden kann.

Standardwert: Nein

Warnung

Die Visualisierung von älteren Dokumentversionen mit geänderten Dateierweiterungen funktioniert nur mit d.3-Anwendungen der d.3 Version 6.3 bzw. mit Anwendungen, die die Erweiterungen der API des 6.3er Servers unterstützen.

Anmerkung

Das Aktualisieren von Dokumenten mit einer anderen Dateiendung ist ab d.3 Version 6.3 nur per Drag&Drop auf das d.3- Dokument bzw. über den Hostimport möglich.

Eine Aktualisierung über die Anwendung **Speichern unter ..** erzeugt einen Neuimport.

Abschneiden der Eigenschaftswerte**CUT_ATTR_VALUES_TO_DEF_LEN**

Bei Aktivierung werden die Eigenschaftswerte beim Import bzw. bei der Eigenschaftsaktualisierung auf die im Eigenschaftsrepository definierte Länge abgeschnitten.

Beim Hostimport kann das Verhalten durch den Parameter `cut_attr_val_to_def_len` in der JPL-Datei bzw. in der `default.ini` individuell eingestellt werden.

Standardwert: Nein

Anzahl der Werte pro Mehrfacheigenschaftsfeld

CUR_60ER_FIELD_NR

Legt die Anzahl der Werte fest, die pro Mehrfacheigenschaftsfeld (60er Feld) bei Import und bei der Suche berücksichtigt werden. Der Defaultwert ist 100. Der maximal mögliche Wert für diesen Parameter ist 2000.

Wenn der Wert dieses Parameters verringert wird, und es Dokumente geben sollte, die in einem Mehrfacheigenschaftsfeld mehr Werte als hier eingestellt haben, wird bei jeglicher Änderung am Dokument ein Fehler ausgelöst und die Aktion abgebrochen!

Warnung

Der Parameter sollte nur erhöht werden, wenn tatsächlich so viele Werte für Mehrfacheigenschaftsfelder verwaltet werden müssen. Ein hoher Wert für diesen Parameter geht zu Lasten der Performance bei Import, Eigenschaftsänderung und bei der Suche.

d.3-Oberfläche und d.3-Verhalten**Formatierung von Datumswerten in Titel-Feldern****CAPTION_DATE_FORMAT**

Um eine alphanumerisches Sortierung in Titel-Feldern, die Datumswerte enthalten, zu ermöglichen, lässt sich eine Formatierung für Daten definieren. Folgende Kürzel werden dabei unterstützt:

- y für Jahr
- m für Monat
- d für Tag

```
CAPTION_DATE_FORMAT = 'yyyy-mm-dd' -> Datumswert = '2012-12-15'
```

d.3 gateway-Kommunikation**d.3 internes Serverkürzel****d3fc_server_id**

Mit diesem Kürzel meldet sich der d.3- Serverprozess am d.3 gateway an. Dieses Kürzel muss daher eine gültige d.3 gateway Repository-ID (Server-ID) sein. Dieses Kürzel wird auch per Standard als Präfix des Dateinamens (Dokument-ID), den d.3 für die verwalteten Dokumente vergibt, verwendet.

d.3 gateway Host**d3fc_server_name**

Der d.3 -Serverprozess muss sich bei einem d.link-Service registrieren. Er braucht dazu den Namen oder die IP-Adresse des Servers, auf dem d.3 gateway läuft.

d.3 Asynchrone Verarbeitung**Quittungen vom Sekundärmedium asynchron verarbeiten****ASYNC_INTERPRET_OK_FILES**

Wenn dieser Schalter aktiviert wurde, werden die OK-Dateien vom Sekundärmedium von einem asynchronen d.3-Prozess interpretiert. Wird der Schalter nicht aktiviert, muss ein separater Prozess diese Dateien verarbeiten.

Standardwert: Ja

Verzeichnisse für asynchrone Jobs**ASYNC_JOB_DIR**

Verzeichnisse, in denen Jobs für die asynchrone Verarbeitung abgelegt werden.

Vorgaben für die Job-Verarbeitung**ASYNC_JOB_DEFAULT**

Enthält, analog zur **default.ini** des Hostimports, Standardeigenschaften für die Jobs.

Job Typ

ASYNC_JOB_TYPE
Typ des Jobs:
MULTILINK: Mehrfachverknüpfungen
ATTRUPDA: Kenndaten-Update von bereits importierten Dokumenten
CUSTOMJOB: Kundenspezifische async-Jobs
Endungen der Eigenschaftsdateien
ASYNC_JOB_FILE_EXT
Dateierweiterungen, die für die Job-Dateien verwendet werden.
Endungen der gesicherten Eigenschaftsdateien
ASYNC_JOB_SAVE_EXT
Dateierweiterungen, die zum Sichern von fehlerhaften Job-Dateien verwendet werden sollen. Fehlerhafte Job-Dateien erhalten eine andere Endung, damit die Job-Verarbeitung sie nicht immer wieder interpretiert.
Verzeichnis für neu generierte Importaufträge
IMPL_FOLDER_DIR
Verzeichnis, in dem die asynchrone Job-Verarbeitung neu generierte Importaufträge ablegt. Die Importaufträge legen z. B. neue Akten an. Sie werden vom normalen d.3 import (HOSTIMP) verarbeitet. Dieses Verzeichnis muss auch für den HOSTIMP als eines der Importverzeichnisse definiert sein.
Endung für die Importaufträge
IMPL_FOLDER_EXT
Dateierweiterung für die neu generierten Importaufträge.
Standardwert: fol
Verzeichnis für asynchronen Import
ASYNC_IMPORT_DIR
Verzeichnis, in dem der d.3 -Serverprozess die Daten für den asynchronen Import ablegt. Diese Daten übernimmt dann der HOSTIMP. Dieses Verzeichnis muss auch bei den Hostimport-Verzeichnissen inklusive der Dateierweiterung mit aufgeführt werden.
Aufbewahrungsdauer für erfolgreich bearbeitete Jobs in der Datenbank
D3_JOBS_RUN_OK_LIFE_TIME_DAYS
Anzahl der Tage, die Jobs nach erfolgreichem Durchlauf noch in der Datenbank verbleiben
Standardwert: 0
Aufbewahrungsdauer für fehlerhafte Jobs in der Datenbank
D3_JOBS_RUN_ERROR_LIFE_TIME_DAYS
Anzahl der Tage, die Jobs nach fehlerhaftem Durchlauf noch in der Datenbank verbleiben
Standardwert: 31
Aufträge pro Durchlauf löschen
D3_JOBS_DELETE_PER_CALL
Anzahl der alten Jobs, die d.3 async bei jedem Durchlauf bereinigt.
Standardwert: 500
Erkennung der Akten
FOLDER_UNIQUE_KEY_NAME
Diese Felder der Datenbank werden zur Erkennung der Akte von d.3 async herangezogen. Dieser Mechanismus wird nur dann verwendet, wenn die Aktenverknüpfungen über ".A0?-Dateien (LIN001)" erstellt werden und wenn in diesen Dateien der Parameter folder_definition auf "1" steht. Bei Aktenverknüpfungen über die aktplan.ini hat dieser Parameter keine Bedeutung.
Löschen (logisch) von Dokumenten nach Ablauf der Lebensdauer
DELETE_DOCS_ELAPSED_AUTO
Bei Aktivierung werden Dokumente nach Ablauf der Lebensdauer logisch gelöscht.
Standardwert: Nein
Löschen (physikalisch) von Dokumenten nach Ablauf der Lebensdauer

DELETE_DOCS_ELAPSED_PHYSICAL
Bei Aktivierung werden Dokumente, die nach Ablauf der Lebensdauer logisch gelöscht wurden und eine bestimmte Anzahl von Tagen im Papierkorb verweilen (PAPIERKORB_VERWEILDAUER), physikalisch gelöscht.
Standardwert: Nein
Anzahl Dokumente pro Durchlauf löschen
DELETE_DOCS_ELAPSED_PER_CALL
Gibt die maximale Anzahl von Dokumenten an, die pro Durchlauf vom d.3 async gelöscht werden.
Standardwert: 50
Löschen von Dokumenten vom Sekundärspeicher
DELETE_DOCS_ELAPSED_SEC_STORAGE
Bei Aktivierung wird beim physikalischen Löschen von Dokumenten nach Ablauf der Lebensdauer ein entsprechender Job für den d.ecs storage manager geschrieben.
Standardwert: Nein
Verweildauer gelöschter Dokumente im Papierkorb
RECYCLE_STORAGE_PERIOD
Gibt eine Anzahl von Tagen an, die Dokumente nach dem logischen Löschen im Papierkorb verweilen, bis diese physikalisch gelöscht werden.
Standardwert: 365
Dateien beim Löschen von Dokumentversionen im Status "Bearbeiten" entfernen
DELETE_FILES_FROM_PROCESSING
Gibt an, ob die Nutzdatei beim Löschen aus dem Status "Bearbeitung" entfernt werden soll. Wird der Schalter deaktiviert, können gelöschte Bearbeitungsversionen aus dem Papierkorb wiederhergestellt werden.
Dateien beim Löschen von Dokumentversionen im Status "Prüfung" entfernen
DELETE_FILES_FROM_VERIFICATION
Gibt an, ob die Nutzdatei beim Löschen aus dem Status "Prüfung" entfernt werden soll. Wird der Schalter deaktiviert, können gelöschte Bearbeitungsversionen aus dem Papierkorb wiederhergestellt werden.
Spezialisierten DEL100-Async für automatisiertes logisches Löschen verwenden
USE_DEL100_ASYNC
Wenn kurzfristig sehr große Mengen an Dokumenten gelöscht werden müssen, sollte dies ein spezialisierter DEL100-Async durchführen. Genauere Informationen entnehmen Sie bitte der Dokumentation.
Automatisches Entfernen von gesendeten Postkorbeinträgen
CLEANUP_HOLDFILE_SENT
Steht dieser Wert auf 0 (Standard), so werden gesendete Postkorbeinträge nicht automatisch entfernt. Ansonsten steht der Wert für die Anzahl Tage, nach denen gesendete Postkorbeinträge nach dem Quittieren des Empfängers automatisch entfernt werden.

Sekundärspeicher

Sekundärmedium ansprechen
jukebox_daemon
Falls ein Dokument im d.3-Status "Freigabe" oder "Archiv" nicht auf dem Dokumentenserver gefunden wurde, kann zusätzlich auf dem Sekundärmedium weitergesucht werden.
Standardwert: Nein
Automatisches Auslagern auf Sekundärspeicher
AUTO_DOCS_ON_SEC_STORAGE
Dokumente, die in den d.3-Status "Freigabe" oder "Archiv" übertragen werden, können auf Wunsch sofort auf den Sekundärspeicher dupliziert werden.
Standardwert: Nein
Freigabe-Auslagerungsverzeichnis

SEC_STORAGE_PUBLIC_DIR

Pfad auf das Verzeichnis, von dem aus der Sekundärspeicher die d.3-Dokumente abholt, die im Status "Freigabe" sind und auf den Sekundärspeicher ausgelagert/dupliziert werden sollen.

Beispiel: O:\D3\D3.DOK\JUKEBOX\public

Freier Plattenplatz im Auslagerungsverzeichnis**STORAGE_DIR_MIN_FREE_SPACE**

Wenn im Auslagerungsverzeichnis weniger freier Platz ist als dieser Wert (in MB), dann wird nicht weiter ausgelagert. Sobald wieder mehr freier Platz vorhanden ist, wird der Storage Async die Auslagerung nachholen. Der freie Platz im Verzeichnis wird alle fünf Minuten neu ermittelt.

Synchrone Auslagerung**EXPORT_TO_STORAGE_SYNCHRON**

Beim Import werden die Dateien synchron in das Auslagerungsverzeichnis kopiert und auch der Auslagerungsjob wird synchron erstellt. Wenn man höhere Importperformance benötigt, kann man diesen Schalter deaktivieren. Dann führt d.3 storage async die Auslagerung asynchron durch. d.3 storage async sollte unbedingt daraufhin überwacht werden, dass er mit der Arbeit nachkommt.

Cachebereinigung durch d.3 async**ASYNC_CLEANUP_DISK**

d.3 async schafft Platz auf der Festplatte, wenn das Sekundärspeichersystem aktiv und der Parameter `MIN_FREE_DISK_SPACE` unterschritten ist.

Standardwert: Ja

Untere Grenze für freien Plattenplatz**MIN_FREE_DISK_SPACE**

Speicherplatz in Megabyte, der auf dem d.3-Fileserver (Dokumentenserver) mindestens frei bleiben muss. Wird diese Grenze unterschritten, werden auf dem Fileserver einige Dateien, die bereits erfolgreich auf den Sekundärspeicher übertragen wurden, gelöscht.

Diese Löschkaktion führt der d.3 asy nc-Prozess so lange durch, bis er die in der Konfiguration erreichte Anzahl der zu löschenden Jobs erreicht hat (`DELETE_NR_DOCS_PER_CYCLE`), bzw. bis er alle Dokumente, zu denen es einen Quittungseintrag für die erfolgreiche Auslagerung gibt, gelöscht hat.

Warnung

Dabei kann es auch vorkommen, dass Dokumente gelöscht werden, deren Cache-Verweildauer vom Datum her in der Zukunft liegt.

Zusätzlich kann auch der Parameter `DISK_CACHE_CLEANUP_DEP_DOCS` Auswirkungen auf die Cache-Bereinigung haben.

Standardwert: 500

Dokumente pro Durchlauf aus Cache löschen**DELETE_NR_DOCS_PER_CYCLE**

Gibt die maximale Anzahl von Dokumenten an, die pro Durchlauf von d.3 async aus dem Cache gelöscht werden.

Warnung

Sollte diese Zahl zu gross gewählt worden sein, kann der Löschvorgang u.U. den asynchronen Prozess von d.3 längere Zeit blockieren.

Standardwert: 1000

Abhängige Dokumente aus Cache löschen**DISK_CACHE_CLEANUP_DEP_DOCS**

Bei Aktivierung werden auch abhängige Dokumente aus dem Cache gelöscht.

Standardwert: Ja

Dokumenteigenschaften speichern**ATTR_TO_XML**

Alle Dokumenteigenschaften sind in der d.3-Datenbank abgespeichert. Wird dieser Parameter aktiviert, dann werden die Eigenschaften von Dokumenten ab dem Status 'Freigabe' zusätzlich in XML-Dateien abgelegt.

Diese werden bei aktivierter Jukebox-Auslagerung auf den Sekundärspeicher ausgelagert. Das Ablageverzeichnis muss per Parameter `D3_VERZ_DOK_ATTRIBUTE` konfiguriert sein und existieren.

Größe der Dokumenteigenschaftsdatei

ATTR_FILE_MAX_KB

Sofern der Schalter **ATTR_TO_XML** aktiviert ist, ist dies die maximale Größe der Datei, die Dokumenteigenschaften beinhaltet und auf den Sekundärspeicher geschrieben wird. Eine solche Datei kann die Eigenschaften zu mehreren Dokumenten beinhalten.

Anmerkung

Die Größe der XML-Datei kann im laufenden Betrieb auch mehrfach geändert werden. Die Größe wird jeweils nach dem Anfügen eines neuen Eigenschaftssatzes in die XML-Datei kontrolliert, und entscheidet darüber, ob die Datei geschlossen und Richtung Sekundärspeicher transferiert wird. Die empfohlene Größe sind die voreingestellten 50 KB.

Standardwert: "50"

Verzeichnis für Dokumenteigenschaftsdateien**ATTR_FILE_DIR**

Verzeichnis, in das die Dateien mit den Dokumenteigenschaften geschrieben werden sollen. Von dort werden sie dann abgeholt und auf den Sekundärspeicher gespielt.

Nachträgliches Auslagern**ASYNC_STORAGE_EXPORT**

Wenn dieser Schalter aktiviert ist, wird d.3 async Dokumente nachträglich auf den Sekundärspeicher auslagern, die nach aktueller Konfiguration noch nicht ausgelagert sind, aber ausgelagert werden müssten. Funktionalität wird nur ausgeführt wenn **AUTO_DOCS_ON_SEC_STORAGE** aktiviert ist.

Standardwert: Ja

Uhrzeit zur Ermittlung nachträglich auszulagernder Dokumente**ASYNC_STORAGE_EXPORT_TIME**

Da die Ermittlung noch auszulagernder Dokumente in großen Systemen einige Zeit beanspruchen kann, wird dies nun nur noch einmal täglich ausgeführt und die benötigten Informationen in einer separaten Datenbanktabelle abgelegt. Hier kann die Uhrzeit geändert werden, zu der dieser Vorgang ungefähr durchgeführt werden soll (Format: "hh:mm").

Standardwert: 21:00

Import-Verfahren HOSTIMP**Dateierweiterung für Action-Dateien****HOSTIMP_ACTION_FILE_EXT**

Wenn in einem Hostimport-Verzeichnis Dateien mit mehreren unterschiedlichen Dateierweiterungen angeliefert werden sollen, muss man für jede Dateierweiterung einen neuen Hostimport-Eintrag

(as400_import_*) erstellen.

Mit Hilfe einer sogenannten "Action-Datei" kann man einen indirekten Datei-Import initiieren und muss damit nur noch einen Eintrag pro Verzeichnis tätigen. Dabei muss zusätzlich zu den anderen Dateien, die für den Hostimport angeliefert werden, noch eine Action-Datei erzeugt werden. In dieser Action-Datei steht dann in der Variablen **import_file_ext** die Dateierweiterung der eigentlichen Nutzdatei. Die Dateierweiterung der Action-Datei wird in diesem Parameter festgelegt und muss als Dateierweiterung für den Hostimport in die Variable **as400_import_datei_erw** eingetragen werden.

Standardwert: action

Anmerkung

Action-Dateien werden von den neuen Versionen von d.link for lotus notes bzw. d.link for microsoft exchange erzeugt.

Beispiel einer Zuordnung in einer Action-Datei:

```
import_file_ext = „doc“
```

Max. Anzahl Dokumente pro Durchlauf**HOSTIMP_MAX_NR_DOCS_PER_SESSION**

Maximale Anzahl an Dokumenten, die pro Session des d.3 hostimp nach d.3 importiert werden sollen. Nach Erreichen dieser Anzahl beendet sich der d.3 hostimp selbstständig. Er kann durch Einsatz des Programms d.3 process manager automatisch neu gestartet werden.

Standardwert: 20000

Import-Verzeichnisse

HOSTIMP_IMPORT_DIR

Verzeichnisse, in denen die zu importierenden Dokumente liegen.

Beispiel: O:\D3\HOSTIMP

Standardwerte für die Eigenschaften**HOSTIMP_IMPORT_DEFAULT**

Steuerdatei, die die Eigenschaften angibt, die für alle aus dem entsprechenden Verzeichnis zu importierenden Dokumente gleich sind (z.B.\DEFAULT.INI). Diese Eigenschaften werden vor den durch die JPL-Datei angegebenen, dokumentspezifischen Eigenschaften gesetzt. Sie können durch die dokumentspezifische JPL-Datei überschrieben werden.

Beispiel: O:\D3\HOSTIMP\DEFAULT.INI

Dateierweiterung für den Import**HOSTIMP_IMPORT_FILE_EXT**

Dateierweiterung, die die zu importierenden Dokumente kennzeichnet (z.B. TIF, TXT).

Abhängige Dokumente für Hostimport**HOSTIMP_INCL_DEP_DOCS**

Ja: Der Hostimp sucht im Import-Verzeichnis nach abhängigen Dokumenten mit allen Extensions, die in d.3 für abhängige Dokumente konfiguriert sind (**view_dep_ext_default**).

Nein: Es werden keine abhängigen Dokumente mehr importiert.

Standardwert: Ja

Mindestspeicherplatz auf der Festplatte**HOSTIMP_MIN_DISKSPACE**

Diese Anzahl Megabyte muss auf der Festplatte mindestens frei sein, damit die d.3 hostimport Prozesse arbeiten können. Ansonsten beenden sich die Prozesse wieder.

Standardwert: 10

JPL-Datei notwendig**HOSTIMP_JPL_MANDATORY**

Bei Aktivierung erwartet der Hostimport neben der Nutzdatei auch eine Eigenschaftsdatei mit den Kenndaten zum Dokument.

Standardwert: Ja

Import-Verzeichnis für Restriktionsmengen**D3SET_IMPORT_PATH**

Verzeichnis, in dem Dateien liegen, über die Restriktionsmengen-Zuordnungen erstellt bzw. geändert werden können.

Dabei sind für eine Restriktionsmengen-Zuordnung eine JPL-Datei und eine TXT-Datei in das Verzeichnis zu stellen.

Die JPL-Datei kann dabei zwei Parameter enthalten:

"set_name" steht für den Namen der Restriktionsmenge und ist Pflichtparameter.

"set_object" gibt an, welchem Objekt die Mengen-Filter zugeordnet werden sollen. Dabei können Benutzernamen, Gruppennamen, Tätigkeitsprofile und Organisationseinheiten angegeben werden.

Die TXT-Datei enthält die Mengen-Filter wobei die Filter entweder mit ;-Zeichen oder per Zeilentrenner voneinander zu trennen sind.

Beispiel für .jpl-Datei:

set_name = "Lieferanten von A bis M"

set_object = "Einkauf"

Ignoriere zusätzliche Mehrfacheigenschaften**HOSTIMP_IGNORE_ADD_6X_VALUES**

Erlaubt den Import von Dokumenten mit mehr als CUR_60ER_FIELD_NR Eigenschaftswerten. Dabei werden die zusätzlichen Eigenschaften ignoriert (Achtung: Datenverlust möglich).

Standardwert: Nein

API-Logging-Parameter

Warnung

Loglevel 9 darf nur temporär zu Analysezwecken aktiviert werden, da der Debugmodus die Systemperformance stark belastet.

d.3 Async Log

D3_ASYNC_LOG_LEVEL

0 = nur kritische Fehler

6 = Nur Informationen

7 = jeder Job, der bearbeitet wird, wird im Logviewer angezeigt

9 = alles (Debuglevel)

d.3 Storage Async Log Level

0: Nur kritische Fehler

6: Nur Informationen

7: Jeder Job, der bearbeitet wird, wird im Logviewer angezeigt

9: Alles (Debuglevel)

Achtung: Loglevel 9 darf nur temporär zu Analysezwecken aktiviert werden, da der Debugmodus die Systemperformance stark belastet.

d.3 Server Log Level

D3_SERVER_LOG_LEVEL

Hier kann der Grad der Protokollierung eingestellt werden, mit dem die einzelnen Befehle an das d.3-System aufgezeichnet werden:

0 = nur kritische Fehler

3 = API-Call Einsprung und Aussprung

6 = wie 3, aber zusätzlich Übergabeparameter

7,8 = wie 6, aber zusätzlich SQL-Befehl beim Suchen

9 = alles (Debuglevel)

Standardwert: 6

d.3 API Timeout

D3_API_SELECT_TIMEOUT

Eine Suchanfrage wird nach Ablauf dieser Zeit abgebrochen, sofern der d.3 Server Prozess dem SQL-Server den Abbruch mitteilen kann.

Standardwert: 60

d.3 Hostimp Log Level

D3_HOSTIMP_LOG_LEVEL

6 = nur Informationen (default)

7 = Kurzinformationen zu jeder importierten Datei

9 = alles (Debuglevel)

Standardwert: 6

Maximallänge der Log-Zeilen

MAX_LOG_LINE_LENGTH

Dieser Wert bestimmt die Zeilenlänge der Protokoll-Einträge.

Standardwert: 70

SQL-Laufzeit-Logging-Untergrenze

MIN_SQL_LOG_RUNTIME_MILLIS

Alle ODBC-Operationen, die länger als die hier angegebene Anzahl an Millisekunden laufen, werden mit dem Default-Log-Level (6) und nicht im Debug-Modus (9) protokolliert.

Absturzprotokoll-Dateien (Mini-Dumps)**MINIDUMP_WITH_FULL_MEMORY**

Mit diesem Schalter wird eingestellt, ob und wie Absturzprotokoll-Dateien im Fehlerfall geschrieben werden.

Hook-Funktionen

Groovy-Hook-Verzeichnisse für kundenspezifische Programmanpassungen**HOOK_GROOVY_DIRS_CUSTOMER**

Geben Sie die Verzeichnisse, in denen die per Groovy implementierten, kundenspezifischen Programmanpassungen enthalten sind, hier an.

JPL-Datei für kundenspezifische Programmanpassungen**HOOK_JPL_FILES_CUSTOMER**

Name der JPL-Dateien, in denen die kundenspezifischen Programmanpassungen (Hook-Funktionen) stehen.

Hook-Funktionen ausführen**HOOK_FUNCTIONS_MAPPING**

Angabe der JPL Hook-Funktionen, die an dem jeweiligen Eintrittspunkt (**HOOK_FUNCTIONS_ACTIVATE**) ausgeführt werden.

Groovy Hook-Funktionen müssen hier nicht eingetragen werden!

Bei Prozess-Start werden alle Groovy-Dateien in den definierten Groovy-Hook-Verzeichnissen geparkt und die gefundenen Hook-Funktionen werden automatisch registriert. Das Ergebnis des Parsevorgangs wird in das d.3-Log ausgegeben und in eine Datei `log\groovy_hooks_registered_d3x.txt` geschrieben.

Neuladen von Groovy-Hook-Dateien bei Änderung aktivieren**HOOK_GROOVY_RELOAD_ON_CHANGE**

Ist dieser Schalter aktiviert, so führt das Speichern von Änderungen in Groovy-Hook-Dateien dazu, dass diese direkt neugeladen werden. Dadurch muss kein d.3-Prozess neugestartet werden und die Code-Änderungen sind sofort aktiv. Dieser Schalter kann bei der Entwicklung von Hook-Funktionen hilfreich sein. In Produktivumgebungen sollte er jedoch ausgeschaltet bleiben.

Benutzername für d3fc aus Hooks**HOOK_DEFAULT_D3FC_USER**

Standard-Benutzer für d3fc-Aufrufe aus Hooks heraus.

Passwort für d3fc aus Hooks**HOOK_DEFAULT_D3FC_PASSWORD**

Standard-Passwort für d3fc-Aufrufe aus Hooks heraus.

Passwortbezeichner für zusätzliche DB-Verbindungen**HOOK_PASSWORD_NAMES**

Diese Bezeichner können als Platzhalter für Passwörter in JPL-Hooks verwendet werden.

Die Verwendung wird in "d.3 hook api (jpl)" beschrieben.

Passwörter für zusätzliche DB-Verbindungen**HOOK_PASSWORDS**

Passwörter zur Ersetzung der Platzhalter in JPL-Hooks.

Parallele Nutzung von JPL und Groovy**HOOK_ENTRY_POINT_JPL_AND_GROOVY**

Ist dieser Schalter aktiviert, dann können Sie JPL-Hook-Funktion und Groovy-Hook-Methoden für den gleichen Hook-Einsprungpunkt registrieren.

Wenn Sie unter "Hook-Funktionen ausführen" in der Spalte "Hook-Funktion" den Namen einer JPL-Hook-Funktion angegeben haben und es existiert gleichzeitig

eine Annotation für diesen Einsprungpunkt in einem Groovy-Hook-Modul, so werden beide für diesen Einsprungpunkt registriert.

Bei der Ausführung wird zuerst die JPL-Hook-Funktion aufgerufen und direkt danach die annotierte(n) Groovy-Hook-Methode(n).

Import

<p>Feldnummer für Barcode-Status</p> <p>BARCODE_STATUS_FIELD_NR</p> <p>Nummer de Datenbankfeldes, das den Status des Barcodes beinhaltet.</p> <p>0: vorgebucht</p> <p>1: gescannt</p> <p>Standardwert: 88</p>
<p>Entfernen der Leerzeichen beim Import</p> <p>REMOVE_BLANKS_IMPORT</p> <p>Entfernen führender Leerzeichen in den Kenndaten beim Import.</p> <p>Standardwert: Nein</p>
<p>Hash-Wert Generierung für Dublettenprüfung</p> <p>GENERATE_DUP_HASH</p> <p>Bei Aktivierung werden für neue bzw. geänderte Dokumente Hash-Werte zur Dublettenprüfung erzeugt und in die Datenbank eingetragen. Ältere Dokumente, die vor der Aktivierung des Parameters schon im Repository vorhanden waren, können durch Ausführung des JPL-Scriptes <code>fill_empty_hash_values.jpl</code> mit einem Hash-Wert versehen werden.</p> <p>Standardwert: Nein</p>
<p>Prüfung auf Duplikate</p> <p>TEST_FOR_DUPLICATES</p> <p>Bei Aktivierung wird beim Import eines Dokumentes geprüft, ob sich schon ein Dokument mit gleichem Hash-Wert in der Datenbank befindet.</p> <p>Standardwert: Nein</p>
<p>Anmerkung</p> <p>Existiert bereits solch ein Dokument, wird der Import abgewiesen. Beim Hostimport wird im Falle einer Ablehnung des Dokumentes die Nutzdatei in ein Unterverzeichnis duplicates verschoben und zusätzlich eine Datei mit der Endung <code>.dup</code> erzeugt, die Informationen zum Referenz-Dokument enthält. Beim Import über ImportDocument bzw. ImportNewVersionDocument wird im Falle einer Ablehnung der Fehler "10036" ausgelöst. Informationen zum Referenz-Dokument können dem Export-Parameter <code>doc_id</code> entnommen werden.</p>
<p>Duplikate in Bearbeitung und Prüfung ignorieren</p> <p>IGNORE_DUPS_IN_B_P</p> <p>Mit diesem Schalter wird gesteuert, ob bei der Dublettenprüfung die Bearbeitungs- und Prüfungsversionen von Dokumenten berücksichtigt werden sollen, da diese Versionen nicht revisionssicher sind und somit jederzeit gelöscht werden können. Per Standard werden diese Versionen bei der Prüfung ignoriert.</p> <p>Standardwert: Ja</p>
<p>Duplikate im Status Archiv ignorieren</p> <p>IGNORE_DUPS_IN_A</p> <p>Mit diesem Schalter wird gesteuert, ob bei der Dublettenprüfung die Archiv-Versionen von Dokumenten berücksichtigt werden sollen. Per Standard werden diese Versionen bei der Prüfung berücksichtigt.</p> <p>Standardwert: Nein</p>
<p>Duplikate in anderen Dokumentarten ignorieren</p> <p>IGNORE_DUPS_IN_OTHER_DOCTYPES</p> <p>Mit diesem Schalter wird gesteuert, ob bei der Dublettenprüfung beim Import Dokumente aus anderen Dokumentarten berücksichtigt werden sollen. Per Standard werden Dokumente aus anderen Dokumentarten bei der Prüfung berücksichtigt.</p> <p>Standardwert: Nein</p>

Workflow

<p>Aktivieren des Workflows</p>
--

WORKFLOW_SUPPORT
d.3 unterstützt Geschäftsprozesse mit Workflows.
Standardwert: Nein
Verzeichnis für Ablage der Workflowdefinitionen
WORKFLOW_DEF_DIR
Pfad für die Ablage der Workflowdefinition in XML-Format.
Workflowmodul-Bibliothek - Server
d3fc_wfl_library_server_name
Rechnername des d.3-Servers, auf dem die Workflowmodul-Bibliothek abgelegt ist.
Anmerkung Dieser Wert muss konfiguriert werden, wenn Workflow für dieses Repository aktiviert ist, die Workflowmodul-Bibliothek sich aber in einem anderen Repository befindet.
Workflowmodul-Bibliothek - Repository ID
d3fc_wfl_library_server_id
Repository-ID des d.3-Repositorys, in dem die Workflowmodul-Bibliothek abgelegt ist.
Anmerkung Dieser Wert muss konfiguriert werden, wenn Workflow für dieses Repository aktiviert ist, die Workflowmodul-Bibliothek sich aber in einem anderen Repository befindet.
Workflowmodul-Bibliothek - TCP/IP Port
d3fc_wfl_library_tcpip_port
TCP/IP Port des d.3-Repositorys, in dem die Workflowmodul-Bibliothek abgelegt ist.
Anmerkung Dieser Wert muss konfiguriert werden, wenn Workflow für dieses Repository aktiviert ist, die Workflowmodul-Bibliothek sich aber in einem anderen Repository befindet.
Vertiffung des Workflow-Protokolls
WORKFLOW_LOG_TIFF
Die Workflow-Protokolle werden nach Abschluss des Leitweges vertiffert und als abhängiges TIF <small>w1</small> an das Dokument gehängt.
Standardwert: Nein
Stylesheet für Workflow-Protokoll
WORKFLOW_LOG_STYLESHEET
XSLT-Stylesheet, welches zum Transformieren des Workflow-Protokolls verwendet werden soll und somit das Aussehen des vertifferten Protokolls bestimmt. Das XSLT-Stylesheet muss eine HTML-Datei liefern.
Standardwert: <code>default.xml</code>
Schreibe Workflow-Protokolle auf Sekundärspeicher
WORKFLOW_WRITE_LOG_TO_SEC_STORAGE
Bei Aktivierung werden die Workflow-Protokolle unabhängig vom Parameter <code>SCHREIBE_ABH_DOKS_AUF_JUKEBOX</code> (in der <code>d3fixed.ini</code>) auf den Sekundärspeicher ausgelagert.
Standardwert: Ja
Manueller Workflow-Start von Dokumenten
WORKFLOW_START_MANUALLY
Bei Aktivierung: Ein Dokument kann generell manuell (z. B. über d.3 smart explorer) in jeden Leitweg gestellt werden.
Bei Deaktivierung: Nur Dokumente, für die der manuelle Start eines Leitwegs definiert wurde, können manuell (z. B. über d.3 smart explorer) gestartet werden.
Standardwert: Nein
Sichern der Workflow-Protokolleinträge in der Datenbank

WORKFLOW_SAVE_STEP_PROTOCOL_DB

Wenn diese Option aktiviert ist, werden die Protokolleinträge aller erfolgreich abgeschlossenen Workflowdurchläufe in der Datenbank (Historientabelle) gespeichert.

Standardwert: Ja

Sichern der Workflow-Variablen in der Datenbank**WORKFLOW_SAVE_USER_VALUES_DB**

Wenn diese Option aktiviert ist, werden nach Ende jedes erfolgreichen Workflow-Durchlaufs alle darin verwendeten Workflow-Variablen in der Datenbank (Historientabelle) gespeichert.

Standardwert = Ja

Statistik

Aktivieren der Statistik**STATISTICS_SUPPORT**

Wenn dieser Schalter auf "Ja" steht und die SQL-Statistiktabelle (statistics_archiv und statistics_run) existieren, dann führt d.3 zu allen unterschiedlichen Dateierweiterungen (.TIF, .TXT, ...) und zu allen Dokumentklassen eine Statistik der Belegung (Anzahl Dokument-ID's, Anzahl physikalischer Dateien, Summe KB). Abhängige Dateien werden dabei nicht berücksichtigt.

Möchten Sie eine Statistik über die Dokumente und Dokumentklassen führen, aktivieren Sie diesen Schalter. Dazu stellen Sie den Schalter auf "1". Anschließend müssen Sie noch das Skript **statistik_d3_belegung.jpl** ausführen lassen.

Warnung

Dazu müssen Sie zunächst die d.3 -Prozesse (d3_server, hostimp, d3_async), sowie alle weiteren Prozesse stoppen, die auf die Datenbank zugreifen.

Außerdem sollten Sie eine Datenbanksicherung durchführen.

Starten Sie über die Verknüpfung **Start > Programme > d.velop > d.3 > d.3 server interface (Repositoryname)** den Dialog zur Ausführung externer jpl-Skripte. Das Kennwort des Masters muss manuell in die Login-Maske eingegeben werden. Starten Sie dann über **Programme > Externes Programm** das externe JPL-Programm **statistik_d3_belegung.jpl**, das Sie im Unterverzeichnis **d3server.prg\ext_jpl** finden.

Das Skript durchsucht das komplette d.3-Repository und initialisiert die Statistiktabelle mit den aktuellen Werten. Dieses Programm muss einmal durchlaufen, bevor man mit der Statistik arbeiten kann.

Warnung

Bei einem großen Repository kann das Durchlaufen des Skripts evtl. mehrere Minuten oder länger (bis über eine Stunde) dauern (abhängig von der Anzahl der archivierten Dokumente). Brechen Sie das Skript nicht ab, da sonst Ihr d.3-System fehlerhaftes Verhalten zeigen kann.

Standardwert: Nein

Statistikintervall**STATISTICS_INTERVAL**

Die Statistik der d.3-Repositorybelegung wird in festgelegten Zeitabständen in SQL-Tabellen abgelegt, damit später Auswertungen über Zeiträume gefahren werden können. Erlaubte Werte für **BELEGUNG_STATISTIK_INTERVALL** sind

"W": wöchentlich

"M": monatlich

Standardwert: M

Passwort

Minimale Passwort Länge**PASSWORD_MIN_CHARS**

Minimale Länge des Passwortes, das sich ein Benutzer geben kann.

Standardwert: 8

Erweitere Syntaxregeln für Kennwörter

PASSWORD_EXTENDED_SYNTAX

Mit diesem Parameter kann eingestellt werden, ob die Kennwörter bestimmten Regeln unterliegen sollen.

Folgende Syntax-Regeln gelten bei Aktivierung:

- Jeweils mindestens ein Zeichen aus mindestens zwei der folgenden drei Gruppen: A-Z, a-z, 0-9.
- Mindestens ein Sonderzeichen.
- Das Kennwort darf nicht den Benutzernamen enthalten.

Standardwert: Ja

Anmerkung

Diese Kennwort-Einstellung gilt nur für Änderungen über den Login-Manager.

Lebensdauer eines Passwortes**PASSWORD_EXPIRE_DAYS**

Lebensdauer eines Passwortes in Tagen.

Standardwert: 10957 (= 30 Jahre)

Aktivierung der Kennwortchronik**PASSWORD_HISTORY_ENTRIES**

Wird ein Wert > 0 eingegeben, wird die Kennwortchronik aktiviert und die letzten Kennwörter werden gespeichert. Der Parameterwert gibt diese Anzahl an.

Standardwert: 10

Anmerkung

Ein neues Kennwort muss sich dann von denen in der Chronik gespeicherten Kennwörtern unterscheiden.

Fehlversuche aufzeichnen**PASSWORD_USER_FAILCHECK**

Schaltet die Prüfung der Fehlversuche von Benutzern bei der Anmeldung ein. Damit wird ein Benutzer nach einer bestimmten Anzahl von Fehlversuchen (Parameter: **PASSWORD_INPUT_TRIALS**) gesperrt und ggf. nach einer bestimmten Zeit (Parameter: **PASSWORD_USER_REJECTED**) automatisch wieder freigeschaltet.

Standardwert: Nein

Kontosperrungsschwelle**PASSWORD_INPUT_TRIALS**

Anzahl der Versuche, ab denen ein Benutzer bei fehlerhafter Eingabe seines Kennwortes gesperrt wird. Dieser Parameter erfährt nur dann eine Wirkung, wenn **PASSWORD_USER_FAILCHECK** aktiviert wurde.

Standardwert: 3

Automatische Freischaltung**PASSWORD_USER_REJECTED**

Zeit in Minuten, bis ein gesperrter Benutzer automatisch wieder freigeschaltet wird. Wird der Parameter auf "0" gesetzt, muss der d.3-Administrator den Benutzer freischalten.

Standardwert: 60

Passwort ändern nach Zurücksetzen durch Administrator**PASSWORD_ALTER_ADMINRESET**

Wenn der Parameter aktiviert ist, muss ein Benutzer sein Passwort, das durch einen Administrator zurückgesetzt wurde, bei der nächsten Anmeldung direkt ändern. Der Parameter greift nicht, wenn LDAP verwendet wird, da d.3 nur lesend auf die LDAP-Struktur (wie einem AD) zugreifen kann.

Standardwert: Nein

Anmerkung

d.3-Benutzerpasswörter können maximal 20 Bytes lang sein. Die Beschränkung ergibt sich aus dem d3fc-Protokoll, wo im Header die 20-Bytes vorgesehen sind.

Bei jedem d.3 API-Call werden Benutzername + Passwort übertragen. Das Passwort muss entsprechend in den Call-Header hinein passen.

Längere Benutzerpasswörter können aktuell nur durch die Benutzung von Session-Passwörtern, so wie sie auch bei der LDAP-Schnittstelle mit Kerberos-Authentifizierung genutzt werden, unterstützt werden.

Im Unicode-Modus kann, je nachdem welche (Sonder-)Zeichen im Passwort verwendet werden, die nutzbare Zeichenanzahl auch kleiner sein, weil Nicht-ASCII-Zeichen dabei mit mehreren Bytes kodiert werden.

Bidirektionaler Proxy**Support für den bidirektionalen d.3 Proxy****PROXY_BIDIRECT_SUPPORT**

Support für den bidirektionalen d.3-Proxy (mit aktiviertem Schreibcache)

Warnung

Dieser Schalter darf nicht einfach deaktiviert werden!

Wenn die bidirektionale Proxy-Funktionalität genutzt wird und ausgeschaltet werden soll, dann muss zuerst der Schreibcache aller d.3-Proxy-Systeme, die auf dieses Repository zugreifen, ausgeschaltet werden.

Erst danach darf hier auf d.3-Seitenseite dieser Schalter deaktiviert werden. Ansonsten werden weitere Proxy-Platzhalter archiviert, aber die eigentlichen Dokumente werden nicht mehr automatisch von den Proxy-Systemen in das Repository synchronisiert.

Nach Aktivierung müssen alle d.3-Serverprozesse durchgestartet werden!

Standardwert: Nein

Startzeit für Datenabgleich**proxy_sync_start_time**

Zeitintervall innerhalb dem der d.3 async - Prozess automatisch den Abgleich der Daten aus dem Schreibcache fährt. Bei erforderlichem Zugriff außerhalb dieser Zeit holt d.3 gateway das Dokument "on demand" aus dem Schreibcache.

Standardwert: 18:00

Stopzeit für Datenabgleich**proxy_sync_stop_time**

Zeitintervall, innerhalb dem der d.3 async - Prozess automatisch den Abgleich der Daten aus dem Schreibcache fährt. Bei erforderlichem Zugriff außerhalb dieser Zeit holt d.3 gateway das Dokument "on demand" aus dem Schreibcache.

Standardwert: 23:59

Timeout für Datenabgleich**proxy_sync_timeout**

Maximale Anzahl Sekunden, die d.3 wartet, wenn es auf eine Datei, die noch nicht aus dem Schreibcache synchronisiert wurde, an d.3 gateway eine "on demand"-Abgleichanforderung stellt.

Standardwert: 30

d.ecs rendition service

Support für d.ecs rendition service

DTIFF_SUPPORT

Einstellen der Nutzung des optionalen Moduls d.ecs rendition service (zentrales Vertiffen) für d.3 .

Anmerkung

Die Bezeichnung TIFF in den Parametern steht allgemein für das Rendern von Dokumenten und bezieht sich also auf das Erzeugen von TIFF- oder PDF-Dokumenten (PDF nur bei installierter PDF Extension).

Standardwert: Nein

Server des d.ecs rendition service**d3fc_dtiff_server_name**

Name des Rechners, auf dem d.ecs rendition service (optionales Modul) installiert ist. Bei **DTIFF_LEVEL = 1** muss der Rechnername von d.3 gateway angegeben werden.

Über d.ecs rendition service kann man Dokumente zentral vertiffen.

Standardwert: localhost

TCP/IP Port für d.ecs rendition service**d3fc_dtiff_server_tcpip_port**

TCP/IP-Port des Rechners, auf dem d.ecs rendition service installiert ist. Bei **DTIFF_LEVEL = 1** muss der Rechnername von d.3 gateway angegeben werden.

Timeout für d.ecs rendition service**d3fc_dtiff_server_timeout**

Standardwert: 3404

Maximale Zeit in Sekunden, die d.3 auf das (TIFF)-Ergebnis wartet, wenn es einen Auftrag an den d.ecs rendition service zur synchronen Bearbeitung geschickt hat. Über dieses Timeout werden d.3-Prozessblockaden verhindert, falls das Rendering unerwartet lang dauert.

Render-Prozesse werden nach diesem Timeout asynchron vom d.3 async- Prozess überprüft und das TIFF-Dokument ggf. nach d.3 gebracht.

Standardwert: 30

Volltext-Suche (d.3 search)**Support für d.3 search****DSEARCH_SUPPORT**

Einstellen der Nutzung des optionalen Moduls d.3 search (externe Volltextsuchmaschinen) für d.3 . Für den Import muss der Parameter **KEYWORD_OPTION** mindestens auf "1" stehen.

Warnung

Die Volltext-Unterstützung in einem Unicode d.3- Repository wird nur noch mit d.3 search gewährleistet.

Standardwert: Nein

Volltext-Optionen

KEYWORD_OPTION

Die folgenden Optionen stehen für die Volltextbehandlung zur Verfügung:

- 0: Es werden keine Daten beim Import in den Volltext-Index übernommen.
- 1: Nur die Eigenschaften des Dokumentes werden in den Volltext-Index übernommen.
- 2: Die Eigenschaften des Dokumentes sowie der Dokumenten-Inhalt (OCR-Datei) werden in den Volltext-Index übernommen.
- 3: Die Eigenschaften des Dokumentes sowie der Inhalt der Notiz-Datei werden in den Volltext-Index übernommen.
- 4: Die Eigenschaften, der Dokumenten-Inhalt (OCR-Datei) sowie der Inhalt der Notiz-Datei werden in den Volltext-Index übernommen.

Anmerkung

Voraussetzung für die Volltextbehandlung und Volltextsuche ist eine Installation des Produktes d.3 search!

Damit d.3 search verwendet wird, muss der Schalter **DSEARCH_SUPPORT** (siehe "Support für d.3 search") explizit aktiviert werden.

OCR Extension**ocr_ext**

Endung, an der d.3 die Schlagwort-Datei erkennt.

Beim Batch-Import wird nur dann eine Verschlagwortung durchgeführt, wenn eine Datei mit der angegebenen Endung existiert und die Konfigurationsvariable **KEYWORD_OPTION** auf 2 steht.

Die Schlagwort-Datei sollte eine reine Text-Datei ohne Sonderzeichen sein. Dokumente, die mit Textverarbeitungs-Programmen erstellt wurden, z.B. DOC-Dateien mit Microsoft Word, sind nicht geeignet. Sie müssen erst konvertiert werden, das heißt die Formatierungsinformation muss entfernt werden.

d.3 search Server**d3fc_dsearch_server_name**

Name des Rechners, auf dem d.3 search (optionales Modul) installiert ist. Über d.3 search können externe Volltextengines eingebunden werden.

Standardwert: localhost

Ab d.3 search 3.0 wird auch eine d.3 gateway-Anbindung unterstützt. Als Name müsste der Server, auf dem d.3 gateway läuft, angegeben werden.

TCP/IP Port für d.3 search**d3fc_dsearch_server_tcpip_port**

TCP/IP-Port des Rechners, auf dem d.3 search installiert ist.

Standardwert: 3406

Ab d.3 search 3.0 wird auch eine d.3 gateway-Anbindung unterstützt. Der Standardport ist dann 3400.

Maximale Anzahl der Volltext-Treffer**FULLTEXT_FETCH_LIMIT**

Legt die maximale Anzahl an Treffer für die Volltext-Suche fest.

Timeout für d.3 search**d3fc_dsearch_server_timeout**

Maximale Zeit in Sekunden, die d.3 auf das Ergebnis wartet, wenn es einen Auftrag an d.3 search geschickt hat. Über diesen Parameter wird ein Timeout der d.3 -Prozesse verhindert, falls die Verarbeitung bei d.3 search unerwartet lange dauert.

Standardwert: 30

d.3 search Vorfilterung für Eigenschaftsfelder**DSEARCH_DIRECT_DOCFIELD_SEARCH**

Aktiviert die direkte d.3 search-Suche für die Dokumenteigenschaftsfelder. Bei kombinierter Volltext- und Eigenschaftsfeld-Suche verringert dies die Treffermenge von d.3 search und beschleunigt somit die Nachfilterung durch den d.3-Server.

Standardwert: Ja

d.3 search Standard-Corpus

DSEARCH_DEFAULT_CORPUS

Wird verwendet, wenn kein Corpus für die Dokumentart explizit angegeben ist; bei Leerstring wird dieser Wert vom d.3 gateway Server-Kürzel abgeleitet (d3[d3fc_server_id]).

Darstellung der Datentypen**Warnung**

Ab d.3 admin Version 7.2.0 werden die folgenden Parameter nicht mehr angezeigt und können nicht mehr verändert werden.

Ausnahme: Wurde einer dieser Parameter in einer der vorherigen d.3 admin-Version geändert und enthält somit nicht mehr den Default-Wert, dann wird der Parameter noch angezeigt.

Mit der Version 8.0 werden diese Parameter durch d.3 server nicht mehr interpretiert!

Prüfen Sie daher rechtzeitig vor dem Update auf die Version 8, ob die zuvor genannten Schalter bei Ihnen von den Standardwerten abweichen. Sollte dies der Fall sein, gehen Sie wie folgt vor:

1. Überprüfen Sie bitte Ihre mit d.3 server kommunizierenden Anwendungen (z.B. Webservice, Hostimp-Importverzeichnisse, ...), inwieweit bei der Kommunikation nicht die obigen Standardwerte verwendet werden und passen diese an.
2. Deaktivieren Sie Ihre diesbezügliche kundenspezifische Konfiguration von d.3 server, indem Sie die Standardwerte für die Parameter über d.3 admin setzen.

Tausend-Trenner für Geld-Felder**FORMAT_7X_THOUSANDS_SEPARATOR**

Standardwert: EMPTY

Dezimal-Trenner für Geld-Felder**FORMAT_7X_DECIMAL_SEPARATOR**

Standardwert: DOT

Minimale Anzahl an Nachkommastellen für Geld-Felder**FORMAT_7X_MIN_DECIMAL_DIGITS**

Standardwert: 2

Maximale Anzahl an Nachkommastellen für Geld-Felder**FORMAT_7X_MAX_DECIMAL_DIGITS**

Standardwert: 2

Tausend-Trenner für numerische Felder**FORMAT_8X_THOUSANDS_SEPARATOR**

Standardwert: EMPTY

Dezimal-Trenner für numerische Felder**FORMAT_8X_DECIMAL_SEPARATOR**

Standardwert: DOT

Minimale Anzahl an Nachkommastellen für numerische Felder**FORMAT_8X_MIN_DECIMAL_DIGITS**

Standardwert: 0

Maximale Anzahl an Nachkommastellen für numerische Felder**FORMAT_8X_MAX_DECIMAL_DIGITS**

Standardwert: 2

LDAP

Zeitangabe für Synchronisierung aller d.3-LDAP-Benutzer**LDAP_USER_SYNC_TIME**

Wird hier eine Uhrzeit (Format: hh:mm) angegeben, wird jeden Tag zu dieser Zeit eine Synchronisierung der d.3 -Benutzerverwaltung mit dem über das LDAP-Administrationsmodul konfigurierten Directory Service durchgeführt. Dabei werden neue Benutzer, sowie geänderte Benutzereinstellungen vorhandener Benutzer nach d.3 übernommen.

Administrativer LDAP-Benutzername**LDAP_ADMIN_USER_NAME**

Wenn der benutzte Directory Service kein anonymes Login erlaubt, kann hier ein LDAP-Benutzername angegeben werden, der dann bei der Synchronisierung für das Auslesen aller Benutzerwerte verwendet wird.

Passwort für den administrativen LDAP-Benutzer**LDAP_ADMIN_USER_PASSWORD**

Wenn der benutzte Directory Service kein anonymes Login erlaubt, kann hier das Passwort für den bei der Synchronisierung zu verwendenden LDAP-Benutzer vorgegeben werden.

Benutzerdaten lesen mit administrativem LDAP-Benutzer**LDAP_READ_ACCESS_ADMIN_USER**

Durch Aktivieren des Schalters **LDAP_READ_ACCESS_ADMIN_USER** werden die Benutzerdaten durch den Benutzer (**LDAP_ADMIN_USER_NAME**) vom Directory Service ausgelesen und nicht durch den anmeldenden Benutzer selbst (Default).

Dies kann verwendet werden, wenn Sicherheitsrichtlinien der Kunden-IT den lesenden Zugriff auf den Directory Tree nur für Benutzer mit besonderen Rechten gestatten. In diesem Fall wird mit den Benutzerdaten des anmeldenden Benutzers lediglich die Authentifizierung (**BIND**) durchgeführt. Alle lesenden Zugriffe erfolgen nur mit dem administrativen Benutzer.

Gültigkeit der Session-Passwörter**KERBEROS_SESSION_PASSWORD_DAYS**

Gültigkeit der Session-Passwörter in Tagen. Nach Ablauf des Passwortes wird vom System bei der nächsten Anmeldung ein neues Passwort vergeben.

Standardwert: 2

Session-Passwörter erzeugen**LDAP_GENERATE_SESSION_PASSWORD**

Standardwert: Ja

Durch Aktivieren dieses Schalters werden von d.3 server Session-Kennwörter erzeugt, auch wenn keine Kerberos-Authentifizierung verwendet wird.

Dadurch können sich Applikationen mit dem LDAP-Benutzernamen, aber auch dem d.3-Benutzernamen gleichzeitig für das gleiche Benutzerkonto anmelden.

Analog zur Kerberos-Lösung wird so bei aktivierter LDAP-Schnittstelle ein "Gemischtbetrieb" mehrerer Applikationen des gleichen Benutzers unterstützt, egal ob diese den LDAP-Benutzernamen oder den d.3-Benutzernamen verwenden.

Voraussetzung ist allerdings die Unterstützung von Sessionpasswörtern durch die Client-Applikationen. Ist diese gewährleistet, kann der Schalter aktiviert werden.

Anmerkung

Für d.3 -Applikationen aus dem Hause d.velop ist dies ab d.3 Version 6.3.1 gewährleistet.

Sind weitere, ggf. selbst erstellte Applikationen im Einsatz, die auf d.3 zugreifen, muss geprüft werden, ob diese die vom d.3 Server zurückgelieferten Session-Passwörter übernehmen (siehe Dokumentation d.3 API; Funktion `ValidatePasswordForUser` mit dem Parameter `package=Basic`).

Der Schalter muss in folgenden Situationen aktiviert werden:

- Die LDAP-Schnittstelle ist aktiviert.
- Benutzer nehmen per d.3 web am Workflow teil und verwenden gleichzeitig auch andere d.3-Applikationen.

Beispiel: Ein d.3 -Benutzer nutzt d.3 smart explorer und nimmt per Microsoft Outlook am d.3 -Workflow teil.

In diesem Fall ist der Schalter zu aktivieren, damit die gleichzeitige Nutzung des Benutzerkontos durch d.3 smart explorer und d.3 web flow connector funktioniert.

"Nur neue Benutzer"-Modus für die LDAP-Schnittstelle

LDAP_NEW_USER_ONLY_MODE

Wird dieser Modus aktiviert, so werden über die LDAP-Schnittstelle nur noch neue Benutzer nach d.3 übernommen, aber keine Änderungen mehr an bestehenden Benutzern vorgenommen.

Dieser Modus kann genutzt werden, wenn die Benutzer in d.3 admin gepflegt und verändert werden sollen.

Die Änderungen werden hierbei nicht von der LDAP-Schnittstelle übersteuert.

Die per LDAP-Plugin vorgenommenen Eigenschaften- und Rechtezuweisungen greifen hier nur für die initiale Übernahme eines LDAP-Benutzers nach d.3.

Standardeinstellung = 0 (deaktiviert):

LDAP ist für die d.3-Benutzerverwaltung das führende System.

Alle Änderungen in der LDAP-Konfiguration oder an den Daten im Directory Service werden nach d.3 übernommen.

Java/Groovy**Java/Groovy Support****JAVA_SUPPORT**

Einschalten der Unterstützung für die Ausführung von Java und Groovy Code in d.3.

Standardwert: Nein

Java Virtual Machine**JAVA_JVM_LIBRARY**

Bibliothek mit der zu verwendenden Java Virtual Machine. Diese wird beim Start der d.3-Prozesse geladen, um die Java Laufzeitumgebung zu initialisieren.

Anmerkung

Bei der Java Laufzeitumgebung (JRE) von Oracle wird unter Microsoft Windows die `jvm.dll` und unter Linux die `libjvm.so` genutzt.

JVM Options**JAVA_JVM_OPTIONS**

Optionen für die Java Virtual Machine. Für nähere Informationen schauen Sie in die [Dokumentation der Oracle Java HotSpot VM Options](#).

Beispiel für das Setzen von JVM Optionswerten:

Wenn Sie den verwendeten Speicher der JVM anpassen möchten, ist dies über die Optionen "-Xms" und "-Xmx" möglich. "-Xms" definiert hierbei das Standardvolumen, welches direkt allokiert wird. "-Xmx" definiert das Maximalvolumen an Speicher, welches maximal allokiert werden darf.

Wenn Sie möchten, dass das Standardvolumen 512 MB ist und maximal 1024 MB allokiert werden sollen, würde die Konfiguration folgendermaßen aussehen:

```
-Xms512m -Xmx1024m
```

Anmerkung

Da es sich beim d.3-Server um eine 32-Bit-Applikation handelt, können maximal 1300 MB zugewiesen werden.

Java CLASSPATH**JAVA_CLASSPATH**

Dateipfad zu den eigenen Java Klassen.

Hier kann ein Verzeichnis angegeben werden, in dem die class-Dateien abgelegt sind. Alternativ kann auch der Dateiname einer JAR-Datei eingetragen werden.

Es können mehrere durch ein Semikolon getrennte Dateinamen angegeben werden.

Java/Groovy API-Funktionen**JAVA_API_FUNCTIONS_DIR**

Aktiviert die Plugin-Schnittstelle für API Funktionen entwickelt in Java bzw. Groovy. Groovy-Skripte oder JAR-Dateien, die d.3-API-Funktionen implementieren, werden aus diesem Verzeichnis geladen.

Java/Groovy Support
Java Remote Debugging JAVA_REMOTE_DEBUGGING Java Virtual Machine im Debugmodus starten. Dadurch ist es möglich sich per Remote Java Debugger mit einem d.3-Serverprozess zu verbinden, um die darin ausgeführten Groovy Hooks zu debuggen. Für die Kommunikation wird Port 43400 benutzt. Da jeder d.3-Prozess eine eigene Java Virtual Machine (JVM) startet, werden die benutzten Ports hochgezählt. Der erste mit aktiviertem JAVA_REMOTE_DEBUGGING gestartete Prozess öffnet Port 43400, der Zweite Port 43401 usw. Der ermittelte Port wird beim Start der JVM per Meldung "Java Remote Debugging Port" in das d.3-Log ausgegeben.
Anmerkung Die JVM wird von d.3 auf Nachfrage beim ersten Zugriff auf Groovy-Code gestartet und steht damit i.d.R. noch nicht direkt nach Prozessstart zur Verfügung.

Vertreterregelung

Umverteilung der Dokumente nach Tagen DISTRIBUTION_AFTER_CHECKOUT_DAYS 0: Dokumente werden unverzüglich nach dem Checkout eines Benutzers umverteilt. > 0: Dokumente werden über den d.3 async Prozess erst ... Tage später umverteilt. Standardwert: 0
Gelesene Postkorb-Einträge ignorieren DOC_DISTRIBUTION_IGNORE_READ Wenn diese Option aktiviert ist, fließen nur die ungelesenen Postkorb-Einträge in die Berechnung des Lastverteilers ein. Standardwert: Ja
Dokumenten-Verteilung an Vertreter SEND_MAIL_TO_SUBSTITUTE Wenn ein Benutzer sich abwesend gemeldet und einen Vertreter eingetragen hat, können alle seine Postkorb-Einträge auf den Vertreter umverteilt werden. Bei Anwesenheitsmeldung können alle ungelesenen Einträge wieder an den eigentlichen Empfänger zurückgeleitet werden. Um dieses Verhalten einzuschalten, muss der Parameter SEND_MAIL_TO_SUBSTITUTE aktiviert (= "1") werden. Standardwert: Nein
Gelesene Einträge bei Dokumenten-Verteilung berücksichtigen DISTRIBUTE_READ_DOCS Bei Aktivierung werden bei der Umverteilung an einen Adhoc-Vertreter auch die gelesenen Postkorbeinträge berücksichtigt. Dieser Schalter wirkt sich bei den Parametern SEND_MAIL_TO_SUBSTITUTE und MAILBOX_SUBST_TYPE aus. Hinweis: Nach der Umverteilung werden alle Postkorbeinträge beim Vertreter als ungelesen angezeigt. Findet eine Rückverteilung statt, werden auch hier alle Einträge als Ungelesen markiert.
Typ der Dokumenten-Verteilung an Vertreter MAILBOX_SUBST_TYPE Mit dem Parameter WV_SUBST_TYPE kann gesteuert werden, ob die Postkorb-Einträge kopiert (COPY) oder verschoben (MOVE) werden sollen. Sollen die Einträge verschoben werden, findet eine Rücksendung aller ungelesenen Einträge bei Anwesenheitsmeldung statt. Standardwert: COPY
Kopie an Empfänger

SEND_DOC_TO_ORIGIN

Soll ein Dokument an einen Benutzer versendet werden, der sich abwesend gemeldet und einen Vertreter eingetragen hat, geht dieses an den Vertreter (normales Verhalten);

bei aktiviertem Schalter **SEND_DOC_TO_ORIGIN** aber auch zur Info an den eigentlichen Empfänger.

Standardwert: Nein

Vorgesetzter in optionalem Feld eines Benutzers**SUPERIOR_IN_USER_OPT_FIELD**

1-10: Nummer (1 bis 10) des optionalen Benutzerfeldes, in dem der d.3-Benutzername des Vorgesetzten vermerkt wird.

0: Es wird kein Vorgesetzter gepflegt.

Sollte dieser Wert auf "0" stehen oder das optionale Feld mit der hier angegebenen Nummer leer sein, wird der Vorgesetzte über die d.3- Organisationsstruktur ermittelt. Ansonsten hat dieses Verfahren Vorrang vor der d.3-Organisationsstruktur.

Standardwert: 0

Vorgesetzter auf gleicher Ebene**SUPERIOR_SAME_LEVEL**

Bei der Ermittlung des Vorgesetzten eines Benutzers sind alle Mitglieder seines Tätigkeitsprofils auch die Vorgesetzten. Ist der Schalter deaktiviert, muss der Vorgesetzte in jedem Fall mindestens eine Stufe höher in der Organisationsstruktur eingeordnet sein.

Standardwert: Nein

Rechteprüfung mit Vertretungen bei @D3USER**USER_MACRO_USE_SUBST**

Wird bei einer Dokumentklasse das Makro @D3USER verwendet, können die Benutzer, für die der Aufrufer als Vertreter bestimmt wurde, in die Rechteprüfung integriert werden. Somit wird dann der Zeichenketten-Vergleich sowohl gegen den Benutzernamen des Aufrufers als auch gegen die Benutzernamen der Vertretungen getätigt.

Standardwert: Nein

Berechtigungssteuerung

Dokumente als Vorgesetzter aus Bearbeitung entziehen**REVOKE_PROCESSING_SUPERIOR**

Ja: Wenn ein Dokument in der Bearbeitung eines Benutzers liegt, dann darf nur dieser Benutzer und sein Vorgesetzter dieses Dokument bearbeiten oder im Status verschieben

Nein: Jeder Benutzer mit Schreibrechten darf das Dokument entziehen, wobei vorher eine Warnung erscheint.

Standardwert: nein

Dokumente als Administrator aus Bearbeitung entziehen**REVOKE_PROCESSING_ADMIN**

Ja: Wenn ein Dokument in der Bearbeitung eines Benutzers liegt, dann darf nur dieser Benutzer oder ein d.3-Administrator dieses Dokument bearbeiten oder im Status verschieben.

Nein: Jeder Benutzer mit Schreibrechten darf das Dokument entziehen, wobei vorher eine Warnung erscheint.

Standardwert: nein

Berechtigungsprüfung bei Wiedervorlagen-Versendung**MAILBOX_CHECK_RECIPIENT_RIGHTS**

Bei Aktivierung wird vor dem Versenden der Wiedervorlage (nur bei Einzelempfänger) geprüft, ob der Empfänger das Dokument überhaupt sehen darf. Wenn nein, gibt es eine Fehlermeldung.

Standardwert: Ja

Berechtigungsprüfung nach Eigenschaftsaktualisierung**UPD_DOC_CHECK_NEW_CLASS**

Bei der Aktualisierung von Eigenschaften (UpdateAttributes) wird nach Durchführung eine Prüfung auf das Dokument durchgeführt, ob der Benutzer weiterhin Schreibrechte auf dieses besitzt.

Standardwert: Nein

Zusätzliche Berechtigungsprüfung beim Dateizugriff

EXTRA_RIGHT_CHECK_ON_FILE_ACCESS
Standardmäßig wird bei der Dokumentsuche ein Zugriffsschlüssel erzeugt, der der d.3-Anwendung für eine begrenzte Zeit das Anzeigen und Herunterladen der physischen Dateien eines Dokuments ermöglicht. Wird dieser Schalter aktiviert, so erfolgt direkt beim Dateizugriff noch eine erneute synchrone Rechteprüfung. Die Aktivierung dieses Schalters ist mit erhöhter Systemauslastung verbunden.
Automatische Sperrung bei Inaktivität
BLOCK_USER_AFTER_DAYS
Gibt einen Zeitraum in Tagen an, der seit der letzten Anmeldung eines Benutzers vergangen sein muss, bis dieser automatisch vom System gesperrt wird
Standardwert: 0 (keine automatische Sperrung)
Automatische Deaktivierung bei Inaktivität
DISABLE_USER_AFTER_DAYS
Gibt einen Zeitraum in Tagen an, der seit der letzten Anmeldung eines Benutzers vergangen sein muss, bis dieser automatisch vom System deaktiviert wird
Standardwert: 0 (keine automatische Deaktivierung)
Automatisches Löschen bei Inaktivität
REMOVE_USER_AFTER_DAYS
Gibt einen Zeitraum in Tagen an, der seit der letzten Anmeldung eines Benutzers vergangen sein muss, bis dieser automatisch vom System gelöscht wird
Standardwert: 0 (keine automatische Löschung)

Sonstige Parameter

Farbcode für Repository
ARCHIVE_COLOR_CODE
Legt die Farbe für das Repository-Icon fest.
0 (Standard): Rot
1: Grün
2: Blau
3: Lila
Senden von UDP Paketen für Objekt Monitor
UDP_SUPPORT
Dieser Schalter muss auf "Ja" stehen, damit d.3 server , d.3 hostimp und d.3 async regelmäßig UDP-Pakete an den Überwachungs-dienst senden.
Standardwert: Ja
Unterstützung des Abo-Services
ABOSERVICE_SUPPORT
Bei Aktivierung des Schalters ist ein d.3 abo service Prozess für das d.3- Repository startbar und der Kontextmenüpunkt Abonnieren in d.3 smart explorer wird angezeigt. Für Benutzer, denen eine E-Mail-Adresse zugewiesen wurde, ist der Punkt dann aktiv geschaltet.
Standardwert: Nein
Standard Zeichenkodierung
DEFAULT_CODEPAGE
Dieser Wert sollte gesetzt werden, wenn alle bereits importierten Dokumenteigenschaften die gleiche Zeichenkodierung haben. Enthält das Repository Dokumente mit Eigenschaften in mehreren verschiedenen Zeichenkodierungen, sollte der Wert auf "0" gesetzt bleiben. Ansonsten wird an die Clients für bereits importierte Dokumente unter Umständen eine falsche Zeichenkodierung übergeben.
Standardwert: 0
Wertemengen in Suchergebnissen übersetzen

TRANSLATE_SEARCH_RESULTS

Ist diese Option deaktiviert, werden die Übersetzungen für statische Wertemengen ausschließlich in Eingabemasken (bei der Suche und Eigenschaftsbearbeitung) angezeigt. Wenn dieser Schalter aktiviert ist, werden auch die aktuellen Eigenschaften eines Dokuments übersetzt angezeigt.

Standard: Ja

Syntax von regulären Ausdrücken**REGEX_SYNTAX**

Ist diese Option deaktiviert, werden die Übersetzungen für statische Wertemengen ausschließlich in Eingabemasken (bei der Suche und Attributbearbeitung) angezeigt. Wenn dieser Schalter aktiviert ist, werden auch die aktuellen Eigenschaften eines Dokuments übersetzt angezeigt.

Standard: Ja

Standardmäßig verwendet d.3 die "POSIX Basic Regular Expression Syntax". Um komplexere reguläre Ausdrücke erstellen zu können, kann die "POSIX Extended Regular Expression Syntax" oder die "PERL/JavaScript Regular Expression Syntax" verwendet werden. Diese Typen haben einen größeren Funktionsumfang, unterscheiden sich aber in zentralen Punkten von der 'Basic Syntax'.

Warnung

Es wird dringend empfohlen, bestehende reguläre Ausdrücke in Hooks, Plausibilitäts-Kontrollen von Repository-Feldern und Dokument-Klassen-Filtern darauf zu überprüfen, ob diese mit der neuen Syntax kompatibel sind.

Die "POSIX Basic Syntax" ist im Wesentlichen mit der "JPL Syntax" kompatibel, hat aber mehr Funktionen und ist UNICODE-fähig. Benutzen Sie die "JPL Syntax" nur, wenn 100%ige Abwärtskompatibilität benötigt wird und auf korrekte Behandlung von Unicode-Zeichen verzichtet werden kann.

Anmerkung

Die Besonderheit der "POSIX Extended Regular Expressions Syntax" besteht in der Formulierung von Oder-Ausdrücken.

Beispiel: Der reguläre Ausdruck "d.3 ist (gut|super)!" erlaubt folgende Muster: "d.3 ist gut!" bzw. "d.3 ist super!".

Standardwert: POSIX Basic Regular Expression Syntax

Groß-/Kleinschreibung bei regulären Ausdrücken beachten**REGEX_CASE**

Gibt an, ob bei der Auswertung von regulären Ausdrücken die Groß-/Kleinschreibung berücksichtigt werden soll. Diese Einstellung hat keinen Effekt, wenn die "JPL Regular Expression Syntax" verwendet wird.

Standardwert: Case sensitive

Protokollieren der Job-Laufzeit in der Datenbank**RUNTIME_INFO_DAYS_OF_DB_STORAGE**

Mit dieser Variable wird angegeben, für wie viele Tage Laufzeitinformationen zu dem von d.3 verarbeiteten Jobs in der DB-Tabelle `runtime_info` gehalten werden sollen. API-Calls, asynchrone Jobs und Hostimports werden nach totaler Laufzeit, Hook-Laufzeit, SQL-Laufzeit und Zeit zum Warten auf das Dateisystem aufgeschlüsselt gespeichert. Ist diese Variable auf "0" gesetzt, erfolgt keine Protokollierung in der Datenbank.

Standardwert: 0

Anzeige mit Wasserzeichen aktivieren**WATERMARK_SUPPORT**

Mit dem Aktivieren des Parameters können Sie Benutzern Dokumentklassenrechte zuweisen, sodass diese Benutzer nur Dokumente mit Wasserzeichen anschauen dürfen.

Anmerkung

- Eine Installation von d.ecs pdf extension Version 1.4.2 oder höher ist erforderlich
- Die Anzeige mit Wasserzeichen funktioniert nur mit dem deaktivierten Schalter **V8RunningUpdateBackComp**.
- Die Anzeige mit Wasserzeichen gilt nur für Dokumente, die im PDF-Format abgelegt sind.

Standardwert: 0

Audit-Trail

Protokollierung von Änderungen durch Benutzer

AUDIT_USER_CHANGES
Wenn dieser Schalter aktiviert ist, werden Änderungen von Benutzern an nicht direkt Dokument bezogenen Daten (z. B. abwesend melden oder Kennwort ändern) in der Datenbank protokolliert.
Standardwert: Nein
Auditierte Dokumentarten (vollständig)
audited_doc_types
Kurzbezeichner der Dokumentarten, bei denen alle Änderungen an den Dokumenten im Audit-Trail protokolliert werden sollen.
Auditierte Dokumentarten (einfach)
audited_doc_types_basic
Kurzbezeichner der Dokumentarten, bei denen alle Änderungen an den Dokumenten (ohne Details) im Audit-Trail protokolliert werden sollen.
Nachvollziehbarkeit von Rendern und Vorschlagworten
AUDIT_PROTOCOL_TIF_OCR
Bei aktiviertem Schalter kann das Rendern und Vorschlagworten von Dokumenten in der Datenbank exakt nachvollzogen werden.
Meldung bei unberechtigten Zugriffen
AUDIT_LOG_ACCESS_DENIED
Bei aktiviertem Schalter werden unberechtigte Dokumentenzugriffsversuche im Protokoll innerhalb des Sicherheitskontextes ausgegeben.

Key/Value-Cache (jStore)

jStore-Bucket
KV_STORE_BUCKET
Name des Buckets (ID-Prefix) im jStore. Wenn dieser Parameter nicht gesetzt ist, wird der Wert aus dem Parameter 'd3fc_server_id' verwendet.
Asynchrones Befüllen mit importierten Dokumenten
KV_STORE_IMPORTED_WARMING
d.3 async füllt den Key/Value-Speicher mit den zuletzt importierten Dokumenten.
Anmerkung Unabhängig von diesem Parameter wird der Cache automatisch bei jeder Suchanfrage gefüllt.
Standardwert: Nein
Anzahl der zuletzt importierten Dokumente
KV_STORE_ASYNC_IMPORTED_COUNT
Gibt die Anzahl der zuletzt importierten Dokumente an, mit denen d.3 async den Key/Value-Speicher befüllt. Es werden die neuesten Dokumente in den Cache geladen, bis die hier angegebene Anzahl erreicht ist oder es keine weiteren Dokumente gibt, die nicht im Cache sind.
Standardwert: 0
Asynchrones Befüllen mit Postkorbeinträgen
KV_STORE_HOLDFILE_WARMING
d.3 async berücksichtigt beim Befüllen des Key/Value-Speichers auch Postkorbeinträge.
Anmerkung Unabhängig von diesem Parameter wird der Cache automatisch bei jeder Suchanfrage gefüllt.
Standardwert: 0
Anzahl der Postkorbeinträge
KV_STORE_ASYNC_HOLDFILE_COUNT
Gibt die Anzahl der Postkorbeinträge an, mit denen d.3 async den Key/Value-Speicher befüllt. Es werden Postkorbeinträge in den Cache geladen, bis die hier angegebene Anzahl erreicht ist oder es keine weiteren Dokumente gibt, die nicht im Cache sind.
Standardwert: 0

Signatur

PDF-Dateien auf enthaltene Signaturen prüfen

SIGN_CHECK_PDF

Wenn dieser Parameter aktiviert wird, werden PDF-Dateien beim Import (Hostimport oder API Import) auf enthaltene Signaturdaten geprüft. Dafür muss d.ecs pdf extension installiert sein (mindestens Version 1.2.0.1.)

Standardwert: Nein

Standard-Prüfgruppe für signierte Dokumente

SIGN_DEFAULT_GROUP

Dieser Parameter gibt die Standard-Prüfgruppe für Dokumente an, die noch signiert werden müssen oder deren Signaturen noch nicht vollständig geprüft wurden. Wenn beim Import ein nicht erlaubter Status (vom Standpunkt des Signierens gesehen) angegeben wurde, wird das Dokument automatisch in die Prüfung dieser Gruppe importiert.

Standardwert: ""

Erweiterte Optimierungen/Feintuning

Datenbankspalten mit statischer Abfrage

STATIC_STATEMENT_COLUMNS

Bei vielen Datenbank-Zugriffen, nutzt d.3 Prepared-Statements mit Bind-Variablen. Dies hilft der Datenbank dabei, schneller zu arbeiten, da Ausführungspläne nicht immer neu erstellt werden müssen, wenn sich nur die Werte aber nicht die Form einer Abfrage ändert.

Es gibt jedoch Situationen, in denen der beste Ausführungsplan der Datenbank stark von den übergebenen Werten abhängt. Ein typischer Fall sind hierbei Spalten mit sehr ungleichmäßiger Werteverteilung, also beispielsweise dass die meisten Werte genau einmal vorkommen, andere Werte aber in Millionen von Zeilen stehen.

In dieser Liste können Spalten eingetragen werden, deren Vergleichswerte statisch in SQL-Abfragen geschrieben werden sollen, statt über Bind-Variablen indirekt genutzt zu werden.

Format: "tabellen_name.spalten_name" (Im Spalten-Namen können SQL-Wildcards (% und _) verwendet werden)

Anmerkung

Hinweis 1: Das Standardverhalten von d.3 ist in den meisten Fällen optimal. Bitte nutzen Sie diese Option nur, wenn es konkrete Leistungseinbußen gibt, die auf ungünstige Ausführungspläne zurückzuführen sind. Entfernen Sie Einträge wieder, falls diese keine Verbesserung gebracht haben.

Hinweis 2: Für einige Spalten nutzt d.3 automatisch statische Abfragen, ohne dass diese Spalten hier aufgeführt werden müssten (beispielsweise wenn gefilterte Indizes verwendet werden).

Hinweis 3: Dieser Schalter wirkt sich auf die meisten SQL-Abfragen aus, die von d.3 generiert werden, aber nicht durchgehend auf alle Datenbankzugriffe.

Anzahl der max. über d.3 search gefilterten Dokumentarten

MAX_DOCTYPES_DSEARCH_FILTERING

Gibt die Anzahl der Dokumentarten an, die d.3 bei der Suche maximal an d.3 search übergibt.

Eine Einschränkung der Dokumentarten, kann die Volltextsuche deutlich beschleunigen und die Genauigkeit der Ergebnisse erhöhen.

Anmerkung

Dieser Effekt ist besonders groß, wenn die Anzahl der potenziellen Ergebnisse durch die Dokuart-Liste deutlich reduziert wird.

Falls die Anzahl der ausgewählten Dokumentarten allerdings zu groß ist und somit keine nennenswerte Einschränkung der Ergebnisse mehr darstellt, kann sich die Filterung in d.3 search auch negativ auf die Suchperformance auswirken.

Überschreitet die Liste der Dokumentarten einer Suche den hier eingestellten Wert, erfolgt die Filterung auf Dokumentarten nach der Volltext-Abfrage in d.3 server.

Aktivitäten

Auf der Home-Seite die eigenen Aktivitäten anzeigen

HOME_ENABLE_OWN_ACTIVITIES
0: Eigene Aktivitäten werden nicht angezeigt. 1: Eigene Aktivitäten werden angezeigt.
Auf der Home-Seite alle Aktivitäten anzeigen
HOME_ENABLE_ALL_ACTIVITIES
0: Alle Aktivitäten werden nicht angezeigt. 1: Alle Aktivitäten werden angezeigt.
Benutzernamen anonymisieren
TIMESPAN_BEFORE_ANONYMIZE_ACTIVITIES
Standard: 30 Immer anonymisieren: 0 Nie anonymisieren: -1 Die Benutzernamen werden nach Ablauf der hier angegebenen Zeitspanne bei der Anzeige anonymisiert.
Dokumentarten mit minimalem Log-Level
DOC_TYPES_LOG_MINIMAL[1]
Kurzbezeichner der Dokumentarten, für die minimales Logging aktiviert ist. Ereignisse: Import, Import einer neuen Version, Eigenschaftsaktualisierung, Verknüpfen von Dokumenten und Akten.
Dokumentarten mit erweitertem Log-Level
DOC_TYPES_LOG_EXTENDED[1]
Kurzbezeichner der Dokumentarten, für die erweitertes Logging aktiviert ist. Ereignisse: Statustransfer, zu Favoriten hinzufügen und entfernen, Signieren
Log-Level für das Verknüpfen von Dokumenten und Akten
LOG_LEVEL_LINK
Gibt an, ab welchem Log-Level das Verknüpfen von Dokumenten in die Historie aufgenommen wird. Log-Level: 1 = Minimal, 2 = Standard, 3 = Erweitert
Log-Level für das Auflösen von Verknüpfungen
LOG_LEVEL_UNLINK
Gibt an, ab welchem Log-Level das Auflösen von Verknüpfungen in die Historie aufgenommen wird. Log-Level: 1 = Minimal, 2 = Standard, 3 = Erweitert
Log-Level für das Starten eines Workflows
LOG_LEVEL_START_WORKFLOW
Gibt an, ab welchem Log-Level Starten eines Workflows in die Historie aufgenommen wird. Log-Level: 1 = Minimal, 2 = Standard, 3 = Erweitert
Log-Level für das Beenden eines Workflows
LOG_LEVEL_FINISH_WORKFLOW
Gibt an, ab welchem Log-Level Beenden eines Workflows in die Historie aufgenommen wird. Log-Level: 1 = Minimal, 2 = Standard, 3 = Erweitert
Log-Level für das Senden einer Wiedervorlage
LOG_LEVEL_SEND_HOLDFILE
Gibt an, ab welchem Log-Level Senden einer Wiedervorlage in die Historie aufgenommen wird. Log-Level: 1 = Minimal, 2 = Standard, 3 = Erweitert
Log-Level für das Weiterleiten einer Wiedervorlage
LOG_LEVEL_FORWARD_HOLDFILE
Gibt an, ab welchem Log-Level Weiterleiten einer Wiedervorlage in die Historie aufgenommen wird. Log-Level: 1 = Minimal, 2 = Standard, 3 = Erweitert

<p>Log-Level für das Quittieren einer Wiedervorlage</p> <p>LOG_LEVEL_ACK_HOLDFILE</p> <p>Gibt an, ab welchem Log-Level Quittieren einer Wiedervorlage in die Historie aufgenommen wird.</p> <p>Log-Level: 1 = Minimal, 2 = Standard, 3 = Erweitert</p>
<p>Log-Level für das Hinzufügen eines Redlinings</p> <p>LOG_LEVEL_ADD_REDLINE</p> <p>Gibt an, ab welchem Log-Level Hinzufügen eines Redlinings in die Historie aufgenommen wird.</p> <p>Log-Level: 1 = Minimal, 2 = Standard, 3 = Erweitert</p>
<p>Log-Level für das Entfernen eines Redlinings</p> <p>LOG_LEVEL_REMOVE_REDLINE</p> <p>Gibt an, ab welchem Log-Level Entfernen eines Redlinings in die Historie aufgenommen wird.</p> <p>Log-Level: 1 = Minimal, 2 = Standard, 3 = Erweitert</p>
<p>Log-Level für das Hinzufügen eines Favoriten</p> <p>LOG_LEVEL_ADD_TO_FAVS</p> <p>Gibt an, ab welchem Log-Level Hinzufügen eines Favoriten in die Historie aufgenommen wird.</p> <p>Log-Level: 1 = Minimal, 2 = Standard, 3 = Erweitert</p>
<p>Log-Level für das Entfernen eines Favoriten</p> <p>LOG_LEVEL_REMOVE_FROM_FAVS</p> <p>Gibt an, ab welchem Log-Level Entfernen eines Favoriten in die Historie aufgenommen wird.</p> <p>Log-Level: 1 = Minimal, 2 = Standard, 3 = Erweitert</p>

Das Schreiben der Historieneinträge folgt folgendem System:

1. Es gibt drei verschiedene Log-Level: **Minimal**, **Standard** und **Extended**
 - Jede Dokumentart gehört standardmäßig dem Log-Level "Standard" an mit Ausnahme von:
 - i. **DOC_TYPES_LOG_MINIMAL** (das minimale Log-Level)
 - ii. **DOC_TYPES_LOG_EXTENDED** (das erweiterte Log-Level)

Anmerkung: Dieses Level kann in folgender Form gelesen werden:
"Für eine Dokumentart werden alle Ereignisse geloggt, welche einen Ereignisslevel <= des Log-Levels der Dokumentart besitzen."
2. Jede Aktion (Event) gehört entweder fest oder konfigurierbar einem bestimmten Log-Level an
 - Für folgende Aktionen sind die Log-Level frei konfigurierbar (d.3 config-Schalter):
 - i. **LOG_LEVEL_LINK**
 - ii. **LOG_LEVEL_UNLINK**
 - iii. **LOG_LEVEL_START_WORKFLOW**
 - iv. **LOG_LEVEL_FINISH_WORKFLOW**
 - v. **LOG_LEVEL_SEND_HOLDFILE**
 - vi. **LOG_LEVEL_FORWARD_HOLDFILE**
 - vii. **LOG_LEVEL_ACK_HOLDFILE**
 - viii. **LOG_LEVEL_ADD_REDLINE**
 - ix. **LOG_LEVEL_REMOVE_REDLINE**
 - x. **LOG_LEVEL_ADD_TO_FAVS**
 - xi. **LOG_LEVEL_REMOVE_FROM_FAVS**
3. Die Log-Level/Events sind folgendermaßen definiert:
 - a. Minimaler Log-Level (wird also immer geschrieben):
 - i. **Import**
 - ii. **Update_Client**
 - iii. **Update_Job**
 - iv. **Update_Server**

- v. **Update_Inherit**
 - vi. **ImportNewVersion_Client**
 - vii. **ImportNewVersion_Hostimp**
 - viii. **ImportNewVersion_Async**
 - ix. **StatusTransfer**
 - x. **PublishForWeb**
 - xi. **ClientEvent** (also spezifisch durch die d3fc-API ausgelöste Events)
- b. Standard Log-Level:
An sich jedes Event, welches nicht explizit einen minimalen bzw. extended Log-Level bekommen hat (hier dennoch die Auflistung):
- a. **Import_Hostimp**
 - b. **Import_Async**
 - c. **LinkToChild_Job**
 - d. **LinkToParent_Job**
 - e. **AddNote**
 - f. **Sign**
 - g. **RegisterID**
 - h. **UnregisterID**
 - i. **DeleteVersion**
- c. Extended Loglevel:
Nur wenn per Schalter explizit definiert (siehe Auflistung 2.1).
4. Ausnahmen:
- Abhängig von dem Schalter **AUDIT_PROTOCOL_TIF_OCR** werden folgende Events nur für "Extended" Dokumentklassen bzw. gar nicht geloggt (Schalterstellung auf 0 bedeutet kein Logging):
 - i. **RenditionJobCreated_001**
 - ii. **RenditionJobProcessed_001**
 - iii. **RenditionJobCreated_002**
 - iv. **RenditionJobProcessed_002**
 - v. **RenditionJobCreated_003**
 - vi. **RenditionJobProcessed_003**
 - vii. **RenditionJobFinished**
 - viii. **RenditionJobFlagReset**
 - ix. **KeywordsSend_OnChangedType**
 - x. **KeywordsSend_OnImport**
 - xi. **KeywordsSend_OnClientAPI**
 - xii. **KeywordsSend_OnChangedNote**
 - xiii. **KeywordsSend_OnTranfer**
 - xiv. **KeywordsSend_OnNewVesion**
 - xv. **KeywordsSend_OnRenderedOcr**
 - xvi. **KeywordsSend_OnChangedAttribute**
 - xvii. **KeywordsSend_OnSynchFile**
 - xvi- **KeywordsSend_OnProcOCR001**
 - ii.
 - xix. **KeywordsSend_OnServerAPI**
 - Tritt ein Ereignis des Levels MINIMAL ein (siehe 3.1.), so wird dies in jeden Fall geloggt
 - Tritt ein Ereignis des Levels STANDARD ein (siehe 3.2.), so wird dies für Dokumente geloggt, welche einer Dokumentklasse des Levels STANDARD oder EXTENDED (siehe 1.1.) angehören.
=> D.h. es wird im Umkehrschluss NICHT für Dokumente einer Dokumentart geloggt, welcher des MINIMALEN Levels angehören.
 - Tritt ein Ereignis des Levels EXTENDED ein (siehe 3.3. / 4.), so wird dies für Dokumente geloggt, welche einer Dokumentklasse EXTENDED (siehe 1.1.) angehören.

Transportsystem

Backup der Repository-Stammdaten

MASTERDATA_BACKUP

Aktiviert das automatische Backup der Repository-Stammdaten, was periodisch vom d.3 async Master-Prozess durchgeführt wird.

Der Zeitpunkt und die Periodizität wird eingestellt über die Parameter **MASTERDATA_BACKUP_TIME** und **MASTERDATA_BACKUP_INTERVAL**.

Abgelegt wird die Backup-Datei im Dokumenten-Baum im Verzeichnis `config\d3admin\mdbbackup`.

Stammdaten-Backup Intervall

MASTERDATA_BACKUP_INTERVAL

Das Backup der Repository-Stammdaten wird in festgelegten Zeitabständen durchgeführt. Erlaubte Werte für **MASTERDATA_BACKUP_INTERVAL** sind

"T": täglich

"W": wöchentlich (immer Montags)

"M": monatlich (Der Tag wird über **MASTERDATA_BACKUP_DAYOFMONTH** eingestellt)

Mit **MASTERDATA_BACKUP_TIME** wird die Uhrzeit angegeben, wann das Backup durchgeführt werden soll.

Zeitangabe für das Backup der Repository-Stammdaten

MASTERDATA_BACKUP_TIME

Erwartet wird hier eine Uhrzeit im Format: "hh:mm".

Tag im Monat

MASTERDATA_BACKUP_DAYOFMONTH

Gibt den Tag im Monat an, an dem das Backup durchgeführt wird. Das hat nur Auswirkung, wenn der Parameter **MASTERDATA_BACKUP_INTERVAL** auf "M" steht.

E-Mail-Benachrichtigung

MASTERDATA_BACKUP_SENDEMAIL

Aktiviert die Benachrichtigung nach Durchführung eines Backups.

"0": Keine Benachrichtigung

"1": Benachrichtigung im Fehlerfall

"2": Benachrichtigung immer

Die Parameter **SMTP_SUPPORT** und **SMTP_GATEWAY** müssen gesetzt sein.

E-Mail-Adresse

MASTERDATA_BACKUP_MAILADDRESS

E-Mail-Adresse für Benachrichtigungen nach dem Backup.

Automatischer Import von Repository-Stammdaten-Dateien

MASTERDATA_IMPORT

Mit Aktivierung des Parameters kann der d.3 async Master-Prozess über Steuerdateien/Schnittstellendateien dazu veranlasst werden, Repository-Stammdaten wie Benutzer oder Benutzergruppen zu administrieren, also z.B. Benutzer anzulegen oder zu aktualisieren. Der automatische Import wird alle 5 Minuten ausgeführt.

Übernahme der Storage-Einstellungen bei Dokumentartänderungen

MASTERDATA_TRANS_DTYPE_STORAGE_SETTINGS

Mit Aktivierung des Parameters werden bei Dokumentartänderungen, die über Transportdateien importiert werden, die Storage-Einstellungen überschrieben.

Betroffen sind die folgenden Einstellungen:

- Lebensdauer -> In Monaten
- Lebensdauer -> Ab
- Lebensdauer -> Auf Sekundärspeicher auslagern

Die Einstellung "Lebensdauer -> Ereignisorientiertes Löschen" wird nicht berücksichtigt und wird somit immer transportiert.

Folgende weitere Regeln gelten:

- Bei der Neuerstellung einer Dokumentart bzw. bei direkten Dokumentartänderungen hat der Schalter keine Auswirkung.
- Jede Änderung an den Einstellungen bei den Dokumentarten wird für das Transportwesen aufgezeichnet und auch in die Transportdateien reingeschrieben.
- Wird eine Dokumentart über eine Transportdatei in ein anderes d.3-Repository übertragen, die Dokumentart existiert aber bereits, werden die Storage-Einstellungen bei deaktivierten Schaltern nicht überschrieben.

Übernahme der Caching-Einstellungen bei Dokumentartänderungen**MASTERDATA_TRANS_DTYPE_CACHE_SETTINGS**

Mit Aktivierung des Parameters werden bei Dokumentartänderungen, die über Transportdateien importiert werden, die Caching-Einstellungen überschrieben.

Betroffen sind die folgenden Einstellungen:

- Cache-Verweildauer -> In Tagen
- Cache-Verweildauer -> Vorzeitige Entfernung bei Speicherplatzmangel erlauben

Folgende weitere Regeln gelten:

- Bei der Neuerstellung einer Dokumentart bzw. bei direkten Dokumentartänderungen hat der Schalter keine Auswirkung.
- Jede Änderung an den Einstellungen bei den Dokumentarten wird für das Transportwesen aufgezeichnet und auch in die Transportdateien reingeschrieben.
- Wird eine Dokumentart über eine Transportdatei in ein anderes d.3-Repository übertragen, die Dokumentart existiert aber bereits, werden die Caching-Einstellungen bei deaktivierten Schaltern nicht überschrieben.

d.3 presentation server**d.3 presentation server - Hostname****PRESENTATION_SERVER_HOST**

Hostname des Rechners, auf dem d.3 presentation server läuft.

d.3 presentation server - TCP/IP Port**PRESENTATION_SERVER_PORT**

TCP/IP Port, unter dem d.3 presentation server erreichbar ist.

Standardwert: 8081

d.3 presentation server - HTML-Verzeichnis**PRESENTATION_SERVER_PATH**

Mit diesem Parameter wird der Kontextpfad für d.3 presentation server angegeben.

d.3 presentation server - Verschlüsselung**PRESENTATION_SERVER_SSL**

Wenn d.3 presentation server mit SSL arbeitet, muss dieser Parameter aktiviert werden.

d.3 presentation server - Sicherheitslevel

PRESENTATION_SERVER_SECURITY_LEVEL

Das Sicherheitslevel bestimmt, ob die welche Sicherheitsfeatures von d.3 presentation server und den Anwendungen genutzt werden.

0: Die neuen Sicherheitsfeatures werden nicht genutzt.

1: Die neuen Sicherheitsfeatures werden genutzt.

d.3 presentation server - Gültigkeitsdauer der URLs**PRESENTATION_SERVER_EXPIRES_SECS**

Ist das Sicherheitslevel auf mind. 1 gesetzt, wird die Gültigkeitsdauer der von d.3 server generierten URLs auf diesen Wert gesetzt. Die Angabe der Dauer erfolgt in Sekunden.

Standardwert: 60

d.3 presentation server - Mapping von d3fc-Hosts zu Presentation-Server-URLs**PRESENTATION_SERVER_MAPPING_D3FCHOST**

Hier sind die D3FC-Hosts einzutragen, welche 1 zu 1 (Indexnummer) den zugehörigen PS-URLs zugeordnet werden.

(PRESENTATION_SERVER_MAPPING_PSURI)

d.3 presentation server - Zuordnung Presentation-Server-URLs zu d3fc-Hosts**PRESENTATION_SERVER_MAPPING_PSURI**

Hier sind die PS-URLs zu den entsprechenden D3FC-Hosts einzutragen.

Beispiel: https://ps-server:8444

(PRESENTATION_SERVER_MAPPING_D3FCHOST)

Anmerkung

Damit dieses Mapping greift, darf in d.3 config für **PRESENTATION_SERVER_HOST** kein Host definiert sein.

Wird kein Mapping hinterlegt, verhält sich der API-Call wie bisher, d.h. wenn kein **PRESENTATION_SERVER_HOST** definiert ist und **d3_host** wird als Importparameter des Aufrufs mit übergeben, wird dieser als Presentation Server mit ausgegeben. Wird hingegen keiner mit übergeben, greift ein weiterer Mechanismus und der Server gibt sich selbst als PS-Host an.

d.3 presentation server - Aktivierung der HTTP-Schnittstelle von d.3 server**ENABLE_HTTP**

Bestimmt, ob die HTTP-Schnittstelle des d.3-Servers aktiviert ist.

Konfiguration über die d3addon.ini

Einige spezielle Parameter lassen sich nicht über d.3 admin einstellen. Diese Parameter lassen sich nur manuell in die Datei **d3addon.ini** eintragen.

Alle Parameter finden Sie in einer kurzen Beschreibung in der **d3fixed.ini**.

Nachdem Sie die **d3addon.ini** angepasst haben, müssen Sie die d.3-Prozesse (d.3 server, d.3 hostimp und d.3 async-Prozesse) neustarten, damit die neue Konfiguration richtig gelesen wird.

Warnung

Ändern Sie nie die Einträge in der **d3fixed.ini**! Änderungen hier können zum Stillstand des d.3-Repository und zu Datenverlust führen.

Anmerkung

Beachten Sie die Groß-/Kleinschreibung.

Erstellen Sie mit der Version ein neues Repository, wird dieses Repository mit folgenden Einträgen in der Datei **d3addon.ini** ergänzend definiert:

Diese Parameter dürfen nicht einfach manuell in einem bestehenden System gesetzt werden, da diese entsprechende Datenstrukturen voraussetzen, die ggf. dann auch erst über eine Migration hergestellt werden müssen.

Das ist auch der Grund, warum diese Parameter NICHT in der Konfigurationsdatei **d3config.ini** enthalten sind.

Parameter, die sowohl in der **d3config.ini** als auch in der **d3addon.ini** konfigurierbar sind, setzen keine Migration voraus, dürfen bei Updates aber nicht gesetzt werden, da sie sonst ggf. ein Fehlverhalten nach sich ziehen, z. B. **REVOKE_PROCESSING_ADMIN**. Bei Neuinstallationen allerdings können diese Parameter gefahrlos gesetzt werden, da das neue Verhalten dann auch i.d.R. gewünscht wird.

Im folgenden werden alle Parameter erläutert, die bei Neuinstallation in der **d3addon.ini** gesetzt sind.

CONFIG_PATH_D3CLIENT = "C:\d3\D3T.dok\config\d3client"
Pfad auf das Verzeichnis, in dem sowohl die Suchvorlagen, als auch die Anwendungsprofil-Dateien (client config) abgelegt werden.
UTF8_SUPPORT = "1"
UNICODE Unterstützung des d.3 Repository einschalten.
SEARCH_DEP_DOCS_IN_DB = "1"
Informationen zu den abhängigen Dateien werden aus der Datenbank gelesen, hier werden die Informationen verwaltet.
SUFFIX_DEP_DOCS_ARCHIVE_THREE_DIGITS = "1"
siehe hierzu ergänzend die Informationen zum alten Bezeichner
SUFFIX_ABH_ARCHIV_DREIZIFFRIG in der d3fixed.ini .
TURBO_DOC_FLAGS_2 = "1"
Dokument-Flaginformation zur Beschleunigung der d.3 Dokumentsuche
SUBDIR_VERIFICATION = "1"
Unterverzeichnisse im d.3-Verzeichnis zum Prüfungsverzeichnis erstellen/nutzen
SUBDIR_ARCHIVE = "1"
Unterverzeichnisse im d.3-Verzeichnis zum Archivverzeichnis erstellen/nutzen
SUBDIR_NOTES = "1"
Unterverzeichnisse im d.3-Verzeichnis zum Notizenverzeichnis erstellen/nutzen
SUBDIR_WFL_LOG = "1"
Unterverzeichnisse im Workflow-Protokollverzeichnis erstellen/nutzen
REVOKE_PROCESSING_ADMIN = "1"
Entzug der Bearbeitungsversion durch den Administrator erlauben
MODIFY_ATTR_DB_POSITION = "0"
Nachträgliche Änderung der DB-Position einer Eigenschaft in der Dokumentart erlauben/verbieten
ENABLE_DUMMY_WRITE_ACCESS = "0"
Schreibrecht auf Dummy-Dokumentart entziehen
VALIDATE_NUMERIC_FIELDS = "1"
Prüfung einschalten, ob eine numerisches Eigenschaft nur numerische Zeichen enthält.
OVERWRITE_NEW_ARCHIVE_PARAMS = "0"
Interner Schalter, der angibt, ob die Neuanlage-Parameter schon in die d3addon.ini geschrieben wurden.
WORKFLOW_NOTIFICATION_AUTO_ACKNOWLEDGE_ON_LOCK
1: Die Benachrichtigungen anderer Benutzer für einen Workflowschritt werden automatisch quittiert und sind damit in den Postkörben dieser Benutzer nicht mehr sichtbar, wenn ein Benutzer einen Workflowschritt zur Bearbeitung geöffnet hat und dieser Schritt deshalb gelockt ist.
0: Wurde die Benachrichtigung über eine Gruppe versendet, wird diese dem Aufrufer zugewiesen und ist für die anderen Mitglieder dieser Gruppe nicht mehr sichtbar.

D3_SERVER_HOST

Über die d.3-Server-Config-Variable **D3_SERVER_HOST** kann der Hostname angegeben werden, unter dem der d.3-Server in Cluster-Konfigurationen von außen erreichbar ist. So kann der Default-Hostname (**d3fc_server_name**) überschrieben werden. Dieser Hostname wird dann für die Erzeugung aller Workflow-URLs benutzt. Dies betrifft die API-Funktionen **GetPSUrl**, **LockWorkPathStep**. Diese Config-Variable kann in der **d3addon.ini** gesetzt werden.

1.4.5. Systemüberwachung

Unterhalb der Systemüberwachung finden Sie d.3 async job inspector und die Laufzeitinformationen.

d.3 async job inspector

d.3 async job inspector ermöglicht Ihnen die Überwachung und Steuerung der d.3 async-Aufträge, die auf dem d.3-Server im Hintergrund ausgeführt werden.

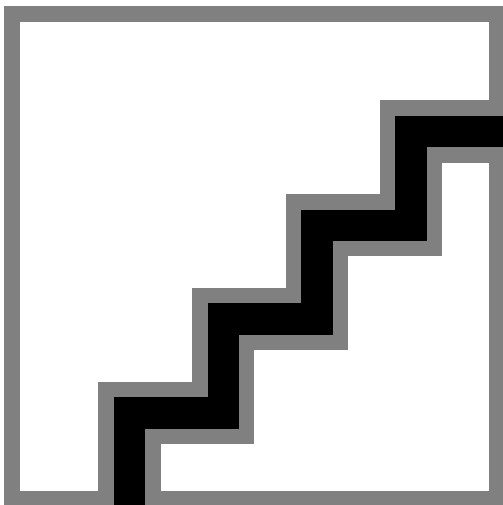


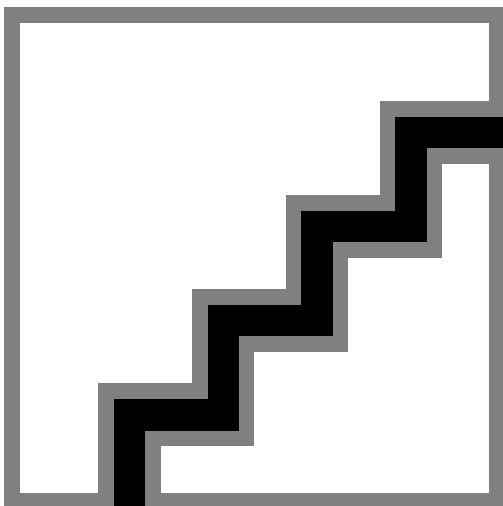
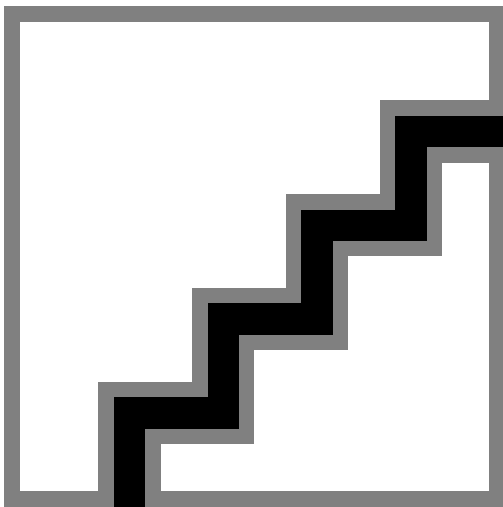
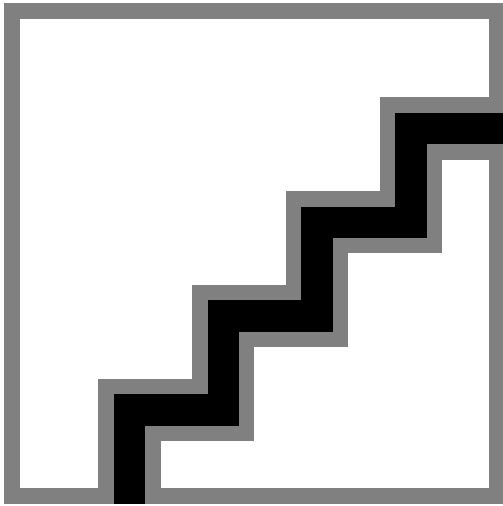
Zur Analyse von Problemen (z.B. bei der Aktenverknüpfung) ist diese Erweiterung von d.3 admin eine wertvolle Hilfe. Mit d.3 async job inspector können Sie Aufträge wiederholen lassen, löschen oder die Ausführungspriorität ändern.

Für weitere Informationen zur Verwaltung von d.3 async Jobs lesen Sie bitte das Handbuch d.3 admin async job inspector.

Laufzeitinformationen

In d.3 admin erhalten Sie über **Systemüberwachung > Laufzeitinformationen** einen Überblick über verschiedene Laufzeitinformationen der letzten Tage/Stunden eines Repositorys.



**Elemente:**

Die Laufzeitinformationen bestehen aus folgenden Anzeigeelementen:

- **Jobübersicht:**
Eine Auflistung der verschiedenen Jobtypen auf der linken Seite. Hier kann zu jedem Jobtyp die Gesamtzahl der dafür abgesetzten Ereignisse (Calls) innerhalb des selektierten Zeitrahmens (Zeitleiste) abgelesen werden.

- **Zeitleiste:**
Eine horizontal verlaufende Auswahlleiste am oberen Rand. Die dargestellte Zeitspanne entspricht dem maximalen Zeitraum der erfassten Daten (siehe Parameter `RUNTIME_INFO_DAYS_OF_DB_STORAGE`). Hier kann zudem der aktuell zur Anzeige selektierte Zeitraum abgelesen werden.
- **Zeitdiagramm:**
Die selektierten Daten werden in Diagrammen unterhalb der Zeitleiste visualisiert. Innerhalb der Diagramme sind jeweils verschiedene Kurven (Total time, SQL time, Hook time, Filesystem time, Service time und K/V-Store time) auswählbar, wobei initial jeweils die Gesamtlaufzeit gezeigt wird und die anderen Kurven zusätzlich eingeblendet werden können. Das erste (oberste) Diagramm stellt das Hauptdiagramm da, bei diesem steht zusätzlich zu den anderen Diagrammen die Schaltfläche **Add Chart** zu Verfügung um das Hinzufügen weiterer Diagramme zu ermöglichen.

Bedienung/Ablauf:

In der initialen Ansicht der Laufzeitinformation werden die Daten aller Jobs des gesamten Datenzeitraumes im Hauptdiagramm visualisiert.

Um die anzuzeigenden Daten nach bestimmten Kriterien zu filtern stehen mehrere, ineinander greifende Mechanismen zu Verfügung:

- Über die Jobübersicht kann ein spezifischer Jobtyp in den Ansichtsfiler aufgenommen werden während ein erneutes Anklicken den Jobtyp wieder aus dem Filter löscht. Der Ansichtsfiler kann beliebig viele Jobtypen enthalten.
Enthält der Ansichtsfiler mindestens ein Element (Job), so ist dieser aktiv und alle nicht enthaltenen Jobtypen werden in der Jobübersicht ausgegraut bzw. in den Zeitdiagrammen nicht mehr angezeigt.
- Über die Zeitleiste ist es möglich mit der Maus einen Zeitbereich zu selektieren (Linke Maustaste gedrückt halten, ziehen und loslassen).
Die Anzeige der Ereignisse in der Jobübersicht passt sich dem ausgewählte Zeitbereich an. Zudem zoomen die Zeitdiagrammen auf diesen Bereich heran, während die Auflösung der angezeigten Daten in Abhängigkeit der selektierten Zeitspanne gegebenenfalls erhöht wird um in dieser detaillierteren Ansicht mehr Information zu bieten. Die Zeit- und Laufzeitachse der Zeitdiagramme skalieren entsprechend der anzuzeigenden Daten automatisch mit.
- Innerhalb des Hauptdiagramms kann der ausgewählte Datenbereich über das Mauseisen noch weiter verfeinert (bzw. die Verfeinerung auch wieder rückgängig gemacht) werden. Hierbei folgt das gleiche Verhalten wie es bei der (gröberen) Selektion über die Zeitleiste zu tragen kommt.
- Sowohl innerhalb der Zeitleiste, als auch im Hauptdiagramm kann der ausgewählte Zeitbereich durch die Maus (gedrückte linke Maustaste) verschoben werden.

Über die **Add Chart**-Schaltfläche im Hauptdiagramm können bis zu fünf zusätzliche Zeitdiagramme erzeugt werden. Diese erscheinen jeweils direkt unterhalb des Hauptdiagramms während die bereits zuvor erzeugten Diagramme somit nach unten geschoben werden. Die visualisierten Daten entsprechen den, durch die Zeit- und Jobauswahl festgelegten Kriterien. Auch der Zoom des Hauptdiagramms wirkt sich direkt auf diese zusätzlichen Diagramme aus.

Die so erzeugten Diagramme haben zwei Schaltflächen:

- Eine Schaltfläche mit einem Minuszeichen: Durch Anklicken kann das jeweilige Zeitdiagramm ausgeblendet werden. Im ausgeblendeten Zustand ist nur noch die Minus-Schaltfläche (nun mit einem Plus-Symbol statt dem Minus) und die **Remove**-Schaltfläche zu sehen.
Ein erneutes anklicken der Schaltfläche zeigt das Diagramm wieder an. Zuvor innerhalb des Diagramms getroffene Einstellungen bleiben erhalten.
- Eine **Remove**-Schaltfläche: Durch Anklicken wird das jeweilige Zeitdiagramm entfernt. Dadurch verschwindet das jeweilige Zeitdiagramm mitsamt seiner Schaltflächen und den jeweils getroffenen Einstellungen vollständig. Die sich darunter befindlichen Diagramme rücken nach oben auf.

Innerhalb eines jeden einzelnen Zeitdiagramms kann frei und beliebig kombinierbar die gewünschte Zeitlinie ein- und ausgeblendet werden. Die Zeitlinie "Total time" spiegelt einfach die Summe der spezifischen Zeiten wieder.

Jeder angezeigte Datenpunkt innerhalb der Diagramme spiegelt ein oder auch mehrere zusammengefasste Ereignisse wieder. Für die Zeitlinie "Total time" erscheint als Tool-Tip (die Maus auf dem jeweiligen Datenpunkt positionieren und einen Moment dort belassen) eine detailliertere Information bezüglich der verursachenden Jobtypen (ist nur ein Jobtyp beteiligt, so wird dieser direkt mit angezeigt) und der zugrunde liegenden Calls angezeigt. Für die übrigen Zeitlinien erscheint als Information der exakte Zeitwert des jeweiligen Zeittyps.

1.4.6. Weitere Dienste

Zu den weiteren Diensten gehören d.3 abo service , d.3 search , d.ecs rendition service und die Formularzuordnung.

d.3 search

d.3 search dient zur Volltextsuche im d.3-Repository. Detaillierte Informationen hierzu entnehmen Sie der entsprechenden Dokumentation.

d.ecs rendition service

d.ecs rendition service dient zur serverseitigen Vertiffung und wird in einer eigenen Dokumentation näher beschrieben.

Formularzuordnung

Die Formularzuordnung bezieht sich auf das Prozessportal und wird in der eigenständigen Dokumentation Prozessportal und Formularintegration beschrieben.

1.4.7. Webhooks

In diesem Kapitel erhalten Sie Informationen über Webhooks in d.3 admin.

Arbeiten mit Ereignissen

Mit Webhooks können Sie auf Ereignisse reagieren, die von bestimmten Prozessen in einem Repository ausgelöst werden. Zusätzlich können Sie mit den HTTP-Antworten Ihrer Webhooks die Ausführung der Prozesse beeinflussen.

Um einen Webhook zu konfigurieren, müssen Sie eine URI bereitstellen. Diese URI wird beim Auftreten des Ereignisses aufgerufen. Sie können für ein Ereignis mehrere Webhooks konfigurieren. Diese Webhooks werden beim Eintreten des Ereignisses nacheinander aufgerufen.

Tragen Sie die Konfigurationen der Webhooks im Menüeintrag **Webhooks** für die gewünschten Ereignisse ein.

Für eine Reihe von Ereignissen, die bei der Arbeit mit Dokumenten in einem Repository auftreten können, lassen sich Webhooks aufrufen.

- Suchen
- Dokumente und Akten erstellen
- Neue Version erstellen
- Eigenschaften aktualisieren
- Dokumente und Akten löschen
- Elemente verknüpfen
- Status ändern
- Generiertes Dokument erstellen

Wenn das Ereignis eintritt, wird an jede eingetragene URL eine HTTP-POST-Anforderung gesendet. Abhängig vom gewählten Ereignis werden im Body der HTTP-POST-Anforderung verschiedene Informa-

tionen an den Webhook übergeben z. B. zu einem gespeicherten Dokument. Diese Informationen kann der Webhook verwenden, um auf Basis der Informationen weitere Aktionen zu starten.

Für jedes Ereignis werden im Folgenden die Informationsobjekte beschrieben.

Suchen

Diese Ereignisse werden ausgelöst, wenn Anwendende eine Suche im Repository ausführen.

- Ereignis 1: Vor dem Suchen

Das Ereignis wird vor einer Suche aufgerufen. Die übergebenen Suchkriterien sind zu dem Zeitpunkt noch nicht auf Plausibilität geprüft worden.

- Ereignis 2: Nach dem Suchen

Das Ereignis wird am Ende der Suche aufgerufen, direkt bevor die Ergebnisse an den Benutzer geliefert werden.

Dokumente und Akten erstellen

Diese Ereignisse werden ausgelöst, wenn ein neues Dokument oder eine Akte im Repository gespeichert wird.

- Ereignis 1: Ablagedialog überprüfen

Das Ereignis wird aufgerufen, wenn einem neu importierten Dokument Eigenschaften zugewiesen wurden.

- Ereignis 2 Vor dem Erstellen eines Dokuments oder einer Akte

Das Ereignis wird aufgerufen, bevor Anwendende ein Dokument oder eine Akte erstellen. Du kannst die Werte der erweiterten Eigenschaften im Webhook ändern.

- Ereignis 3: Nach dem Erstellen eines Dokuments oder einer Akte

Das Ereignis wird aufgerufen, nachdem Anwendende ein Dokument oder eine Akte erstellt haben. Der Prozess ist bei diesem Ereignis bereits abgeschlossen.

Neue Version erstellen

Diese Ereignisse werden ausgelöst, wenn eine neue Version eines Dokuments im Repository gespeichert wird.

- Ereignis 1: Vor dem Erstellen einer neuen Version

Das Ereignis wird aufgerufen, bevor Anwendende eine neue Version eines Dokuments erstellen. Bei diesem Ereignis wurde geprüft, ob das Dokument bereits im Repository existiert. Die erweiterten Eigenschaften können sich du zu diesem Zeitpunkt noch ändern.

- Ereignis 2: Nach dem Erstellen einer neuen Version

Das Ereignis wird aufgerufen, nachdem Anwendende eine neue Version eines Dokuments erstellt haben. Der Prozess ist bei diesem Ereignis bereits abgeschlossen.

Eigenschaften aktualisieren

Diese Ereignisse werden ausgelöst, wenn die Eigenschaften eines Dokuments oder einer Akte geändert werden.

- Ereignis 1: Eigenschaften überprüfen

Das Ereignis wird aufgerufen, wenn die Dokumenteigenschaften überprüft werden.

- Ereignis 2: Vor dem Aktualisieren von Eigenschaften

Das Ereignis wird aufgerufen, bevor die Eigenschaften eines Dokuments aktualisiert werden. Du kannst die Werte der erweiterten Eigenschaften im Webhook ändern.

- Ereignis 3: Nach dem Aktualisieren von Eigenschaften

Das Ereignis wird aufgerufen, nachdem die Eigenschaften eines Dokuments aktualisiert wurden. Der Prozess ist bei diesem Ereignis bereits abgeschlossen.

Dokumente und Akten löschen

Diese Ereignisse werden ausgelöst, wenn ein Dokument oder eine Akte aus dem Repository entfernt wird.

- Ereignis 1: Vor dem Löschen eines Dokuments oder einer Akte

Das Ereignis wird aufgerufen, bevor ein Benutzer ein Dokument oder eine Akte löscht. Zu diesem Zeitpunkt wurde bereits geprüft, ob der Benutzer das Dokument löschen darf.

- Ereignis 2: Nach dem Löschen eines Dokuments oder einer Akte

Das Ereignis wird aufgerufen, nachdem ein Benutzer ein Dokument oder eine Akte gelöscht hat. Der Prozess ist bei diesem Ereignis bereits abgeschlossen.

Elemente verknüpfen

Ereignisse des Typs **Elemente verknüpfen** werden ausgelöst, wenn zwei Elemente miteinander verknüpft werden. Das Ereignis wird bei folgenden Verknüpfungen ausgelöst:

1. Ein Dokument wird mit einer Akte verknüpft.
2. Ein Dokument wird mit einem anderen Dokument verknüpft.
3. Eine Akte wird mit einer anderen Akte verknüpft.

- Ereignis 1: Vor dem Verknüpfen von Elementen

Das Ereignis wird aufgerufen, bevor zwei Elemente verknüpft werden.

- Ereignis 2 Nach dem Verknüpfen von Elementen

Das Ereignis wird aufgerufen, nachdem zwei Elemente verknüpft wurden. Der Prozess ist bei diesem Ereignis bereits abgeschlossen.

Status ändern

Diese Ereignisse werden ausgelöst, wenn der Status eines Dokuments geändert wird.

- Ereignis 1: Vor dem Ändern des Status

Das Ereignis wird aufgerufen, bevor der Dokumentstatus geändert wird.

- Ereignis 2: Nach dem Ändern des Status

Das Ereignis wird aufgerufen, nachdem der Dokumentstatus geändert wurde. Der Prozess ist bei diesem Ereignis bereits abgeschlossen.

Generiertes Dokument erstellen

Diese Ereignisse werden ausgelöst, wenn zu einem Dokument eine neue, abhängige Datei gespeichert wird. In einem Repository wird dieses Ereignis durch die automatische Generierung eines langzeitstabilen PDF-Abbilds des Dokuments ausgelöst.

- Ereignis 1: Vor dem Erstellen eines generierten Dokuments

Das Ereignis wird aufgerufen, bevor eine neue abhängige Datei gespeichert wird.

- Ereignis 2: Nach dem Erstellen eines generierten Dokuments

Das Ereignis wird aufgerufen, nachdem eine neue abhängige Datei gespeichert wurde. Der Prozess ist bei diesem Ereignis bereits abgeschlossen.

Konfigurieren von Webhooks

Sie können den jeweiligen Ereignissen zugeordnete Webhook-Einträge bearbeiten, hinzufügen oder löschen.

Webhooks werden beim Eintreten des Ereignisses nacheinander aufgerufen. Sie können die Reihenfolge der Abarbeitung verändern mit **Reihenfolge bearbeiten**. Mit **Position** verschieben Sie einen markierten Webhook-Eintrag innerhalb der Liste.

Mit **Aktualisieren** können Sie die Webhook-Konfiguration vom Server neu laden lassen.

Mit **Export** und **Import** können Sie die Webhook-Konfigurationen exportieren und importieren. Die Konfigurationsdaten werden als **JSON**-Datei übertragen.

Tragen Sie als Konfigurationskennung einen Namen für den Webhook ein. Die ID des Webhooks wird automatisch generiert und kann nicht geändert werden.

Die **URI** bestimmt die Webadresse, die beim Eintreten eines Ereignisses aufgerufen wird. Das System unterstützt absolute HTTP-Adressen und relative Pfadangaben für lokale Webadressen. Während der Eingabe erfolgt eine einfache Plausibilitätsprüfung der URI, aber keine Prüfung der Verbindung.

Wählen Sie **Webhook aktivieren** aus, um den Webhook im DMS-System zu aktivieren.

Auswerten der Antwort des Webhooks

Sie können festlegen, ob und wie die HTTP-Antwort Ihres Webhooks vom DMS-System ausgewertet werden soll.

Verwenden Sie **Nicht auf Antwort warten** für Webhooks, die nicht auf den laufenden Prozess einwirken müssen. Der Aufruf des Webhooks geschieht asynchron. Das DMS-System wartet nicht auf eine HTTP-Antwort. Die Laufzeit des Prozesses wird nicht beeinträchtigt.

Verwenden Sie **Statuscode berücksichtigen** für Webhooks, die den Prozess abbrechen können. Der Aufruf des Webhooks geschieht synchron und die HTTP-Antwort wird abgewartet. Das DMS-System wertet nur den Statuscode der HTTP-Antwort aus. Mit dem Statuscode kann der laufende Prozess abgebrochen werden. Der Webhook muss dafür einen Statuscode im Bereich von 400 bis 499 zurückgeben.

Verwenden Sie **Statuscode berücksichtigen und Antwort auswerten** für Webhooks, die den Prozess abbrechen oder verändern. Der Aufruf des Webhooks geschieht synchron und die HTTP-Antwort wird abgewartet. Das DMS-System wertet den Statuscode und den Inhalt der HTTP-Antwort aus.

Einschränken auf eine bestimmte Kategorie

Mit **Nur für diese Kategorie ausführen** schränken Sie die Ausführung der Webhooks auf eine Kategorie ein. Wenn Sie keine Kategorie auswählen, dann wird der Webhook für jede Kategorie aufgerufen.

Festlegen eines Authentifizierungsschlüssels

Mit der Option **API-Key** legen Sie einen Authentifizierungsschlüssel fest. Dieser Authentifizierungsschlüssel wird beim HTTP-Aufruf des Webhooks mitgesendet. Dadurch kann der Webhook überprüfen, ob der HTTP-Aufruf tatsächlich von dem DMS-System stammt. Authentifizierungsschlüssel werden nur gesendet, wenn Sie als URI eine relative URI angegeben haben.

Wählen Sie das Sternchen (*) neben dem Eingabefeld aus, um den API-Key als Klartext anzuzeigen.

Anmerkung

Mit der neusten Version wird statt „x-dv-api-key: APIKEY“ nun „Authorization: Bearer APIKEY“ als Header an den Webhook übergeben.

Beeinflussen der Performance

Verwenden Sie **Timeout in Millisekunden**, um festlegen, wie lange das DMS-System auf die HTTP-Antwort des Webhooks wartet. Nach Ablauf des Timeouts wird die HTTP-Anfrage abgebrochen.

Aktivieren Sie die Timeout-Wiederholung mit **Webhook bis zu drei Mal aufrufen, falls ein Timeout oder eine fehlerhafte Antwort auftritt**. Wenn ein Timeout auftritt, wird die HTTP-Anfrage erneut ausgeführt. Die HTTP-Anfrage wird maximal vier Mal gesendet, bevor sie endgültig verworfen wird.

Informationsfelder

Im Textfeld **ID** wird die interne Identifikation des Webhooks angezeigt. Das Textfeld **Entry point** zeigt die interne Zuordnung des Webhooks zu einem Ereignis an.

1.4.8. Wertemengen-Webhooks

In diesem Abschnitt erfahren Sie, wie Sie Wertemengen-Webhooks konfigurieren.

Was sind Wertemengen-Webhooks?

Eine Wertemenge ist eine Liste, mit der Sie Eigenschaftswerte auswählen können. Wenn Sie einer Dokumenteigenschaft eine Wertemenge zuweisen, dann können Anwendende nur Werte aus dieser Wertemenge auswählen.

Der Wertemengen-Webhook ist eine Konfiguration, mit der sich ein Wertevorrat dynamisch von einer Webadresse laden lässt.

Arbeiten mit Wertemengen-Webhooks

Aus der Liste der Wertemengen-Webhooks können Sie Einträge bearbeiten, hinzufügen oder löschen.

Mit **Export** und **Import** können Sie die Konfigurationen exportieren und importieren. Die Konfigurationsdaten werden als **JSON**-Datei übertragen.

Zum Verwenden der Wertemengen-Webhooks wählen Sie unter **Erweiterte Eigenschaften > Zuordnung** von Wertevorräten als Wertevorrat **Webhook** aus. Wählen Sie ebenfalls eine Bezeichnung aus.

Datentypen

Beim Erstellen einer Webhook-Wertemenge wird automatisch der Datentyp **Dynamische Abfrage (Webhook)** ausgewählt. Sie können den Datentyp nicht ändern.

Festlegen der Webhookwerte

Tragen Sie als Konfigurationskennung einen Namen für den Webhook ein. Die Webhook-ID wird automatisch generiert und kann nicht geändert werden.

Die **URI** bestimmt die Webadresse, von der die Wertemenge als Ressource geladen wird. Das System unterstützt absolute HTTP-Adressen, sowie relative Pfadangaben für lokale Webressourcen. Während der Eingabe erfolgt eine einfache Plausibilitätsprüfung der URI, aber keine Prüfung der Verbindung.

Mit der Option **API-Key** legen Sie einen Authentifizierungsschlüssel fest. Wählen Sie das Sternchen (*) neben dem Eingabefeld aus, um den API-Key als Klartext anzuzeigen.

Verwenden Sie **Timeout in Millisekunden**, um festzulegen, wie lange das DMS-System auf die HTTP-Antwort des Webhooks wartet. Nach Ablauf des Timeouts wird die HTTP-Anfrage wiederholt und nach maximal drei Fehlerversuchen abgebrochen.

Im Textfeld **ID** wird die interne Identifikation des Wertemengen-Webhooks als Information angezeigt.

1.5. Allgemeine Erläuterungen

Nachfolgend finden Sie Informationen u.a. zu den Themen:

- Struktur des elektronischen d.3-Repository
- Fallbeispiel
- Erweiterte Eigenschaften-Felder
- Plausibilitätskontrolle
- Zuordnung von Wertevorräten
- Verwendung von Hook-Funktionen
- Berechtigungskonzept
- Hinweise zum Transportsystem

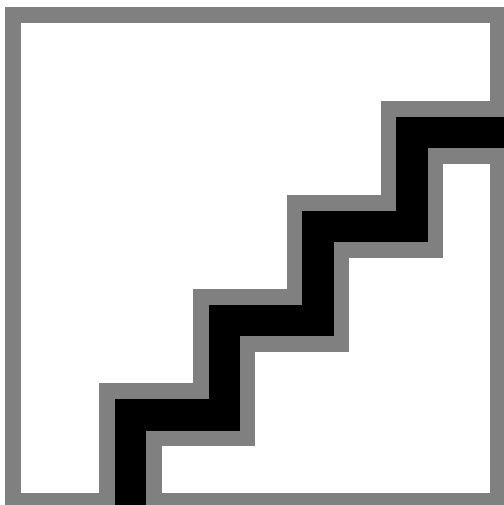
1.5.1. Struktur des elektronischen d.3-Repository

Im Prinzip ist das d.3-Repository (früher auch "Archiv" genannt) ähnlich aufgebaut wie ein typischer Aktenschrank (Repositorium). Auch der Aktenschrank ist in bestimmter Weise organisiert, damit Sie schnell Ihre Akten und Dokumente finden. Sie können die Dokumente in Schubladen oder Fächern nach Dokumentarten oder Akten klassifizieren und deshalb schnell wiederfinden.

Im Aktenschrank können Dokumente jedoch nur anhand eines Merkmals, nämlich des Aufbewahrungsortes, wiedergefunden werden. Im d.3-Repository ist das anders. Dokumentarten erhalten eine Reihe frei definierbarer Merkmale (Eigenschaften), mit deren Hilfe nach den zugehörigen Dokumenten gesucht werden kann. Diese Eigenschaften können z.B. das Datum oder der Dokumentname sein.

Ein Teil dieser Eigenschaften definiert den im Repository (eine Art elektronisches Archiv) nur noch scheinbar vorhandenen Aufbewahrungsort, der durch eine Kategorie (Dokumentart oder Aktenart) bestimmt wird.

Das Sichern vor unbefugtem Zugriff ist im d.3-Repository auf ähnliche Weise wie in einem Aktenschrank sichergestellt.



Einen festgelegten Aufbewahrungsort gibt es im d.3-Repository nicht. Vielmehr ist es in d.3 möglich, Dokumente in mehreren logischen Akten abzulegen, ohne sie mehrfach zu speichern. Dadurch können

Sie beispielsweise Ihre Rechnungen in einer Bestell- und Kundenakte ablegen und wiederfinden. So vermeiden Sie Redundanz: In verschiedenen Akten gibt es Verweise auf dasselbe Dokument.

Unternehmensinterne Verteiler- und Postwege werden vermieden. Einmal elektronisch archivierte Dokumente stehen allen berechtigten Benutzern unmittelbar zur Verfügung und können bei Bedarf auch in einem Geschäftsprozess genutzt werden.

1.5.2. Fallbeispiel

Die Möglichkeiten, die Sie beim Repositorydesign mit d.3 haben, sollen im Folgenden an einem kleinen Fallbeispiel erläutert werden:

In einem Unternehmen sollen ausgehende Bestellungen und dazu gehörende eingehende Auftragsbestätigungen und Rechnungen in einer gemeinsamen Bestellakte gesammelt werden. Bestellakten zu einem Lieferanten sollen in einer gemeinsamen Lieferantenakte gesammelt werden.

Die Aktenstruktur sieht demnach wie folgt aus:



Beim Import einer Bestellung soll eine Bestellakte angelegt werden, in welche der Lieferantennamen und das Bestelldatum gespeichert werden. Die Bestellakte wird mit der Lieferantenakte verknüpft. Existiert diese noch nicht, wird sie angelegt.

Die Lieferantenakte enthält den Lieferantennamen, sowie die Anschrift und die Kundennummer. Die Informationen werden anhand des Lieferantennamen aus einer Datenbanktabelle übernommen.

Die Auftragsbestätigung enthält den Lieferantennamen und das Datum. Die Rechnung enthält zusätzlich noch den Rechnungsbetrag. Demnach sind folgende Eigenschaften notwendig:

- Lieferant: alphanumerischer Wert, 35-stellig
- Anschrift: alphanumerischer Wert, 35-stellig
- PLZ Ort: alphanumerischer Wert, 35-stellig
- Kundennummer: alphanumerischer Wert, 35-stellig
- Datum: Datumswert
- Rechnungsbetrag: numerisch, 0.00 - 9999999.99

1.5.3. Erweiterte Eigenschaften Felder

Die frei definierbaren Eigenschaften werden zunächst für alle Dokument- und Aktenarten erstellt und gesammelt.

Durch die Verwendung gleicher erweiterter Eigenschaften Felder in unterschiedlichen Dokument- und Aktenarten lassen sich verwandte Dokumente auch dokumentartübergreifend suchen.

So können Sie beispielsweise den Auftrag, die zugehörige Rechnung und weitere zugehörige Dokumente anhand der "Auftragsnummer" wiederfinden.

1.5.4. Plausibilitätskontrolle

Bei einigen erweiterten Eigenschaften Feldern ist es notwendig oder wünschenswert, dass die Eingabe in einer bestimmten Weise reglementiert wird.

Angenommen, die Eingabe der Eigenschaft "Auftragsnummer" soll so reglementiert werden, dass nur die Eingabe von einem Großbuchstaben, gefolgt von sieben Ziffern erlaubt ist.

In diesem Fall kann ein so genannter "Regulärer Ausdruck" (Regular Expression) angegeben werden, der nur eine Eingabe der gewünschten Form zulässt.

Bei einer "Regular Expression" handelt es sich, bildlich gesprochen, um eine Art Schablone, die nur Eingaben der gewünschten Form zulässt und andere als fehlerhaft zurückweist.

Zur Eingabe von "Regular Expressions" wird eine Sprache verwendet, auf die im Verlauf des Handbuchs noch näher eingegangen wird.

Für das o.g. Beispiel könnte beispielsweise folgende "Regular Expression" verwendet werden, um die Eingabe wie gewünscht zu reglementieren:

```
[A-Z][0-9]\{7\}
```

1.5.5. Zuordnung von Wertevorräten

In manchen Fällen kommt es vor, dass zu einem erweiterte Eigenschaften Feld nur eine begrenzte Auswahl von festen Werten verwendet werden darf. Der Anwender kann/muss bei der Eingabe einer Eigenschaft (beim Suchen und/oder Archivieren) aus einer Pulldown-Liste einen vordefinierten Wert auswählen.

Angenommen, Sie sammeln Schriftwechsel in einer Dokumentart und anhand einer Eigenschaft "Ein/Aus" unterscheiden Sie, ob es sich um eingehende oder ausgehende Post handelt. Die erlaubten Werte für die Eigenschaft "Ein/Aus" heißen somit "Eingang" und "Ausgang".

Die Lösung des Problems besteht in der Verwendung eines Wertevorrats, aus dem ein Wert verwendet werden muss. Dieser Wertevorrat lässt sich vom d.3-Administrator anlegen, aus einer Datenbanktabelle des d.3-Repository entnehmen oder über neue Funktionen bereit gestellt werden. Über den Aufruf einer Hook-Funktion kann der Wertevorrat auch aus einer externen Tabelle entnommen werden.

Im ersten Fall kann in d.3 admin eine Wertemenge erstellt werden. Im zweiten Fall kann eine zusätzliche Datenbanktabelle in der d.3-Datenbank angelegt werden, aus der d.3 den Vorrat an Werten bezieht.

Es ist auch möglich, Werte über eine Datenbank-View zu liefern. Diese Datenbank-View darf allerdings dann nur eine Spalte zurückliefern.

Anmerkung

Der Wertevorrat kann als Vorgabe/Vorschlag für ein geeignetes erweiterte Eigenschaften Feld definiert werden. Ob in der Anwendung das Feld dann einen Werte aus der Liste enthalten muss oder ob zusätzliche Eingaben erlaubt werden, wird in den Eigenschaften bei der Dokumentart festgelegt.

Anmerkung

Mit einem Wertemengen-Webhook kann ein Wertevorrat dynamisch von einer Webadresse geladen und einem Eigenschaftsfeld zugewiesen werden. Zum Wertevorrat **Webhook** wird ein Webhook aus der Liste der konfigurierten Wertemengen-Webhooks zugewiesen.

1.5.6. Verwendung von Hook-Funktionen

Angenommen, die "Bestellnummer" der Dokumentart "Bestellung" soll von d.3 automatisch vergeben werden, wobei die ersten zwei Buchstaben von der Person abhängen sollen, welche die Bestellung angenommen hat und die folgenden Ziffern eine fortlaufende Nummer darstellen sollen.

Um diesen Vorgang zu automatisieren, kann man Hook-Funktionen verwenden. Eine Hook-Funktion ist eine auf dem d.3-Server ablaufende Funktion, welche kundenspezifische Aufgaben löst.

Anmerkung

Hook-Funktionen werden auf Anfrage kundenspezifisch entwickelt. Wenn Sie eigene Hook-Funktionen erstellen möchten, sollten Sie unbedingt an einer Schulung bei der d.velop AG teilnehmen.

1.5.7. Berechtigungskonzept

Das Berechtigungskonzept in d.3 legt fest, "Wer auf Was Wie zugreifen darf".

Im Berechtigungskonzept bestimmen Sie über [Dokumentklassen](#) das Was, z.B. eine Teilmenge aller Dokumente einer Dokumentart. Bsp: Nur Dokumente mit einem bestimmten Buchungskreis.

Berechtigungskonzept allgemein

Die Art des Zugriffs, also das Wie, kann die folgenden Ausprägungen haben (z.T. noch erweiterbar):

Lesen



Schreiben



Statuswechsel



Verknüpfungen von Dokumenten in eine Akte oder ein anderes Dokument.



Zu allen Rechten treffen Sie Festlegungen:

Recht erteilt: Voraussetzung, dass ein User überhaupt auf ein Dokument zugreifen darf

Recht verweigert: explizite Verweigerung eines Rechtes, kann nicht mehr übersteuert werden

Recht ignoriert: Recht wird weder erteilt, noch verweigert; wird über andere Ebenen keine Entscheidung getroffen, gilt das Recht als nicht erteilt (implizite Verweigerung des Rechtes)

Das Berechtigungskonzept erlaubt die Vergabe von Restriktionen über Attribute, die wiederum in Berechtigungsprofilen (ehemals Rollen) zusammengefasst werden, um gemäß eines Aufgabenbereichs die nötigen Zugriffe zu gestatten. Es ist aber ebenso möglich, Rechte explizit zu verbieten.

Weiterhin gibt das Berechtigungskonzept an, welcher Anwender überhaupt mit dem Repository arbeiten darf (Policies).

Berechtigungsprofile und Dokumentklassen

Im Berechtigungskonzept ab der Version 7 werden nur noch **Berechtigungsprofile** und **Dokumentklassen** zur Vergabe von Berechtigungen verwendet. Berechtigungsprofile werden dazu verwendet, mehrere Dokumentklassen zusammenzufassen und das jeweilige Zugriffsrecht auf die Klasse zu definieren.

Berechtigungsprofile erhalten eine Ansammlung von Dokumentklassen, die Mitarbeiter für ihre Aufgaben benötigen.

Eine Dokumentklasse kann sich auf eine spezielle Dokumentart beziehen oder übergreifend auf alle Dokumentarten, die in einem Berechtigungsprofil zusammengefasst werden. Wenn sich eine Dokumentklasse auf eine spezielle Dokumentart bezieht, können Sie bei den Eigenschaften dieser Dokumentart die Beschränkungen angeben.

Eine Klasse können Sie sich als eine Schablone über eine (oder dokumentart-unabhängig über alle) Dokumentart(en) vorstellen, die nach bestimmten Kriterien filtert. Mit Dokumentklasse bestimmen Sie Teilmengen aller Dokumente, über ein Profil lassen sich mehrere dieser Schablonen kombinieren.

Beispiel: In Ihrem d.3-Repository ist die Dokumentart "Rechnungen" definiert. Diese Dokumentart hat insgesamt zehn Eigenschaften. Eines dieser Eigenschaften ist das Feld mit der Bezeichnung "Rechnungs-Betrag" vom Typ "numerisch". Wenn Sie beim Anlegen der Dokumentklasse nun als Dokumentart "Rechnungen" auswählen, können Sie in dem Feld "Rechnungs-Betrag" den Wert "-5000" eintragen. Dieser Wert besagt: alle Rechnungen bis zu einem Rechnungsbetrag von 5.000 (Währungseinheiten!).

Beschreibung der Dokumentklassen:

- Eine Dokumentklasse ist eine dynamische Menge von d.3-Dokumenten.
- Eine Dokumentklasse wird durch "Suchkriterien" in d.3 charakterisiert.
- Per Standard ist jede Dokumentart eine Dokumentklasse, denn beim Anlegen einer neuen Dokumentart wird automatisch eine Standarddokumentklasse erzeugt, die denselben Namen hat wie die Dokumentart. Bei den Standarddokumentklassen beginnt das Klassenkürzel mit der Bezeichnung CLAS_. Zusätzlich wird an den Namen der Standarddokumentklasse die Bezeichnung (K) angehängt. Bei englischen d.3-Installationen wird die Bezeichnung (C) angehängt.
- Eine Dokumentklasse ist normalerweise eine Untermenge einer Dokumentart. Man kann jedoch auch Dokumentklassen bilden, die dokumentartübergreifend sind.

Beispiele für Dokumentklassen

- alle Rechnungen (Standardklasse)
- alle Rechnungen, deren Rechnungsbetrag größer als 100000 ist.
- alle Bestellungen von Lieferant „Müller“
- alle Sachnummern mit Muster S30854-%-123_-%
- alle Zeichnungen zum Projekt mit der Nummer XY4711
- alle Dokumente eines Firmenstandorts
- alle Dokumente eines Mandanten

Berechtigungsprofile

- Ein Berechtigungsprofil ist eine Zusammenfassung von Kombinationen aus Dokumentklassen und zugehörigen Rechten.
- Ein Berechtigungsprofil kann das technische Gegenstück zum Aufgabenbereich von Mitarbeitern (Abteilung etc.) sein, d.h. es werden alle Informationen zusammengefasst, auf die z.B. ein Sachbearbeiter für den Einkauf Europa Zugriff haben muss.
- Da einem Mitarbeiter mehrere Profile zugeordnet werden können, kann z.B. bei leitenden Personen die Berechtigung auch ergänzt werden.
- Ebenso ist es möglich, ein ("globales") Profil zuzuordnen, durch das Rechte wieder entzogen werden (Konträrrechte).
- Durch ein Berechtigungsprofil wird somit ein Rechteprofil auf Dokumente definiert. Dadurch, dass Benutzern diese Berechtigungsprofile zugewiesen werden, erhalten sie ihre Rechte auf die Dokumente.
- Einem Benutzer können beliebig viele Berechtigungsprofile zugewiesen werden.

Anmerkung

Zur flexibleren Handhabung können Benutzern direkt Kombinationen (Dokumentklasse, Recht) zugeordnet werden. Das sollte aber eher als Ausnahme genutzt werden, z.B. um schnell den Zugriff auf Dokumente zu sperren.

Beispiel: Berechtigungsprofil eines Projektmitarbeiters Projekt XY

Dokumentklasse - Recht

Rechnungen zum Projekt XY mit Betrag kleiner 10.000 - Lesen freigegebener Dokumente

Zeichnungen zum Projekt XY - Statuswechsel geprüft

Korrespondenzen zum Projekt XY - Bearbeiten (inhaltlich und Eigenschaften)

Rechte

Für jede Dokumentklasse innerhalb eines Berechtigungsprofils werden Rechte festgelegt. Folgende Rechte können einer Dokumentklasse zugeordnet werden:

- Lesen
- Schreiben (anlegen, löschen, bearbeiten, versionieren)
- Statuswechsel (prüfen, geprüft, freigeben)
- Verknüpfungen erstellen und lösen

Zu allen Rechten können auch die Konträrrechte vergeben werden (Verweigerung dieses Rechtes). Ein explizites Verweigerungsrecht kann auf der Ebene der Benutzer Klassenzuordnung gesetzt werden oder bei der Zuordnung einer Klasse zu einem Berechtigungsprofil. Es hat den Sinn einer „Notbremse“. Wenn einem Benutzer explizit ein Recht auf eine Klasse verweigert wird, ist das Recht selbst dann entzogen, wenn es ihm aufgrund seines Berechtigungsprofils eigentlich erteilt wurde.

Anmerkung

Eine explizite Verweigerung eines Rechts kann NICHT durch erteilte Rechte über andere Zuordnungen aufgehoben werden!

Es gibt zwei Möglichkeiten, einem Benutzer Rechte auf Dokumentklassen zu geben:

- Implizit: Man weist dem Benutzer ein oder mehrere Berechtigungsprofil(e) zu.
- Explizit: Man weist dem Benutzer direkt Rechte auf einzelne Dokumentklassen zu.

Dokumentarten und Klassenkonzept

Dokumentarten, die einem Benutzer in d.3 smart explorer und in d.3 import angeboten werden:

Zur Ermittlung der Dokumentarten, die dem Benutzer angeboten werden, werden zunächst alle Dokumentklassen, auf die er irgendein Recht hat, ermittelt. Für jede dieser Klassen wird ermittelt, zu welcher Dokumentart diese in Relation steht. Somit ergibt sich die Liste der Dokumentarten, die dem Benutzer angeboten wird.

Des Weiteren wird unterschieden, ob der Benutzer lesend oder schreibend auf die Dokumentart zugreifen darf. Damit eine Dokumentart in d.3 import (manuelle Ablage) angeboten wird, muss der Benutzer schreibenden Zugriff auf die Klasse haben, aus der die Dokumentart abgeleitet wurde.

Wenn einem Benutzer nur dokumentartunabhängige Klassen zugeordnet wurden, dann kann dieser Benutzer zunächst in den d.3-Anwendungen (d.3 smart explorer, d.3 import) keine Dokumentarten sehen. Um diesem Benutzer nun auch die gewünschten Dokumentarten zur Verfügung zu stellen, weist man diesem einfach die Standardklassen ohne eine Rechteangabe über das Berechtigungsprofil oder direkt zu (siehe auch Kapitel [Dokumentklassen](#)).

Effektive Rechte eines Benutzers

Zur Ermittlung der Rechte eines Benutzers auf die Dokumentklassen werden zunächst alle Berechtigungsprofile des Benutzers ausgewertet. Anschließend werden die Rechte (sofern vorhanden), die dem Benutzer direkt auf die Klassen erteilt wurden, darüber gelegt.

Anmerkung

Erhält ein Benutzer über die zugeordneten Berechtigungsprofile und den direkt zugeordneten Dokumentklassen unterschiedliche Rechte, "gewinnt" die Zuordnung, die dem Benutzer direkt erteilt wurde. Auch ein verweigertes Recht kann hierdurch übersteuert werden!

Ein Dokument kann keiner, einer oder mehreren Klassen zugeordnet sein. Ein Benutzer erhält ein gewünschtes Recht auf ein Dokument, wenn das Dokument mindestens einer Klasse zugeordnet ist, für welche der Benutzer das gewünschte Recht besitzt.

Grundsätzlich ist zu beachten, dass ein Benutzer - über welche Zuordnungen auch immer - mindestens an einer Stelle das Recht erteilt bekommt, ansonsten kann er keine Dokumente recherchieren. Die Standardeinstellung bei "Recht ignoriert" ist immer "Recht verweigert".

1.5.8. Hinweise zum Transportsystem

Mit dem Transportsystem können Sie schnell und unkompliziert viele Einstellungen von d.3 admin in weitere Repositorys übernehmen. Durch Verwendung des Transportsystems erreichen Sie stets eine Synchronität von mehrstufigen d.velop documents-Umgebungen und verhindern, dass sich Konfigurationen im Laufe der Zeit unterscheiden.

Projekte und Meilensteine - Sinn und Zweck

Damit Änderungen an Stammdaten in d.3 admin durchgeführt werden können, muss man den Bearbeitungsmodus zu einem Projekt aktivieren. Damit werden alle Änderungen im aktiven Meilenstein des Projektes aufgezeichnet.

Bei einem Export des Projektes oder der Meilensteine des Projektes werden somit gezielt die Änderungen erfasst, die innerhalb des Projektes durchgeführt werden. Genau diese Änderungen können dann in ein anderes d.3-Repository übertragen werden. Gibt es Kollisionen durch Änderungen an gleichen Stammdaten innerhalb mehrerer Projekte, wird der Stand, der beim Schließen eines Meilensteines aktuell ist, erfasst und gesichert. Dabei werden auch alle Abhängigkeiten berücksichtigt (z.B. bei Änderungen an Dokumentarten werden auch die erweiterten Eigenschaftsfelder der Dokumentart gesichert).

Projekte allgemein

Bei der Arbeit mit d.3 admin ist darauf zu achten, dass Änderungen immer nur im Bearbeitungsmodus durchgeführt werden. Um in den Bearbeitungsmodus zu gelangen, benötigen Sie mind. ein Projekt, welches sich im Status "geöffnet" befindet. Pro Projekt kann immer nur ein Administrator den Bearbeitungsmodus aktivieren. Mehrere Administratoren können zeitgleich in unterschiedlichen Projekten arbeiten, aber niemals im gleichen Projekt.

Projekterstellung

Bei der Erstellung eines Projektes muss ein Name (maximal 50 Zeichen) angegeben werden. Dieser Name muss eindeutig sein und kann nicht so ohne weiteres geändert werden. Optional kann auch eine Beschreibung (maximal 255 Zeichen) angegeben werden. Das Projekt wird im Status "geöffnet" erstellt und kann vom Administrator nicht geschlossen oder gelöscht werden.

Umbenennen von Projekten

Projekte können über die Oberfläche von d.3 admin nicht umbenannt werden. Dazu muss das Plugin "d.3 project manager" verwendet werden.

Geschlossene Projekte

Es existieren auch geschlossene Projekte, die im Standard nicht angezeigt werden. Dabei handelt es sich entweder um das vom System automatisch erstellte Snapshot-Projekt oder aber es handelt sich um Projekte, die mittels Einspielen von Transportdateien erzeugt wurden. Diese Projekte können nicht wieder geöffnet werden.

Snapshot-Projekt

Das Snapshot-Projekt enthält Sicherungen der Stammdaten, die bei der Einleitung eines Import-Vorganges einer Transportdatei automatisch erstellt werden können. Für jede Sicherung wird dabei ein neuer Meilenstein angelegt.

Offene Sitzungen zu Projekten

Wie schon erwähnt kann pro Projekt nur ein Administrator den Bearbeitungsmodus aktivieren. Wer gerade in welchem Projekt arbeitet, kann man in d.3 admin unter "Offene Sitzungen" sehen. Sollte mal ein Projekt für längere Zeit blockiert sein, kann man die offene Sitzung für dieses Projekt beenden. Dazu klickt man mit der rechten Maustaste auf den Eintrag der Sitzung. Daraufhin erscheint ein Kontextmenü mit dem Menüpunkt "Session beenden". Durch betätigen der Schaltfläche wird die Sitzung beendet. Allerdings kann man eine Sitzung nur dann beenden, wenn mind. 1 Stunde lang keine Aktivität in der Sitzung stattgefunden hat.

Meilensteine allgemein

Meilensteine dienen dazu, um bestimmte Änderungen in d.3 admin festzuhalten und diese exportieren und auf bspw. auf andere Systeme importieren zu können.

Ein Meilenstein ist immer Bestandteil eines Projektes und kann nicht eigenständig erstellt werden. Ebenso kann ein Meilenstein nicht gelöscht werden.

Bei Erstellung eines Projektes wird automatisch ein Meilenstein erstellt. Jeder Meilenstein trägt eine Nummer, die, pro Projekt, fortlaufend bei 1 beginnt. Meilensteine liegen entweder im Status "geöffnet" oder "geschlossen" vor. Nur, wenn ein Meilenstein den Status "geöffnet" hat (wird rot in der Meilenstein-Übersicht angezeigt), werden darin Änderungen aufgezeichnet. Ein Meilenstein im Status "geschlossen" (wird grün in der Meilenstein-Übersicht angezeigt), kann nicht wieder geöffnet werden. Pro Projekt kann maximal ein Meilenstein im Status "geöffnet" vorliegen. Dabei ist dies immer der zuletzt erstellte. Es gibt auch Projekte, in denen kein Meilenstein den Status "geöffnet" hat. In solchen Projekten können keine Änderungen mehr aufgezeichnet werden. Solche Projekte sind über das Einspielen von Transportdateien aus einem anderen d.3-Repository entstanden.

Aufzeichnung von Daten

Folgende Daten werden innerhalb eines Meilensteines aufgezeichnet:

- Wertemengen
- Dokumentarten
- Erweiterte Eigenschaften
- Mehrsprachigkeit
- Aktenbildung
- Gruppen (außer Mitgliedschaften von Benutzern)
- Dokumentklassen
- Berechtigungsprofile
- Berechtigungsprofil-Zuordnungen (nicht für Benutzer)
- d.3 organizational structure
- d.3 policy manager (nicht für Benutzer)
- d.3 restriction set Manager (nicht für Benutzer)

- d.3 config (nicht für alle Parameter)
- d.ecs rendition service Assistent

Änderungen von Stammdatenobjekten in einem Meilenstein

Bei Änderungen von Stammdatenobjekten werden diese innerhalb des Meilensteines vermerkt. Technisch gesehen läuft folgendes ab:

- Anhand der Synchronisations-ID wird der Änderungszeitpunkt aktualisiert
- Zu jeder Änderung wird in der Datenbank ein Eintrag erstellt. Dieser Eintrag wird auch in der Protokollansicht in d.3 admin angezeigt.

Schließen eines Meilensteines

Sie können einen Meilenstein nur im Bearbeitungsmodus schließen. Zu jedem Meilenstein müssen Sie einen Beschreibungstext eingeben. Beim Schließen werden folgende Aktionen durchgeführt:

- Anhand der Liste der Änderungen an Stammdaten-Objekten werden alle Abhängigkeiten ermittelt und der aktuelle Stand dieser Objekte in eine Transportdatei geschrieben.

Anmerkung

Da immer der aktuelle Stand eines Objekts (z.B. einer Dokumentart) zur Anwendung kommt, werden auch Änderungen berücksichtigt, die innerhalb anderer Projekte durchgeführt wurden.

- Es werden nur die Stammdaten-Objekte in die Transportdatei geschrieben, die sich seit dem letzten Meilenstein geändert haben. Dazu kommen noch die Objekte, die als Abhängigkeiten ermittelt wurden.
- Diese Transportdatei wird im Repository in die Dokumentart **Audit-Log** importiert.
- Der aktuelle Meilenstein wird geschlossen und ein neuer Meilenstein im Status **geöffnet** wird erstellt.

Löschen von Stammdatenobjekten

Beim Löschen von Stammdatenobjekten, z.B. einer Dokumentart gibt es eine Besonderheit: Die eigentlichen Daten zum Objekt werden, wie früher auch, gelöscht. Allerdings werden die für das Transportsystem relevanten Daten, z.B. die Synchronisation-ID, nicht gelöscht. Das bedeutet: Legt man nach dem Löschen eine Dokumentart mit dem gleichen Kürzel noch mal an, wird keine neue Synchronisations-ID erstellt, sondern die für das Dokumentartkürzel erzeugte wird wiederverwendet.

Auswirkungen kann das beim Transportieren von Daten auf ein anderes System haben: Legt man im Zielsystem eine Dokumentart an, die das gleiche Kürzel einer Dokumentart aus dem Quellsystem hat und löscht diese im Zielsystem wieder, wird ein Transport vom Quellsystem ins Zielsystem scheitern, da die Synchronisations-IDs nicht übereinstimmen.

Löscht man im Quellsystem Stammdatenobjekte mit Benutzerbezug, müssen vor dem Einspielen der Transportdatei, welche diese Änderung enthält, alle Referenzen auf dieses Stammdatenobjekt entfernt werden, da solche Referenzen nicht über das Transportsystem erfasst werden.

Beispiel: Im Quellsystem soll ein Berechtigungsprofil gelöscht werden. Dieses Berechtigungsprofil existiert im Zielsystem und ist noch einzelnen Benutzern zugewiesen. Damit der Löschvorgang über das Einspielen einer Transportdatei im Zielsystem ausgeführt werden kann, müssen die Benutzerzuweisungen im Zielsystem vorher entfernt werden. Dabei sind auch die Einstellungen der LDAP-Konfiguration zu berücksichtigen.

Geschützter Modus

Der geschützte Modus stellt sicher, dass transportable Konfigurationsdaten nur über Transportdateien erstellt und gelöscht werden können. Der Modus wird beim Import einer Transportdatei automatisch aktiviert und das aktuelle Repository mit dem Quellsystem der Transportdatei verbunden.

Beachten Sie folgende Regeln zum geschützten Modus:

- Sie können nur noch Transportdateien aus dem verbundenen Quellsystem importieren.
- Sie können keine transportablen Objekte (Eigenschaftsfelder usw.) neu erstellen.
- Sie können keine transportablen Objekte löschen.
- Sie können Objekte weiterhin ändern.
- Sie können den geschützten Modus im Bereich **d.3 config** über den Parameter **MASTERDATA_RESET_PROTECTED_MODE** vorübergehend zurücksetzen, z.B. um beim Aufbau eines neuen Testsystems die bisherige Verbindung aufzuheben und eine neue Verbindung zu erstellen.

Begriffsbestimmung

Mit der d.3 Version 8.0 gibt es nicht nur optische Veränderungen in d.3 admin (siehe Kapitel [Starten von d.3 admin](#)), sondern auch neue Menüpunkte und Begriffe, deren Bedeutung hier näher erklärt wird.

Projekt

Ein Projekt ist eine Sammlung von Meilensteinen und dient der Aufzeichnung von Änderungen von Repository-Stammdaten wie Dokumentarten oder erweiterte Eigenschaftsfelder sowie von Änderungen an Konfigurationsschaltern. Ein Projekt hat einen Namen und einen optionalen Beschreibungstext. Jedes Projekt hat einen Status: Entweder "offen", was bedeutet, dass man Änderungen innerhalb dieses Projektes aufzeichnen kann oder "geschlossen", was jegliche Aufzeichnung von Änderungen verhindert. Ein einmal geschlossenes Projekt kann nicht mehr geöffnet werden und wird per Standard nicht in d.3 admin angezeigt werden.

Meilenstein

In einem Meilenstein werden Änderungen an den Repository-Stammdaten bzw. an Konfigurationsschaltern aufgezeichnet und können auf ein anderes d.3-Repository übertragen werden. Meilensteine werden, von 1 beginnend, aufsteigend durchnummeriert und tragen den Namen "Meilenstein <Nummer>". Jeder Meilenstein hat einen Status. Entweder "offen", was bedeutet, dass Änderungen in diesem Meilenstein aufgezeichnet werden können oder "geschlossen", was jegliche Aufzeichnung von Änderungen in diesem Meilenstein verhindert. Ein einmal geschlossener Meilenstein kann nicht mehr geöffnet werden.

Abhängigkeiten

Das Transportsystem erfasst Änderungen, die im Rahmen eines Projekts im Bearbeitungsmodus getätigt werden. Bei Schließen eines Meilensteins werden diese Änderungen in die Transportdatei geschrieben. Zusätzlich wird zu jedem erfassten Objekt der Objekttyp ermittelt.

Folgende Abhängigkeiten werden berücksichtigt:

- Erweiterte Eigenschaften haben Wertemengen als Abhängigkeit.
- Dokumentarten haben erweiterte Eigenschaften als Abhängigkeit.
- Dokumentklassen haben Dokumentarten, Restriktionsmengen und Wasserzeichen als Abhängigkeit.
- Berechtigungsprofile haben Dokumentklassen als Abhängigkeit.
- Aktenbildungsregeln haben Dokumentarten und Dokumentklassen als Abhängigkeit.
- Rendition-Regeln haben Dokumentklassen als Abhängigkeit.
- Gruppen haben Berechtigungsprofile und Organisationseinheiten als Abhängigkeit.

Diese Abhängigkeiten werden zusätzlich mit in die Transportdatei aufgenommen, um die Konsistenz sicherzustellen.

Import

Mit der Import-Funktion können aufgezeichnete Änderungen von Projekten oder Meilensteinen aber auch aus Backups bzw. Snapshots in das d.3-Repository eingespielt werden. Vor jedem Import wird eine Sicherung gemacht, wodurch ein Meilenstein im Snapshot-Projekt entsteht.

Export

Über die Export-Funktion können ausgewählte Projekte oder Meilensteine in Form von ZIP-Dateien aus dem d.3-Repository exportiert werden. Diese Dateien können dann über die Import-Funktion in ein anderes d.3-Repository übertragen werden.

Backup

Ein Backup enthält die kompletten Stammdaten und Konfigurationsparameter des d.3-Repositorys und kann zum Rollback eines bestehenden oder zum Neuaufbau eines neuen d.3-Repositorys verwendet werden. Ein Backup kann entweder automatisiert oder aber explizit erstellt werden. Die so erzeugte Datei trägt die Dateierweiterung ".d3backup".

Snapshot

Ein Snapshot enthält die gleichen Daten wie ein Backup und wird automatisch durch einen Import-Vorgang erzeugt. Snapshots werden in einem eigenen Projekt mit dem Namen "Snapshot" verwaltet, wobei das Projekt den Status "geschlossen" hat. Jeder Snapshot ist dabei ein Meilenstein innerhalb des Snapshot-Projektes.

Transport

Ein Transport ist eine Datei, die durch die Export-Funktion erzeugt wird und die Dateierweiterung `.d3trans` trägt. Ein Transport kann durch die Import-Funktion in ein anderes d.3-Repository eingespielt werden. Der Transport ist für stetigen Austausch zwischen Test- und Produktivsystem gedacht, das Backup dient eher zur eigentlichen Datensicherung.

Bearbeitungsmodus

In diesem Modus können Änderungen an Stammdaten und Konfigurationsparameter in d.3 admin durchgeführt und aufgezeichnet werden. Pro Projekt kann nur ein Administrator in den Bearbeitungsmodus wechseln.

Ansichtsmodus

In diesem Modus können keine Änderungen vorgenommen werden. Alle Module innerhalb d.3 admin werden in einem Readonly-Modus gestartet.

Sitzungen

Wenn ein Administrator zu einem Projekt in den Bearbeitungsmodus wechselt, wird eine Sitzung auf dieses Projekt eröffnet. Pro Projekt kann es nur eine Sitzung geben und ein Administrator kann immer nur eine Sitzung geöffnet haben. Nach einer Stunde Inaktivität kann die Sitzung durch einen anderen Administrator geschlossen werden.

Objekttyp

Objekttypen werden im Protokoll zu einem Meilenstein in d.3 admin angezeigt und kennzeichnen den Typ eines Stammdatenobjektes, z.B. eine Dokumentart oder ein Eigenschaftsfeld.

Aktion

Aktionen werden im Protokoll zu einem Meilenstein in d.3 admin angezeigt und kennzeichnen, ob ein Objekt hinzugefügt (INSERT), aktualisiert (UPDATE) oder gelöscht (DELETE) wurde.

Synchronisations-ID

Jedes Stammdatenobjekt bekommt beim ersten Start von d.3 admin nach dem Update auf die d.3-Version 8 eine Synchronisations-ID zugewiesen, die als Referenz für die Übertragung von Transportdaten in andere d.3-Repositorys verwendet wird. Damit kann die Synchronität der Stammdaten zwischen den d.3-Repositorys gewährleistet werden.

Aufzeichnung der Änderungen

Änderungen, die ein Administrator im Bearbeitungsmodus vornimmt, werden innerhalb eines Meilensteines gespeichert und somit für den Transport in ein anderes d.3-Repository aufgezeichnet. Nicht alle Änderungen können aufgezeichnet, im Protokoll angezeigt und transportiert werden.

Praktische Hinweise

Wie arbeite ich mit Projekten und Meilensteine, wie starte ich damit nach einem Update?

Die allgemeine Arbeit mit Projekten und Meilensteinen wird in den vorherigen Kapiteln erklärt.

Wenn nur ein Repository betrieben wird, legt man nach dem Update Projekte an und kann dann Änderungen über den Bearbeitungsmodus vornehmen.

Wenn man 2 Repositorys betreibt, die den gleichen Aufbau haben und bisher immer synchron gehalten wurden, hat man 2 Möglichkeiten:

1. Man baut sich ein neues Testsystem auf anhand einer aktuellen Datensicherung aus seinem Produktivsystem
2. Über das Plugin "d.3 project manager" werden die Synchronisations-IDs der Stammdatenobjekte angeglichen. Das funktioniert nur dann zuverlässig, wenn der Aufbau der 2 Repositorys tatsächlich nahezu gleich ist (Repository 1 enthält alles aus Repository 2 und evtl. noch zusätzliche Daten). Voraussetzung dafür ist, dass noch keinerlei Projekte angelegt wurden. Dieser Schritt muss also direkt nach dem Update erfolgen.

Wenn man mehrere Repositorys betreibt, die einen unterschiedlichen Aufbau haben, bleibt nur der Weg, ein neues Repository auf Basis einer Datensicherung aufzubauen.

Welche Voraussetzungen müssen gegeben sein damit das Transportsystem genutzt werden kann?

- Das Quellsystem und das Zielsystem müssen auf Version 8 laufen
- Das Quellsystem und das Zielsystem enthalten die gleichen Stammdatenobjekte, bauen also aufeinander auf
- Das Zielsystem muss aus einem Export aus dem Quellsystem aufgebaut werden oder
- Die Synchronisations-IDs der Stammdatenobjekte des Quell- und Zielsystems sind gleich (möglich über das Plugin "d.3 project manager")
- Die transportablen Daten (siehe nächster Punkt) werden immer vom Quellsystem auf das Zielsystem übertragen
- Im Zielsystem werden keine Änderungen an den Stammdatenobjekten vorgenommen

Was wird vom Transportsystem abgedeckt?

Folgende Stammdatenobjekte werden vom Transportsystem berücksichtigt:

- Wertemengen
- Dokumentarten
- Erweiterte Eigenschaften
- Mehrsprachigkeit
- Aktenbildung
- Gruppen (außer Mitgliedschaften von Benutzern und Gruppen)
- Dokumentklassen
- Berechtigungsprofile

- Berechtigungsprofil-Zuordnungen (nicht für Benutzer)
- d.3 organizational structure
- d.3 policy manager (nicht für Benutzer)
- d.3 restriction set Manager (nicht für Benutzer)
- d.3 config (nicht für alle Parameter)
- d.ecs rendition service Assistent

Folgendes muss somit noch nachträglich angepasst werden:

- Benutzer inklusive Gruppenmitgliedschaften, Berechtigungsprofil-Zuordnungen, benutzerspezifische Rechte und Eigenschaften sowie Restriktionsmengen-Zuordnungen
- Hook-Funktionen (Groovy-Hooks können ab 8.1.0 Rising 2 auch transportiert werden)
- LDAP-Einstellungen
- Archiv abhängige Konfigurationsparameter (z.B. Hostimport-Pfade)
- Plugin "d.3 explorer Folder browser"
- Plugin "Automatische Ablage"
- Plugin "d.3 client config"
- Plugin "d.3 content service"
- Plugin "d.3 abo service"
- Plugin "d.3 search Admin"
- Plugin "Formularzuordnung"
- Workflows

Anmerkung

Das Ändern von Benutzer-Kennwörtern kann auch im Ansichtsmodus durchgeführt werden!

Initialer Transport vs. Folgetransport

Was ist zu beachten, bei dem initialen Import? / Was ist bei dem Export für den initialen Import zu beachten?

Der initiale Import, also der Import in ein leeres Repository, kann entweder über eine Backup-Datei (Datensicherung) oder über einen Projekt- bzw. Meilenstein-Import erfolgen. Beim Export für einen initialen Import muss nur dann etwas bedacht werden, wenn das Quellsystem schon vor Version 8 aufgesetzt wurde und somit schon administrative Änderungen vor dem Update stattgefunden haben, und zwar folgendes: Der Meilenstein-Export enthält nur die Änderungen an den Stammdaten, die explizit durchgeführt werden. Dabei werden auch die Abhängigkeiten zu anderen Objekten berücksichtigt. Allerdings werden andere Objekte, die nicht in die Abhängigkeiten fallen, unberücksichtigt gelassen. Möchte man diese Objekte ebenfalls in den Export aufnehmen, muss man entweder "Schein-Änderungen" (mittels Durchklicken der Objekte) ausführen oder aber mittels des "d.3 project manager"-Plugins die Objekte gezielt einem Projekt und damit dem aktuellen Meilenstein zuordnen.

Wie gehe ich mit parallelen Projekten um?

Wenn parallel mehrere Projekte in Bearbeitung sind, achten Sie darauf, dass eventuelle Abhängigkeiten aus anderen geschlossenen Meilensteinen mit in einem Transport aufgezeichnet werden.

Zur Reduzierung von Abhängigkeiten in den Transporten, können Sie alternativ ein Projekt nur für den Transport von Berechtigungsprofilen und Gruppen erstellen. Wenn ein Meilenstein bzw. das gesamte Projekt exportiert und importiert wird, werden sämtliche Einstellungen zu Berechtigungsprofilen, Dokumentklassen, Dokumentarten, Eigenschaften, Wertemengen und ggf. Einstellungen aus dem Aktenplan (auch aus geschlossenen Meilensteinen aus anderen Projekten) mittransportiert.

Achten Sie bei administrativen Berechtigungsprofilen darauf, dass diese Profile häufig sämtliche Dokumentklassen innerhalb eines Repositorys beinhalten.

Beim Export wird immer der aktuelle Stand der Daten berücksichtigt und zusätzlich der Zeitpunkt der letzten Änderung am Objekt festgehalten. Dies wird beim Import dann berücksichtigt, so dass eine ältere Änderung keine neuere überschreibt.

Was ist beim Entfernen von Dokumentarten, Eigenschaften, etc. zu beachten?

Prinzipiell nichts.

Wenn man in Projekt 1 eine Dokumentart löscht, die in Projekt 2 vorher geändert wurde, würde beim Import folgendes ablaufen:

Wird Projekt 2 vor Projekt 1 importiert, würde die Dokumentart zunächst einmal erstellt bzw. geändert. Wenn dann Projekt 1 importiert wird, wird die Dokumentart gelöscht.

Wird Projekt 1 vor Projekt 2 importiert, würde die Dokumentart gelöscht bzw. nicht berücksichtigt. Wenn dann Projekt 2 importiert wird, wird die Dokumentart nicht angelegt.

Wie funktioniert der Transport rein technisch? Was wird wie exportiert und importiert?

Export

Beim Schließen eines Meilensteines wird der aktuelle Stand der Stammdatenobjekte (z.B. einer Dokumentart), die im Bearbeitungsmodus des Meilensteines geändert wurden erfasst und in eine XML-Datei geschrieben. Dabei werden alle Abhängigkeiten (z.B. die erweiterten Eigenschaften zur Dokumentart) berücksichtigt und vorweg in die XML-Datei geschrieben. Zudem wird der Zeitstempel der letzten Änderung (dabei ist es egal, ob das Objekt innerhalb des Meilensteines, der gerade geschlossen wird, oder in einem anderen geändert wurde) in die XML-Datei aufgenommen. Dieser Zeitstempel dient dann beim Import dazu, dass ältere Änderungen neuere nicht überschreiben. Die so erstellte XML-Datei wird in die Dokumentart "Audit-Log" importiert.

Wird nun ein Meilenstein exportiert, wird die XML-Datei heruntergeladen und in eine ZIP-Datei aufgenommen. Diese ZIP-Datei enthält noch weitere Steuerdateien.

Man kann auch mehrere Meilensteine auf einmal exportieren (Achtung: Die Liste der Meilensteine kann nur von einem Projekt sein und muss durchgängig, also lückenlos sein). Auch ein ganzes Projekt kann exportiert werden, wobei hier nur die geschlossenen Meilensteine berücksichtigt werden.

Import

Vor dem Import findet zunächst eine Konsistenzprüfung der Daten aus der ZIP-Datei statt. Dabei wird zu jeder Datei ein Hash-Wert berechnet und mit den Hash-Werten aus der .hash-Datei abgeglichen. Eine Änderung der Dateien ist somit nicht gestattet um sicherstellen zu können, dass der Import nach den Regeln des Transportsystems stattfindet. Wenn die .hash-Datei nicht existiert, kann kein Import durchgeführt werden.

Beim Import werden die Objekte nach ihrem Vorkommen in den XML-Dateien verarbeitet. Wenn Stammdatenobjekte schon existieren, wird der Zeitpunkt der letzten Änderung im Zielsystem mit dem in der XML-Datei abgelegten Zeitpunkt der letzten Änderung aus dem Quellsystem verglichen. Wenn der Zeitpunkt aus der XML-Datei jünger ist als der im Zielsystem, wird das Objekt mit den Daten aus der XML-Datei aktualisiert. Ist der Zeitpunkt aus der XML-Datei älter als der Zeitpunkt im Zielsystem, wird das Objekt übersprungen.

Wenn beim Import ein Fehler auftritt, wird der komplette Importvorgang abgebrochen und alle Änderungen werden verworfen.

Nach dem Import wird das Projekt um die Meilensteine aus der Importdatei erweitert. Im Protokoll der Meilensteine können sich im Zielsystem Unterschiede zum Protokoll aus dem Quellsystem ergeben, da alle mehrfachen Änderungen im Quellsystem zu einer Änderung im Zielsystem zusammengefasst werden

und somit nur einmal im Protokoll erscheinen. Änderungen aus dem Quellsystem, die älter sind als Änderungen im Zielsystem, werden übersprungen und nicht im Protokoll dargestellt.

Beim Import werden die Synchronisations-IDs bei neu erstellten Objekten aus dem Quellsystem in das Zielsystem übertragen. Damit wird eine Verbindung der Objekte zwischen Quell- und Zielsystem geschaffen. Interne IDs wie z.B. die ID von Eigenschaftsfeldern werden nicht übernommen und können zwischen den Systemen voneinander abweichen.

Wie ist die empfohlene Vorgehensweise wenn mehrere Umgebungen im Einsatz sind (Testsystem, Abnahmesystem, Produktivsystem)?

Ausgangspunkt sollte immer ein System (also hier das "Testsystem") sein. Hier werden die Änderungen an den Stammdatenobjekten vorgenommen. Anhand eines Exports aus dem Testsystem werden die Daten dann in das Abnahmesystem übertragen. Änderungen sollten dann wieder im Testsystem vorgenommen werden. Passt alles für einen Import in das Produktivsystem, wird das über das Testsystem heraus gemacht, wobei aber auch ein Export aus dem Abnahmesystem möglich wäre.

Installation der Basis-Workflows

Die Installation der Basis-Workflows kann folgendermaßen durchgeführt werden:

- Erstellung eines Projektes im Testsystem zur Durchführung von Aktionen, die vom Basis-Workflow benötigt werden
- Aktivierung des d.3-Parameters **WORKFLOW_SUPPORT**
- Einrichtung der Dokumentklasse **WEITERLEITUNG** mit dem Kürzel **ALL**
- Einrichtung der Benutzergruppe **wfl_admin**
- Erstellung eines Benutzers mit den Rechten, wie man die für die Basis-Workflowinstallation benötigt
- Schließen des Meilensteines
- Installation der Basis-Workflows über das Setup.

Möchte man nun nach der Installation des Basis-Workflows in einem Testsystem diesen auch im Produktivsystem einrichten, nimmt man den Export des Meilensteines, in dem man die Einrichtung der Stammdatenobjekte im Testsystem vorgenommen hat und transportiert diese in das Produktivsystem. Der Installationsbenutzer wird dabei aber nicht berücksichtigt und muss im Produktivsystem "per Hand" angelegt werden. Danach kann man dann für das Produktivsystem das Setup des Basis-Workflows ausführen.

Änderungen im Zielsystem

Sie können auch weiterhin Änderungen in einem Produktivsystem vornehmen, also dem Zielsystem von Transportdateien. Achten Sie darauf, auf Änderungen an den Stammdaten zu verzichten, die über das Transportsystem erstellt wurden, da ansonsten die Synchronität der Objekte zwischen Quell- und Zielsystem nicht mehr gewährleistet werden kann und Importe von Transportdateien fehlschlagen können. Insbesondere die Neuerstellung von Objekten ist hier kritisch. Allerdings fallen im Produktivsystem auch Änderungen an Benutzern oder an d.3-Parametern an. Um solche Änderungen durchführen zu können, kann man sich ein "Notfall-Projekt" anlegen und die Änderungen innerhalb dieses Projektes durchführen. Im Regelfall wird man in der Protokollansicht keine Einträge finden, da z.B. Benutzer oder bestimmte d.3-Parameter nicht transportabel sind und somit nicht aufgezeichnet werden.

Empfehlungen

- Nehmen Sie im Zielsystem keine direkten Änderungen an transportablen Objekten vor. Die Synchronität zwischen den Systemen wird durch diese Änderungen gefährdet. Bei einer Systemkonstellation von Entwicklung, Test und Produktiv ist dabei das Entwicklungssystem das Quellsystem und die anderen beiden Systeme sind die Zielsysteme.
- Erstellen bzw. löschen Sie im Zielsystem auch keine transportablen Objekte direkt, da ansonsten die Synchronisations-IDs zwischen den Systemen nicht zusammenpassen und Transporte fehlschlagen können.

- Verzichten Sie auf unnötiges Löschen und Erstellen der gleichen Objekte.
- Wenn Sie die erweiterten Eigenschaftsfelder löschen möchten, um diese direkt erneut zu erstellen, um die DB-Position zu ändern, tragen Sie am besten einen anderen Beschreibungstext ein. Für das Transportsystem handelt es sich dann um ein komplett neues Feld mit einer neuen Synchronisations-ID und es gibt keinen Verweis mehr auf das alte Feld.
- Arbeiten Sie mit so wenig Projekten wie möglich und versuchen Sie, die Änderungen an Objekten immer im gleichen Projekt durchzuführen.
- Zur Reduzierung von Abhängigkeiten in den Transporten, können Sie alternativ ein Projekt nur für den Transport von Berechtigungsprofilen und Gruppen erstellen. Wenn ein Meilenstein bzw. das gesamte Projekt exportiert und importiert wird, werden sämtliche Einstellungen zu Berechtigungsprofilen, Dokumentklassen, Dokumentarten, Eigenschaften, Wertemengen und ggf. Einstellungen aus dem Aktenplan (auch aus geschlossenen Meilensteinen aus anderen Projekten) mittransportiert.
- Achten Sie bei administrativen Berechtigungsprofilen darauf, dass diese Profile häufig sämtliche Dokumentklassen innerhalb eines Repositorys beinhalten.

1.6. Aufbewahrungsfristen und Löschen von Dokumenten

Dieses Kapitel gibt Ihnen hilfreiche Informationen zum Thema Aufbewahrungsfristen und dem Löschen von Dokumenten.

Definitionen

Ein Dokument enthält Eigenschaften und Dokumentversionen. Eine Dokumentversion enthält nur Nutzdateien (die Originaldatei und abhängige Dateien).

Aufbewahrungsfrist

Die Aufbewahrungsfrist beschreibt die Mindest-Aufbewahrungszeit eines Dokumentes in d.3ecm bevor dieses gelöscht werden darf.

Sie wird in d.3 admin pro Dokumentart in Monaten konfiguriert. Beim Import eines neuen Dokumentes wird das Ablaufdatum der Frist ermittelt und dem Dokument zugeordnet. Werden neue Versionen dieses Dokumentes erzeugt, so wird auch das Ablaufdatum der Frist für das Dokument neu ermittelt. Bei Übergabe an einen Sekundärspeicher wird das Ablaufdatum mitgeliefert.

Wenn zu einer Dokumentart eine "ewige" Aufbewahrungsfrist konfiguriert wurde, so wird zum Dokument kein Ablaufdatum hinterlegt. Bei Übergabe an einen Sekundärspeicher wird jedoch in diesem Fall ein Ablaufdatum von "Import plus 50 Jahre" übergeben.

Wenn zu einer Dokumentart das ereignisorientierte Löschen konfiguriert wurde, so beginnt der hierzu konfigurierte Aufbewahrungszeitraum durch späteres Auslösen eines Ereignisses. Dieses Ereignis wird über die d.3 server scripting api-Funktion `document_start_lifetime` pro Dokument ausgelöst. Beim Import eines Dokumentes wird in diesem Fall kein Ablaufdatum hinterlegt. Bei der Übergabe an den Sekundärspeicher wird ein Ablaufdatum von "Import plus Aufbewahrungszeitraum" gesetzt.

Wenn die Aufbewahrungsfrist durch einen Stichtag vorgegeben wird, so kann beim "Löschen per d.3 async durch Verschieben in den Papierkorb" (siehe unten) eine große Anzahl von Dokumenten an einem Tag anfallen. Weitere Informationen zur Verarbeitungsgeschwindigkeit durch d.3 async finden Sie in der Dokumentation [d.3 batch](#).

1.6.1. Überblick über die Löschung von Daten

Grundsätzlich lassen sich in d.3 admin die folgenden Einstellungen je Dokumentart treffen:

- Lebensdauer des Dokuments in Monaten
- ereignisorientiertes Löschen oder ereignisloses Löschen
- Kombination aus Lebensdauer (>einen Monat Lebensdauer) und ereignisorientiertem Löschen

Weitere Informationen zu den Einstellungen finden Sie im Kapitel [Dokumentart | Lebensdauer](#).

1.6.2. Statische Ermittlung der Lebensdauer

Bei der Erfassung der Lebensdauer und Deaktivierung des ereignisorientierten Löschs wird die Aufbewahrungszeit des Dokuments statisch, d.h. durch den Importprozess oder eine Aktualisierung ermittelt und in den d.3-Tabellen gesetzt. Die Aufbewahrungszeit wird für jede Version des Dokuments neu gesetzt.

Beispiel: Eine Auftragsbestätigung, die am 11.12.2016 importiert wird, führt unter Berücksichtigung der eingestellten Lebensdauer von 72 Monaten zu der statischen Ermittlung des Ende der Aufbewahrungszeit 11.12.2022.

Falls der zusätzliche Parameter **Ende <Monatsname>** gesetzt wurde, wird das Ende der Aufbewahrungszeit entsprechend auf den letzten Tag des Monats erhöht.

Beachten Sie dabei, dass damit für sehr viele Dokumente die gleiche Aufbewahrungszeit gesetzt wird und somit das Löschen erhebliche Performance-Einschränkungen zur Folge haben kann.

Warnung

Um Probleme zu vermeiden, sollte im Idealfall darauf verzichtet werden, die Fristen nachträglich zu ändern bzw. zwischen statischer und ereignisbasierter Setzung der Aufbewahrungszeit zu wechseln.

Ein solcher Schritt erfordert in der Regel Nachkorrekturen des bestehenden Datenbestandes, welcher durch kundenspezifisch anzupassende Skripte (z.B. **korrigiere_sterbedatum.jsp**, **retention2storage.jsp**) erfolgt. Diese stellt die d.velop AG auf Anfrage zur Verfügung.

Beachten Sie, dass eine solche Korrektur unter bestimmten Voraussetzungen nachträglich nicht mehr möglich ist.

1.6.3. Dynamische Ermittlung der Lebensdauer

Wollen Sie alternativ oder zusätzlich durch eine Hook-Funktion dynamisch (Ereignisorientiert) bestimmen, wie die Aufbewahrungszeit eines Dokuments berechnet und in die Datenbank bzw. das Auslagerungssystem eingetragen wird, aktivieren Sie zusätzlich die Option **Ereignisorientiertes Löschen**.

Beim Erfassen der Lebensdauer und aktiviertem ereignisorientierten Löschen in d.3 admin wird keine Aufbewahrungszeit für das Dokument ermittelt, d.h. das Dokument wartet auf ein Startereignis für den Beginn der im Feld "Lebensdauer" eingestellten Frist.

Wird dieses Ereignis wahr, wird die angegebene Lebensdauer in Monaten auf das dann aktuelle Datum addiert und dieses erzeugte Datum als Aufbewahrungszeit in die Datenbank eingetragen.

1.6.4. Setzen des Ereignisses

Bei der dynamischen Ermittlung der Aufbewahrungszeit muss zunächst ein Ereignis definiert werden, welches zur dynamischen Ermittlung dieser Aufbewahrungszeit führen soll. Diese Ereignis kann z.B. eine Produktaufkündigung oder eine Definition von Auslaufartikeln sein. Dieses Ereignis wird z. B. über eine Statusänderung in der Produktakte oder einer Eigenschaftsänderung eines Dokuments in der jeweiligen Dokumentart ausgelöst und führt zum Setzen der Aufbewahrungszeit in den d.3-Tabellen durch eine Hook-Funktion.

Anmerkung

Um die Funktionalität des ereignisgesteuerten Löschs zu benutzen, sollte in einer Hook-Funktion entsprechend für das Dokument die Server-API-Funktion **document_start_lifetime** aufgerufen werden.

1.6.5. Löschen von Dokumenten

Auf den nachfolgenden Seiten erfahren Sie, welche Wege es gibt, um Dokumente zu löschen und welche Hinweise dabei zu beachten sind.

Löschen per API

Beachten Sie folgende Hinweise beim Löschen von Dokumenten durch Verschieben in den Papierkorb, wenn Sie die d.3 api-Funktion **DeleteDocument** verwenden:

1. Nach dem Löschen verbleiben Daten im Papierkorb.
2. Alle Versionen eines Dokuments in den Status Bearbeitung, Prüfung und Freigabe müssen nacheinander (also einzeln) gelöscht werden. Um alle Dokumentversionen zu löschen, muss **DeleteDocument** gegebenenfalls mehrfach (bis zu drei Mal) aufgerufen werden.
3. Die Archivversionen eines Dokumentes können erst dann gelöscht werden, wenn keine anderen Versionen aus 2 mehr vorhanden sind.
4. Alle Archivversionen werden im Gegensatz zu 2 mit einem einzigen Funktionsaufruf gelöscht.

Löschen von Dokumentversionen im Status Bearbeitung oder Prüfung

a) Es gibt weitere Dokumentversionen in Freigabe oder Archiv.

Beim Löschen wird die Dokumentversion in den Papierkorb verschoben, das Dokument bleibt aber weiterhin recherchierbar.

Trotzdem kann die Dokumentversion später nicht wiederhergestellt werden (Ausnahme: Folgende Schalter wurden gesetzt: **DELETE_FILES_FROM_PROCESSING** oder **DELETE_FILES_FROM_VERIFICATION**).

b) Es gibt keine weiteren Dokumentversionen in Freigabe oder Archiv.

Beim Löschen wird das Dokument in den Papierkorb verschoben und ist nicht mehr recherchierbar.

Trotzdem kann das Dokument später nicht wiederhergestellt werden (Ausnahme: Folgende Schalter wurden gesetzt: **DELETE_FILES_FROM_PROCESSING** oder **DELETE_FILES_FROM_VERIFICATION**).

Löschen von Dokumentversionen im Status Freigabe

Für das Löschen ist zuvor in d.3 admin die Aktivierung des globalen Schalters **ALLOW_DELETE_FROM_RELEASE** zu aktivieren. Anschließend sind in d.3 admin zusätzliche Benutzerrechte verfügbar, die dann dem Benutzer hinzugefügt werden müssen.

a) Es gibt weitere Dokumentversionen im Status Archiv.

Beim Löschen wird die Dokumentversion in den Papierkorb verschoben, das Dokument bleibt aber weiterhin recherchierbar.

Die Dokumentversion kann aus dem Papierkorb wiederhergestellt werden.

b) Es gibt keine weitere Dokumentversion im Status Archiv.

Beim Löschen wird das Dokument in den Papierkorb verschoben und ist nicht mehr recherchierbar.

Das Dokument kann aus dem Papierkorb wiederhergestellt werden.

Löschen von Dokumenten im Status Archiv

Beim Löschen wird das Dokument in den Papierkorb verschoben und ist nicht mehr recherchierbar.

Das Dokument kann aus dem Papierkorb wiederhergestellt werden.

Beachten Sie folgende Hinweise beim Löschen von Dokumenten durch Verschieben in den Papierkorb, wenn Sie die Funktion **document_delete** aus der d.3 server scripting api (jpl + groovy) verwenden:

Das Verhalten ist hier wie bei der API-Funktion **DeleteDocument** mit folgenden Ausnahmen:

1. Der Schalter **ALLOW_DELETE_FROM_RELEASE** ist nur dann relevant, wenn der Parameter **user_name** gesetzt wird.
2. Wenn der Parameter **del_from_each_status** auf 1 gesetzt wird, so wird das Dokument mit allen Dokumentversionen in den Papierkorb verschoben.
Das Dokument kann aus dem Papierkorb wiederhergestellt werden.

Privilegiertes Löschen per API

Beachten Sie folgende Hinweise beim Nutzen der API-Funktion **DeleteDocument** aus der d.3 api oder **document_delete** aus der d.3 server scripting api:

1. Nach dem Löschen sind alle Daten des Dokuments aus d.3ecm entfernt. Es verbleibt nur ein Minieintrag in der Datenbank:
 - Dokument-ID
 - Dokumentart
 - Dokumentnummer
 - Löschdaten
 - d.3-Benutzer, der das Dokument privilegiert gelöscht hat
 - Vom Benutzer angegebener Grund für das Löschen (Freitext).
2. Das privilegierte Löschen ist nur für Dokumente möglich, die in d.3ecm recherchierbar sind. Dokumente, die sich mit allen Versionen im Papierkorb befinden, ist privilegiertes Löschen derzeit **nicht** möglich.
Über eine minimal eingestellte Standard-Verweildauer von Dokumenten im Papierkorb können auch diese Dokumente vollständig gelöscht werden.
3. Es ist ein spezieller Lizenzschlüssel in der Kundenlizenz erforderlich.
Ist dieser vorhanden, so kann ein zusätzliches Benutzerrecht zum privilegierten Löschen vergeben werden.
4. Wenn Dokumentversionen in Status Freigabe oder Archiv gelöscht werden sollen, so muss zusätzlich in d.3 admin der Schalter **ALLOW_DELETE_FROM_RELEASE** gesetzt sein.
5. Alle Versionen eines Dokuments in den Status Bearbeitung, Prüfung und Freigabe müssen nacheinander (also einzeln) gelöscht werden. Um alle Dokumentversionen zu löschen, muss **DeleteDocument** gegebenenfalls mehrfach (bis zu drei Mal) aufgerufen werden.
6. Die Archivversionen eines Dokumentes können erst dann gelöscht werden, wenn keine anderen Versionen aus 2 mehr vorhanden sind.
7. Alle Archivversionen werden im Gegensatz zu 2 mit einem einzigen Funktionsaufruf gelöscht.
8. Wenn Sekundärspeicher vorhanden:
Folgende Storage-Systeme unterstützen das privilegierte Löschen vor Ablauf der Aufbewahrungsfrist. Bitte beachten Sie, dass diese Informationen herstellerabhängig und in jedem Einzelfall von Ihnen zu prüfen sind. Die Angaben erfolgen ohne Gewähr:
 - • NAS
 - Netapp
 - TSM
 - Centera
 - HCP
 - iCAS

Löschen per d.3 async

Das Löschen von Dokumenten, bei denen die Aufbewahrungsfrist überschritten ist, erfolgt durch d.3 async. Die Löschfunktion ist im Standard abgeschaltet und muss in d.3 admin unter **d.3 config > d.3 Asynchrone Verarbeitung** aktiviert werden.

Löschen von Dokumenten nach Ablauf der Aufbewahrungsfrist

Beachten Sie folgende Hinweise beim Löschen von Dokumenten nach Ablauf der Aufbewahrungsfrist per d.3 async durch Verschieben in den Papierkorb:

1. Nach dem Löschen verbleiben Daten im Papierkorb.
2. Wird für eine Dokumentart in d.3 admin eine Aufbewahrungsfrist konfiguriert und ist der Schalter **DELETE_DOCS_ELAPSED_AUTO** gesetzt, so werden Dokumente nach Ablauf dieser Frist automatisch durch d.3 async in den Papierkorb verschoben.
3. Es wird dabei das Dokument mit allen Versionen in den Papierkorb verschoben.
Das Dokument kann aus dem Papierkorb wiederhergestellt werden.
4. Um eine permanente Belastung des d.3 async-Prozesses zu vermeiden, kann die Anzahl der zu löschenden Dokumente pro Job mit dem Parameter **DELETE_DOCS_ELAPSED_PER_CALL = "50"** gesteuert werden. Alle fünfzehn Minuten wird von d.3 async geprüft, ob zu löschende Dokumente vorhanden sind. Pro Löschvorgang wird die vorgenannte Anzahl an Dokumenten gelöscht.

Löschen von Dokumenten durch "ereignisorientiertes Löschen"

Beachten Sie folgende Hinweise beim Löschen von Dokumenten durch "ereignisorientiertes Löschen" per d.3 async durch Verschieben in den Papierkorb:

1. Nach dem Löschen verbleiben Daten im Papierkorb.
2. Wenn zu einer Dokumentart das ereignisorientierte Löschen konfiguriert wurde, so beginnt der hierzu konfigurierte Aufbewahrungszeitraum durch späteres Auslösen eines Ereignisses. Dieses Ereignis wird über die d.3 server scripting api (jpl und groovy) Funktion **document_start_lifetime** pro Dokument ausgelöst.
3. Im Anschluss greift das oben beschriebene Vorgehen "Löschen von Dokumenten nach Ablauf der Aufbewahrungsfrist".

Löschen von Dokumenten per d.3 async durch Entfernen aus dem Papierkorb

Beachten Sie folgende Hinweise beim Löschen von Dokumenten per d.3 async durch Entfernen aus dem Papierkorb:

1. Nach dem Löschen sind alle Daten des Dokuments aus d.3ecm entfernt. Es verbleibt nur ein Minieintrag in der Datenbank:
 - Dokument-ID
 - Dokumentart
 - Dokumentnummer
 - Löschdaten
 - d.3-Benutzer, der das Dokument gelöscht hat
 - Vom Benutzer angegebener Grund für das Löschen (Freitext).
2. Die Standard-Verweildauer von Dokumenten im Papierkorb beträgt standardmäßig 365 Tage und kann in d.3 admin angepasst werden (Parameter **RECYCLE_STORAGE_PERIOD**)
3. Wenn in d.3 admin der Schalter **DELETE_DOCS_ELAPSED_PHYSICAL** aktiviert ist, so werden durch d.3 async automatisch alle Dokumente aus dem Papierkorb gelöscht, deren Verweildauer im Papierkorb länger als der in **RECYCLE_STORAGE_PERIOD** eingetragene Wert ist.

Löschen von Dokumenten vom Sekundärspeicher

Mit dem Parameter **DELETE_DOCS_ELAPSED_SEC_STORAGE = "1"** kann d.ecs storage manager angewiesen werden, die Dokumente auch vom Sekundärspeicher zu löschen.

Warnung

Wurden Dateien eines Dokumentes auf einen Sekundärspeicher ausgelagert, so wird ein Löschauftrag an d.ecs storage manager übermittelt. Erst mit Ablauf der ursprünglich an den Sekundärspeicher übermittelten Aufbewahrungsfrist für das Dokument werden die Dateien des Dokuments vom Sekundärspeicher entfernt. Zwischen dem Löschauftrag und dem Ablauf der Aufbewahrungsfrist können Jahre liegen.

Löschen per Skript

Neben dem Löschen per d.3 async-Prozess ist die Löschung über ein parallel zum d.3 async-Prozess laufendes Lösch-Skript möglich. Diese Alternative sollte bei einem hohen zu löschenden Volumen favorisiert werden.

Wenden Sie sich in solchen Fällen an die d.velop AG. Der Einsatz von Lösch-Skripten ist immer eine kunden- und projektspezifische Aktion und das definierte Lösch-Szenario muss im Vorfeld mit dem Kunden abgestimmt und dokumentiert sein.

Beispiele

Beispiel 1

Die Lebensdauer wird in der Dokumentart auf 72 Monate gesetzt, ereignisorientiertes Löschen ist nicht aktiviert.

Liegt die letzte Änderung des Dokuments sechs Jahre zurück, wird das Dokument über d.3 async in den Papierkorb verschoben.

Beispiel 2

Die Lebensdauer wird in der Dokumentart auf 72 Monate gesetzt, ereignisorientiertes Löschen ist aktiviert und ein JPL-Script ist erstellt, der ein entsprechendes Ereignis abfängt.

Tritt das Ereignis ein, z.B. Produktabkündigung, wird über das Skript die Aufbewahrungszeit auf "heute" plus 72 Monate gesetzt und somit in sechs Jahren über d.3 async gelöscht.

Aufbewahrungszeit auf dem Storage:

Ein ereignisorientiertes Dokument wird mit der eingestellten Aufbewahrungsfrist (z. B. 72 Monate) auf das Stagesystem (z. B. NetApp) geschrieben. Wenn der d.ecs storage manager kurz vor Ende der Aufbewahrungsfrist keine Informationen zu dem Dokument bekommt, weil das Ereignis im d.3 noch nicht eingetreten ist, verlängert er die Aufbewahrungszeit immer so lange (um mindestens 180 Tage), bis das Ereignis eintritt.

Danach erhält der d.ecs storage manager von d.3 einen Retention-Job, mit dem das Dokument auf seine endgültige Aufbewahrungsfrist auf der NetApp gesetzt wird.

1.7. Problembehandlung

1.7.1. Erweiterte Eigenschaftsfelder

Numerischen Datentyp in alphanumerischen ändern

Warnung

Vor jeder Änderung am System ist eine Sicherung der Daten empfohlen.

Vergewissern Sie sich vor diesem administrativen Einsatz, in welchen Dokumentarten das (numerische) erweiterte Eigenschaftsfeld vorkommt. Hierzu können Sie in d.3 admin in der Übersicht der erweiterte

Eigenschaftsfelder das gewünschte erweiterte Eigenschaftsfeld in der Dokumentart auswählen und dann im Kontextmenü den Punkt **Übersicht DB Felder** anwählen. Hier haben Sie dann die Möglichkeit, nach der Spalte Titel zu sortieren.

Sollte sich das erweiterte Eigenschaftsfeld in mehreren Dokumentarten befinden, können Sie nach Markierung des Bereiches diesen über die Kontextmenü-Auswahl speichern unter... in eine externe Datei sichern. Anschließend können Sie über die Eigenschaften des erweiterten Eigenschaftsfeldes die Datenbank-Position ändern. Dazu wählen Sie eine Datenbank-Position zwischen 1 und 49.

Wenn Sie dann das erweiterte Eigenschaftsfeld bezüglich der Datenbank-Position geändert haben, müssen Sie in den Dokumentarten, die dieses Feld enthalten, ebenfalls noch die Datenbank-Position ändern.

Warnung

Überprüfen Sie vor Änderung der Datenbank-Position, ob diese ggf. in einer der anderen Dokumentarten von einem anderen erweiterte Eigenschaftsfeld belegt ist.

Wenn diese administrativen Änderungen vorgenommen wurden, werden alle neu importierten Dokumente nun auf eine alphanumerische Datenbank-Position geschrieben.

Für die im Repository bereits vorhandenen Dokumente muss der Inhalt des 80er-Feldes auf das geänderte alphanumerische Datenbank-Feld kopiert werden, da sonst der erweiterte Eigenschaftsfeld-Inhalt nicht angezeigt werden kann und damit auch nicht mehr recherchierbar ist.

Anmerkung

Sollte in einem vorhandenen Aktenplan eine Aktenerkennung bzw. Eigenschaftsvererbung über das erweiterte Eigenschaftsfeld erfolgen, muss auch dieser Aktenplan überarbeitet werden.

Eine nachträgliche Änderung des Datentyps einer Eigenschaft ist nur möglich, wenn die Eigenschaft nicht in einer Dokumentart verwendet wird.

1.7.2. Benutzer verwalten

Kennwörter, die nicht den Regeln entsprechen

Überprüfen Sie, auf welche Weise das Kennwort für den User angelegt wurde. Wurde das Kennwort in d.3 admin angelegt, gelten die Sicherheitseinstellungen bezüglich der Syntaxregeln nicht. Diese Sicherheitseinstellungen bezüglich der Syntax-Regeln gelten nur beim Ändern des Kennwortes über d.3 login manager (d.3 Login). Der User d3_admin hat weiterhin die Möglichkeit über d.3 admin, unabhängig von der eingestellten Syntax-Definition, die Kennwörter zu vergeben.

Benutzer in der Administration löschen

Um einen Benutzer zu löschen, müssen die folgenden Voraussetzungen erfüllt werden:

1. Wiedervorlage entleeren: gesendete und empfangene Objekte (über **Entfernen / Quittieren**)
2. Bereinigen der Dokumente, die sich in der **Bearbeitung** oder **Prüfung** des zu löschenden Benutzers befinden.
3. Im d.3 Dokumentenbaum dürfen sich keine Dokumente mehr unter `\bearbeit\Benutzername` befinden.

Sollte trotz der o.g. Einstellungen der Benutzer nicht zu löschen sein, prüfen Sie bitte, ob Microsoft Windows im Bearbeitungsverzeichnis einen Ordner **Thumbs** erstellt hat. Dieser wird nach den Microsoft Windows-Standard-Einstellungen nicht angezeigt (Option **Geschützte Systemdateien ausblenden** in den **Ordneroptionen**).

Benutzer löschen oder sperren

Sie können die Benutzer in d.3 admin einzeln mit rechter Maustaste anklicken und sperren. Damit der entsprechende Menüpunkt erscheint, müssen die folgenden Parameter in d.3 config gesetzt sein:

Passwort-Einstellungen

Fehlversuche aufzeichnen

`PASSWORD_USER_FAIL_CHECK = "1"`

und

Kontosperrungsschwelle

`PASSWORD_INPUT_TRIALS = <Anzahl der Fehlversuche z. B. "3">`

ODER

Passwort-Verwaltung

`PASSWORD_EXTENDED_SYNTAX = „Ja“`

Diese Einstellung zieht eine erhöhte Sicherheits-Stufe für das Passwort nach sich. Es dürfen nur Kennwörter verwendet werden, die einer vorgegebenen Syntaxregel gehorchen:

Jeweils mindestens ein Zeichen aus mindestens drei der folgenden vier Gruppen:

- A-Z
- a-z
- 0-9
- Sonderzeichen

Das Kennwort läuft nach vorgegebener Zeit (in Tagen) ab. Keines der letzten "n" Kennwörter darf verwendet werden, wobei der Wert für "n" über den Parameter `PASSWORD_HISTORY_ENTRIES` bestimmt wird.

Diese Kennwort-Einstellungen gelten nur für Änderungen über den d.3 login manager. Nach mehrmaliger fehlerhafter Anmeldung wird das Benutzerkonto gesperrt. Nach Umschaltung auf die erweiterte Syntax müssen alle Benutzer das Kennwort ändern.

1.7.3. Postkorb

SMTP-Mail für die Wiedervorlage konfigurieren

1. Starten Sie d.3 admin.
2. Öffnen Sie über die **Systemeinstellungen** die Konfiguration (**d.3 Config**).
3. Unter dem Punkt **d.3 SMTP Unterstützung** nehmen Sie die entsprechenden Einstellungen vor:
 - a. **Aktiviere SMTP Unterstützung**
 - b. **Aktiviere SMTP für die Wiedervorlage**
 - c. **Mail-Versand inklusive Dokumenten-Referenz**
 - d. **SMTP Gateway**
 - e. **SMTP Betreffzeile**
4. Speichern Sie diese Konfigurationsänderungen.

Anmerkung

Überprüfen Sie, ob jedem Benutzer in d.3 admin seine E-Mail-Adresse innerhalb der Benutzerverwaltung zugeordnet wurde. Mit diesen Einstellungen sollte nun der Benutzer bei Vorlage einer Wiedervorlage auch per E-Mail benachrichtigt werden. Sollte dies wider Erwarten nicht funktionieren, wäre zu prüfen, ob es sich um ein Konfigurationsproblem des E-Mail-Servers handelt.

Dazu überprüfen Sie bitte mit dem Kommandozeilen-Testprogramm **sendmail.exe**, ob das Versenden von SMTP-Mails überhaupt funktioniert.

Der Aufruf lautet wie folgt:

```
sendmail.exe Sender Empfänger Textdatei [Betreff]
```

In der **sendmail.ini** muss der Mail-Server angegeben sein.

```
[SendMail]
Server=<SMTP-Servername oder IP-Adresse>
```

Das Testprogramm **sendmail.exe** finden Sie im Ordner **.\d3\d3server.prg**.

Verwendung der Verfeinerungsansicht im d.3 smart explorer Postkorb

Wenn Sie die Funktion zur Verfeinerung der Suche in d.3 smart explorer auch im Postkorb nutzen möchten, können Sie dies mit der Konfiguration einer Dummy-Dokumentart erreichen.

Die so konfigurierte Dummy-Dokumentart steht dann mit ihren konfigurierten Eigenschaften auch im Postkorb für eine verfeinerte Suche zur Verfügung.

In der Dokumentation zu d.3 smart explorer finden Sie nähere Informationen zur verfeinerten Suche.

1.7.4. Dokumentarten bearbeiten**Bedeutung der Dokumentart Audit-Log****Warnung**

Mit der d.3 Version 7 wird die Protokollierung der administrativen Änderungen NICHT mehr in dieser Dokumentart vorgenommen. Administrative Änderungen werden in einem Audit-Trail vorgenommen und damit direkt in die Datenbank geschrieben. Zunächst können diese Informationen nur über d.3 API Calls abgerufen werden (GetAuditData).

Die Informationen werden in den Datenbank-Tabellen:

audit_trail, audit_trail_action und audit_trail_detail abgelegt.

Der Aufbau der Tabellen sieht folgendermaßen aus:

Tabelle audit_trail	
Spalte	Bedeutung
audit_id	Primärschlüssel und die Klammer um alle Einträge zu einem API-Call, einem Async-Job oder einer Hostimportaktion
app_id	Die dreistellige Kennung der aufrufenden Anwendung (d.3-Produktkennung aus dem Nummernband)
module_id	Die dreistellige Modulkennung/Versionsnummer, die von der aufrufenden Anwendung gesendet wird
timestamp	Uhrzeit, zu der die Operation ausgeführt wird
editor	Die d.3-Benutzerkennung des Aufrufers (diese kann auch „d.3“ selbst sein)
	Hierbei handelt es sich um den Akteur/das Subjekt einer Aktion, also den, der die Aktion durchführt

Tabelle audit_trail	
editor_host	IP-Adresse von welcher der API-Call kam; bei einer mehrschichtigen Architektur (z.B. mit d.3one) ist dies nicht zwangsläufig der Rechner, an dem der Benutzer tatsächlich arbeitet
srv_status	Interne Verwaltungsdaten für technische Nachvollziehbarkeit und Debuggingzwecke (Format: „ProzessID-ApiCallNummer“, hiermit lässt sich ein Audit-Trail-Eintrag leicht einem Eintrag im technischen d.3-Log zuordnen)

Tabelle audit_trail_action	
Spalte	Bedeutung
audit_id	Fremdschlüssel auf die Tabelle audit_trail
action_id	Bildet zusammen mit der Spalte audit_id den Primärschlüssel dieser Tabelle; Wenn innerhalb eines API-Calls mehrere Objekte bearbeitet oder mehrere Aktionen auf einem Objekt ausgeführt werden, können diese Aktionen anhand der action_id unterschieden werden
object_type	Der Typ des Objektes in d.3, das bearbeitet/verändert wird
object_id	Eindeutige Kennung des Objektes, auf dem die aktuelle Aktion ausgeführt wird
action	Vordefinierte Kennung der Art der Aktion, die vom editor auf dem Objekt ausgeführt wurde (Erstellen, Bearbeiten, Löschen ...) (Details entnehmen Sie der d.3 API-Dokumentation.

Tabelle audit_trail_detail	
Spalte	Bedeutung
audit_id	Erster Teil des Fremdschlüssels auf die Tabelle audit_trail_action
action_id	Zweiter Teil des Fremdschlüssels auf die Tabelle audit_trail_action
attribute_name	Name der Objekteigenschaft, die geändert wurde; die Werte für dieses Feld stimmen in der Regel mit den entsprechenden Bezeichnern in der d.3 API überein
attribute_value	Der neue Wert für die jeweilige Objekt-Eigenschaft

Weitere Informationen finden Sie im Handbuch zur d.3 Server-API.

Die Dokumentart Audit Log wird mit der d.3-Version 7 nur noch für d.3-Konfigurationsänderungen genutzt, Änderungen in den Dateien:

d3addon.ini, d3config.ini, d3admin.ini, AdminImportLog, AdminLog.

Verwendung von Titel-Feldern

Titel-Felder dienen zur besseren Darstellung der Dokumenteigenschaften in d.3 smart explorer.

In älteren d.3-Versionen wurde in d.3 smart explorer in der Strukturansicht die Dokumenten-Nummer zusammen mit der Repository-ID des d.3-Repository und dem Dokumententyp, z. B. D000065565 Rechnung, angezeigt. Da dies nicht aussagekräftig genug erschien, wurde die Möglichkeit geschaffen, die Dokumenterkennung über die Definition der Titel-Felder pro Dokumentart individuell gestalten zu können.

Titel-Felder lassen sich folgendermaßen definieren:

In d.3 admin können Sie jeder Dokument- bzw. Aktenart eine eigenständige Titel zuweisen. Diese Einstellung erfolgt in den [Dokumentarten](#).

Diese Titel-Definition gilt nur für die Akten- und Dokumentarten, in denen die Definitionen vorgenommen werden.

Im Fenster **Position des Titels** können Sie die betreffenden Eigenschaften auswählen, die in die Titel-Definition mit aufgenommen werden sollen. Dazu markieren Sie das entsprechende Eigenschaft und führen einen Doppelklick aus oder klicken auf **Eigenschaften**. Dann können Sie auf der Seite **Titel Eigenschaften** die entsprechenden Definitionen vornehmen.

Wenn Sie mehrere Eigenschaften zu Titel-Feldern definieren, entscheidet die Reihenfolge in der Dokumentart über den Aufbau des Gesamt-Titel.

Beispiel: Möchten Sie also einem Auftrag mehr deskriptive Namen zuweisen, können Sie ein Titel-Feld in der Dokumentart "Auftrag" definieren. Dazu markieren Sie unter **Standard** das Feld **Titel** und stellen "Ja" ein. Unter **Titel** können Sie weitere Eigenschaften festlegen:

Hier können Sie ein Suffix und ein Präfix setzen und außerdem die Länge des angezeigten Textes in d.3 smart explorer begrenzen (von, bis).

Neben den Verknüpfungen werden die Titel-Felder auch in Funktionen, wie z. B. **Senden an via E-Mail** benutzt. Die Titel-Definition und die Dateierweiterung, z. B. doc wird zur Bildung des Dateinamens herangezogen.

In der Datei **d3config.ini** können Sie für ein Datumsfeld eine Formatierung erzeugen, so dass ein Datumsfeld in der Sortierung genutzt werden kann.

1.7.5. Beispiel für Berechtigungsmengen Dokumentklassen über Restriktionsmengen

Bei der Definition der Restriktionen stehen Ihnen unterschiedliche Möglichkeiten zur Verfügung.

- Konstanter Ausdruck, auch mit Wildcards ("*", "?", weitere sind möglich, müssen aber definiert sein)
- Makros: @D3USER, @D3GROUP, @D3REGEXPR,
- Restriktionsmengen, die mit dem Makro: @D3SET referenziert werden

Restriktionsmengen werden durch Einzelwerte, aber auch Bereichsangaben und auch Negationsausdrücke definiert und als Textdokument abgelegt.

Sie ordnen die Mengen den unterschiedlichen Zielobjekten (Benutzer, Gruppe, global, ...) zu. Erst zur Laufzeit wird dann die Menge der zu prüfenden Werte ermittelt.

Zunächst legen Sie über das d.3 admin-PlugIn d.3 restriction set manager die „Container“ für die Restriktionsmengen an.



Im zweiten Schritt listen Sie die Werte, gegen die später bei der Berechtigungsprüfung verglichen werden soll, also die erlaubten bzw. verbotenen Werte.

Sie haben die Möglichkeit, globale Werte (keine Zuordnung), benutzer- bzw. gruppenbezogene Werte zuzuordnen, aber auch Werte an einer Organisationseinheit festzumachen (Organisationsstruktur).

Legen Sie am besten zunächst die Basiseinträge (keine Zuordnung) fest.

Anschließend spezialisieren Sie, z.B. vergeben Sie einer Gruppe weitere Einträge, für die nur die Gruppenmitglieder (Buchhaltung) zusätzlich berechtigt werden sollen. Ist der Name der Restriktionsmenge identisch mit dem Namen einer statischen Wertemenge, können Sie aus den hinterlegten Werten auswählen.



Somit ist es möglich, Basiswerte für alle (Gruppen)Mitglieder festzulegen, aber auch Ergänzungen und Spezialisierungen zu definieren (Gruppe / Benutzer).

Die Zuordnungen werden Ihnen entsprechend dargestellt.

Aus Benutzer- bzw. Gruppensicht können Sie sich die zugeordneten Werte anzeigen lassen.



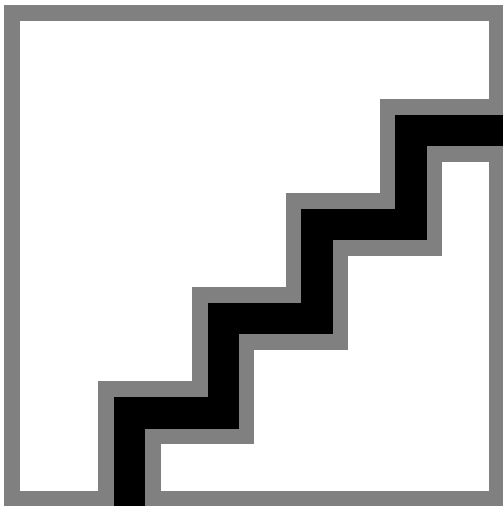
Bei der Definition der Dokumentklasse nutzen Sie anschließend das Makro @D3SET, idealerweise, indem Sie über den Button ... am Ende des Eigenschaftsfeldes die passende Restriktionsmenge auswählen.

Diese Dokumentklasse muss nicht mehr geändert werden, wenn den Anwendern andere oder erweiterte/reduzierte Werte zugeordnet werden sollen. Es reicht aus, in der Restriktionsmenge diese Werte entsprechend zu ändern!

Um diese Aufgabe nicht dem d.3-Administrator zu überlassen, können Sie Verantwortliche benennen, die das Recht erhalten, fachbezogen die Restriktionsmengen dem jeweiligen, z.B. auch kurzfristigen Bedarf auf Grund einer Krankmeldung, die Werte anders zuzuordnen.

Hierfür erhält ein solcher Fachverantwortlicher über eine Dokumentklasse auf die Systemdokumentart **\$Restriction Set\$** das entsprechende Recht.

Im Beispiel wird eine Dokumentklasse definiert, über die ein Verantwortlicher von allen definierten Berechtigungsmengen nur die mit dem Namen Standorte bedienen kann, und von allen Zuordnungen nur die Benutzerzuordnungen (1). Der Zugang erfolgt über d.3 smart explorer und einen entsprechenden Eintrag im Werkzeuge-Menü.



1.7.6. d.3-Repository-Konfiguration

Ändern des Vorspanns der Dokument-ID im d.3-Repository

Sie möchten den Vorspann der Dokument-IDs im d.3-System ändern, da die maximale Anzahl an Dokument-IDs für diesen Vorspann erreicht ist.

Um den Vorspann zu ändern, z. B. von CA nach C, müssen Sie die **d3addon.ini** für das entsprechende Repository aufrufen (... \d3\d3server.prg\d.3 Repositoryname\d3addon.ini), wobei d.3-Repositorynamen für das jeweilige d.3-Repository, z. B. d3R stehen.

Ergänzen Sie diese Datei mit dem Eintrag server = "x", wobei "x" für den entsprechenden Vorspann steht. Starten Sie anschließend den hostimp-Prozess, die d.3-Serverprozesse und den d.3 async-Prozess neu.

Alle neuen Dokumente bekommen jetzt als Dokument-ID eine Nummer aus Vorspann + Nummer z. B. C0000001.

1.7.7. Serverprozesse

Wenn Sie Serverprozesse für bestimmte Aufgaben spezialisieren möchten, müssen Sie eine Konfiguration einer alternativen d3fc-Server-ID für die Kommunikation mit d.3 gateway vornehmen.

So geht's

1. Legen Sie eine prozessspezifische Ini-Datei im Konfigurationsverzeichnis des Repositorys an.
2. In dieser Datei weisen Sie die Server-ID per Konfigurationsvariable **d3fc_alternative_server_id** zu.

Beispiel:

Erstellen Sie die Datei **dxchange_api_import.ini** mit folgendem Inhalt:

```
d3fc_alternative_server_id = "E"
```

Diese Datei wird als Process-Ini-Kommandozeilenparameter für die hinzugefügten Serverprozesse angegeben. Siehe Parameter der **d3odbc32.exe**.

3. Nun können die Prozesse mit der neuen Server-ID gezielt von ebenfalls dafür konfigurierten Clients angesprochen werden.

1.8. Infrastrukturkomponenten

1.8.1. d.ecs task

Damit Sie d.ecs task nutzen können, müssen Sie sie zunächst installieren und bei der d.ecs http gateway-App registrieren.

Aktivieren Sie den Schalter **ENABLE_TASKAPP** in der Datei **d3addon.ini**, um die d.ecs task-Unterstützung des d.3-Servers einzuschalten.

Anmerkung

Lesen Sie auch die Voraussetzungen und wichtigen Informationen zum Aktivieren des Schalters **ENABLE_TASKAPP** in unserem KB-Artikel [000001788](#) "Wie migriere ich meinen Postkorb zu d.ecs task mit dem Parameter ENABLE_TASKAPP?".

Sollte es nach Aktivieren des Schalters bei der Migration zu Fehlern gekommen sein, kann Ihnen der KB-Artikel [000001797](#) "Beheben von Migrationsfehlern nach Aktivieren des Parameters ENABLE_TASKAPP" helfen.

In zukünftigen Versionen wird d.ecs task den d.3-Postkorb vollständig ersetzen. In einer der nächsten d.3ecm Currentversionen wird dieser Schalter bei Neuinstallationen entsprechend automatisch aktiviert werden. Bei Updateinstallationen bleibt der aktuelle Status zur Nutzung des d.3-Postkorbs bzw. von d.ecs task unverändert.

Tragen Sie in d.3 config noch **DECS_SERVICE_USER** und **DECS_SERVICE_USER_PWD** ein, damit sich der d.3-Server gegenüber der Task-App authentifizieren kann. Geben Sie dem Servicebenutzer, den Sie in d.3 config angegeben haben, in der Task-App die Rolle "Servicebenutzer". Die Einrichtung hierzu finden Sie im Kapitel "Einrichten von Benutzerrollen" in der Dokumentation Administrationshandbuch d.ecs task.

Folgende Auswirkungen hat diese Aktivierung:

- Alle neuen Postkorbeinträge werden nicht mehr in der d.3-Datenbank, Tabelle wieder_vorlage erstellt, sondern direkt zu d.ecs task weitergeleitet.
- Alle API-Funktionsaufrufe mit einem direkten Postkorbbezug (außer **SendHoldFile**) laufen auf einen Fehler.

- Die bisherigen Postkorbeinträge werden an d.ecs task weitergeleitet und aus der Tabelle wieder_vorlage gelöscht. Dabei werden nur die Einträge berücksichtigt, die noch nicht quittiert wurden. Alle quittierten Einträge werden gelöscht.
- Für alle nicht quittierten Postkorbeinträge wird ein Eintrag in der Historientabelle mit dem Aktionstypen WVMIG1 erstellt.

Eine nachträgliche Deaktivierung des Schalters hat folgende Auswirkungen:

- Die Einträge bei d.ecs task werden nicht zurück in den d.3-Postkorb übertragen.

1.9. Weitere Informationsquellen und Impressum

Wenn Sie Ihre Kenntnisse rund um die d.velop-Software vertiefen möchten, besuchen Sie die digitale Lernplattform der d.velop academy unter <https://dvelopacademy.kelearning.de/>.

Mithilfe der E-Learning-Module können Sie sich in Ihrem eigenen Tempo weiterführende Kenntnisse und Fachkompetenz aneignen. Zahlreiche E-Learning-Module stehen Ihnen ohne vorherige Anmeldung frei zugänglich zur Verfügung.

Besuchen Sie unsere Knowledge Base im d.velop service portal. In der Knowledge Base finden Sie die neusten Lösungen, Antworten auf häufig gestellte Fragen und How To-Themen für spezielle Aufgaben. Sie finden die Knowledge Base unter folgender Adresse: <https://kb.d-velop.de/>

Das zentrale Impressum finden Sie unter <https://www.d-velop.de/impressum>.