

# d.veLop

d.ecs content crawler:  
Administrieren

# Inhaltsverzeichnis

1. d.ecs content crawler .....	4
1.1. Basisinformationen zur Anwendung und zum Handbuch .....	4
1.1.1. Über d.ecs content crawler .....	4
1.1.2. Architektur einer d.3ecm-Systemumgebung .....	4
1.1.3. Wissenswertes zu d.3one-Lizenzen .....	6
1.1.4. Wissenswertes zum lizenzabhängigen Funktionsumfang der d.3one-Integrationen .....	7
1.1.5. Wissenswertes zur Architektur und Arbeitsweise von d.ecs content crawler .....	8
1.2. Installieren und Deinstallieren .....	9
1.2.1. Systemvoraussetzungen .....	9
1.2.2. Vorbereiten der Installation von d.ecs content crawler .....	9
1.2.3. Installieren von d.ecs content crawler .....	11
1.2.4. Deinstallieren von d.ecs content crawler .....	12
1.2.5. Rollback einer Installation von d.ecs content crawler .....	12
1.2.6. Freigeben des Standardports für d.ecs content crawler .....	12
1.2.7. Installieren von Updates für d.ecs content crawler .....	12
1.3. Konfigurieren von d.ecs content crawler .....	12
1.3.1. Vorbereiten der Authentifizierung der Groupware-App mit OAuth 2.0 in Azure Active Directory .....	12
1.3.2. Vorbereiten der Authentifizierung der Groupware-App mit OAuth 2.0 und Microsoft Graph in Azure Active Directory .....	13
1.3.3. Angeben der Registrierungsinformationen aus Azure Active Directory für die Authentifizierung mit OAuth 2.0 .....	14
1.3.4. Festlegen von mehreren Verbindungen zum Microsoft Exchange-Server mit Microsoft Exchange (on-premises) .....	14
1.3.5. Festlegen von mehreren Verbindungen zum Microsoft Exchange-Server mit Exchange Online und Microsoft EWS .....	15
1.3.6. Festlegen von mehreren Verbindungen zum Microsoft Exchange-Server mit Exchange Online und Microsoft Graph .....	17
1.3.7. Herstellen einer Verbindung zwischen d.3one-Anwendungsserver und d.ecs domino .....	18
1.3.8. Festlegen der d.ecs domino-Verbindungsdaten in d.3one .....	18
1.3.9. Festlegen der allgemeinen Einstellungen von d.ecs content crawler .....	19
1.3.10. Konfigurieren des Datenbankservers .....	19
1.3.11. Konfigurieren einer Journalarchivierung .....	20
1.3.12. Konfigurieren einer regelbasierten Archivierung .....	22
1.3.13. Konfigurieren eines Servicebenutzers .....	26
1.3.14. Konfigurieren von Error-Jobs .....	26
1.3.15. Konfigurieren der Änderungsprotokollierung .....	27
1.4. Tipps und Tricks .....	27
1.4.1. Aktivieren von HTTPS für eine sichere Kommunikation zwischen d.ecs http gateway und den App-Instanzen (optional) .....	27
1.4.2. Anpassen des Protokollierungsgrads in d.ecs content crawler .....	29
1.4.3. Vorbereiten der Prüfung von Duplikaten .....	29
1.4.4. Aktivieren der Prüfung von Duplikaten .....	30
1.4.5. Konfigurieren einer Berechtigungsprüfung .....	30
1.4.6. Aktivieren der Funktion zum gleichzeitigen Wiederherstellen von mehreren E-Mails .....	31
1.4.7. Wiederherstellen von mehreren E-Mails aus der Ergebnisliste einer Suche .....	31
1.4.8. Überwachen von d.ecs content crawler mit d.ecs monitor .....	32
1.4.9. Überwachen der Journalarchivierung .....	32
1.4.10. Festlegen eines anderen Ports und HTTP-Protokolls .....	32
1.5. Häufig gestellte Fragen .....	32

1.5.1. Aus welchen Ordnern werden gelöschte Elemente archiviert, wenn ich das Beweissicherungsverfahren oder In-Situ Speicher aktiviert habe? .....	33
1.5.2. Für welche Nachrichtenklassen kann ich das Journaling, die Postfacharchivierung oder das manuelle Speichern mit dem Microsoft Outlook-Add-In verwenden? .....	33
1.5.3. Warum wird die Option zum Archivieren von gelöschten Elementen beim Profilerstellen nicht angezeigt? .....	37
1.5.4. Was ist der Unterschied zwischen dem Löschen und Zurücksetzen von Jobs? ..	37
1.5.5. Was ist eine Named-User-Lizenz? .....	37
1.5.6. Was sind Kategorien? .....	37
1.5.7. Was sind Profile? .....	38
1.5.8. Was sind Quellen? .....	38
1.5.9. Was sind Quellensammlungen? .....	39
1.5.10. Was sind Regelsammlungen? .....	39
1.5.11. Was sind Verarbeitungsschrittsammlungen? .....	41
1.5.12. Was sind Zuordnungen? .....	42
1.5.13. Welche Authentifizierungsmöglichkeiten habe ich beim Konfigurieren eines Datenbankservers? .....	42
1.5.14. Welche Jobs werden verarbeitet, wenn ich ein Profil für die regelbasierte Archivierung ändere? .....	42
1.5.15. Welche Quelleigenschaften sind welchen Feldnamen in HCL Notes oder Microsoft Outlook zugeordnet? .....	43
1.5.16. Wie archiviere ich PST-Dateien regelbasiert? .....	46
1.5.17. Wie archiviere ich rechtskonform mit Microsoft Exchange Online ohne ein externes Postfach? .....	46
1.5.18. Wie kann eine d.ecs content crawler-Konfiguration aufgebaut sein? (Anwendungsbeispiel) .....	46
1.5.19. Wie kann ich d.ecs content crawler ohne d.3one-Anwendungsserver verwenden? .....	47
1.5.20. Wie kann ich Detailinformationen zu Jobs anzeigen und filtern? .....	47
1.5.21. Wie kann ich regelbasiert das Verknüpfen von eingebetteten Anlagen festlegen, wenn ich HCL Domino verwende? .....	48
1.5.22. Wie konfiguriere ich eine E-Mail-Archivierung für unterschiedliche Domänen? .....	48
1.5.23. Wie konfiguriere ich eine externe Regelprüfung? .....	48
1.5.24. Wie konfiguriere ich eine externe Regelprüfung mit d.ecs script? .....	51
1.5.25. Wie öffne ich die Konfiguration der Anbindung für Microsoft Exchange oder HCL Domino? .....	53
1.5.26. Wie öffne ich die Konfiguration von d.ecs content crawler, wenn das Feature auf der Startseite nicht angezeigt wird? .....	53
1.5.27. Wie prüfe ich Duplikate von verschlüsselten oder signierten E-Mails? .....	53
1.5.28. Wie prüfe ich nach dem Verknüpfen von Zertifikat und Port, ob sich die Apps bei d.ecs http gateway mit HTTPS registrieren? .....	53
1.5.29. Wie verhindere ich, dass verschlüsselte E-Mails archiviert werden? .....	53
1.5.30. Wie verschiebe ich Datenbankeinträge zu Jobs manuell, wenn die Jobs nach dem Ändern meiner Datenbank noch vorhanden sind? .....	54
1.5.31. Wie werden E-Mails ohne Jobs von d.ecs content crawler verarbeitet? .....	54
1.5.32. Wie werden E-Mails von d.ecs content crawler verarbeitet, wenn die E-Mails verschoben wurden? .....	54
1.5.33. Wozu dient die Protokollierung? .....	54
1.5.34. Wie ordne ich eine d.3-Repository-ID einer Repository-ID zu? .....	54
1.5.35. Wie setze ich den Zähler für Jobs zurück? .....	55
1.5.36. Was sind priorisierte Profile und wie verwende ich sie? .....	55
1.6. Weitere Informationsquellen und Impressum .....	55

# 1. d.ecs content crawler

## 1.1. Basisinformationen zur Anwendung und zum Handbuch

Diese Dokumentation beschreibt das Installieren, Konfigurieren und Aktualisieren von d.ecs content crawler und richtet sich an Administratoren.

Für das Verständnis ist es hilfreich, wenn Sie über Kenntnisse in Microsoft Windows und Microsoft Outlook und/oder HCL Notes verfügen. Weitere Informationen zur Bedienung der d.3one-Integrationen finden Sie in der Kurzanleitung für die E-Mail-Integrationen von d.3one.

### 1.1.1. Über d.ecs content crawler

Mithilfe von d.ecs content crawler können Sie E-Mails regelbasiert, rechtssicher und revisionskonform in Ihrer d.3ecm-Systemumgebung zentral speichern und Ihren Anwendern bereitstellen.

Sie können die E-Mails aus Ihrem Journal mithilfe der Journalingfunktion von Microsoft Exchange und HCL Domino rechtssicher und revisionskonform in Ihrem d.3-Repository speichern.

Darüber hinaus können Sie den E-Mails Akten und Vorgänge zuordnen oder E-Mails einfach rechtskonform im d.3-Repository speichern.

d.ecs content crawler ist primärer Bestandteil folgender Lösungspakete:

- dbs | journal archiver for Microsoft Exchange
- dbs | journal archiver for IBM Domino
- dbs | mailbox archiver for Microsoft Exchange
- dbs | mailbox archiver for IBM Domino

Wenn Ihre Anwender weder d.3one in Microsoft Outlook noch d.3one in IBM Notes erworben haben, können sie mithilfe eines Add-Ins oder Widgets bei Bedarf E-Mails wiederherstellen und Elemente lokal speichern. Weitere Informationen zu diesem Thema finden Sie im Kapitel zum lizenzabhängigen Funktionsumfang der d.3one-Integrationen.

### 1.1.2. Architektur einer d.3ecm-Systemumgebung

Die d.velop AG setzt auf eine moderne Software-Architektur, die u.a. auf Microservices basiert.

Beispielsweise ist d.3ecm eine Sammlung einzelner Microservices, die interagieren und dem Anwender die DMS-Funktionalitäten an der Benutzeroberfläche bereitstellen. Jeder Microservice ist eine eigenständige Anwendung.

In der d.3ecm-Architektur wird ein Microservice als App bezeichnet.

Jedes d.velop-Produkt besteht aus eigenen Apps, die spezifisch für das Produkt sind und mit einem eigenen Setup installiert werden. Wenn beispielsweise von einer App mehrere App-Instanzen installiert sind (z.B. im Clusterbetrieb oder zwecks Skalierung), müssen alle Apps die gleiche Version aufweisen.

Mit diesem Architekturdesign können Sie den Anforderungen Ihrer Serverumgebung entsprechend flexibel entscheiden, welche App Sie wie häufig auf welchem Host in einer d.3.ecm-Umgebung installieren. Sie haben mit diesem Architekturdesign die größtmögliche Freiheit, Ihre speziellen Anforderungen der IT-Umgebung zu berücksichtigen.

Neben den produktspezifischen Apps gibt es die zentralen Apps, die Sie immer separat berücksichtigen müssen.

#### Zentrale Apps in der d.velop documents-Architektur

In der d.velop documents-Systemlandschaft gibt es eine Reihe von Apps, die eine zentrale Bedeutung für viele Produkte der d.velop AG haben. Alle folgenden Apps werden als Produkt **Infrastruktur** mithilfe von d.velop software manager installiert und sind nicht Gegenstand anderer d.velop-Produkte:

### **d.ecs http gateway**

Die d.ecs http gateway-App ist die zentrale HTTP-Schnittstelle zu allen Apps in einer d.3ecm-Umgebung. Die gesamte HTTP-Kommunikation findet über diese App statt. Technisch gesehen ist es ein Reverse Proxy. Jede App registriert sich bei der d.ecs http gateway-App. Anschließend ist die neu registrierte App unter `https://<BaseUri>/<App-Name>` für alle anderen Apps erreichbar. Sollen in einer d.3ecm-Umgebung mehrere d.ecs http gateway-Apps ausgeführt werden, müssen alle d.ecs http gateway-Apps unter derselben Basisadresse erreichbar sein. Pro d.3ecm-Umgebung darf es nur eine Basisadresse geben.

### **d.ecs jstore**

Die App d.ecs jstore ist eine NoSQL-Datenbank, die häufig vom d.3-Server angefragte Daten, wie z.B. Eigenschaftswerte für häufig gesuchte Dokumente, im Speicher des Anwendungsservers zwischenspeichert. Die erforderlichen Datenbankzugriffe auf die d.3-Datenbank werden auf diese Weise reduziert und somit wird die Leistungsfähigkeit des gesamten Systems erhöht.

Zudem wird d.ecs jstore von den unterschiedlichen d.velop-Komponenten (z.B. d.3one, d.ecs monitor) genutzt, um Daten zu persistieren.

d.ecs jstore basiert auf Redis (Remote Dictionary Server) und ersetzt Couchbase als Zwischenspeicher, das bis zur d.3ecm Version 8.0 eingesetzt wurde. Die App ist unter anderem leichter zu konfigurieren und bietet damit deutliche Vorteile gegenüber der bisherigen Lösung.

Die App d.ecs jstore wird pro Windows-Host installiert, auf dem eine d.velop-App ausgeführt wird.

In einer d.3ecm-Umgebung müssen die einzelnen d.ecs jstore-Instanzen, die sich jeweils auf einem Windows-Host befinden, zu einem Cluster zusammengeführt werden, damit ein Datenaustausch stattfinden kann.

### **d.ecs identity provider**

Die App d.ecs identity provider übernimmt stellvertretend für die einzelnen Apps die Authentifizierung von Benutzern. Zur Authentifizierung können Systeme wie z.B. der Windows Active Directory-Dienst genutzt werden. Die Autorisierung des Benutzers ist Aufgabe der jeweiligen App.

### **d.ecs shell**

Die d.ecs shell-App stellt den gemeinsamen Rahmen für die HTML-Oberflächen der einzelnen Apps bereit und implementiert ein einheitliches Bedienkonzept, sodass die Oberflächen der Apps konsistent sind und wie aus einem Guss wirken. Die App bietet darüber hinaus Zugriff auf die nativen Funktionen des Hosts. Mit einem Host ist in diesem Zusammenhang z.B. eine E-Mail-Anwendung, eine ERP-Anwendung oder auch ein Browser gemeint.

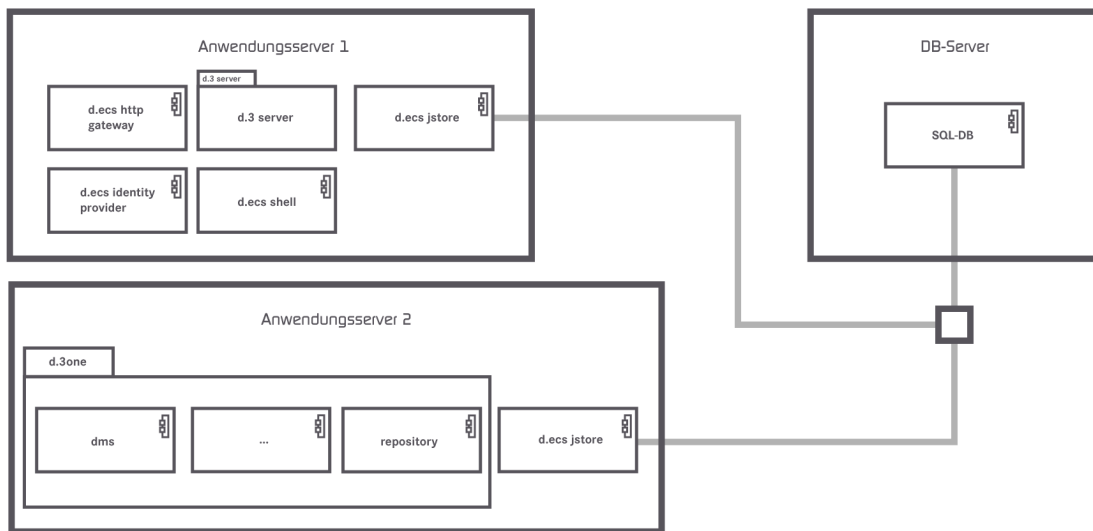
### **Mögliche Szenarien für eine d.3ecm-Umgebung mit d.3one**

Sie können Ihre d.3ecm-Umgebung ganz speziell gemäß den Anforderungen Ihres Unternehmens oder Ihrer Organisation gestalten. Sie haben die Möglichkeit, mindestens einen zentralen Anwendungsserver zu nutzen oder die Apps auf verschiedene Anwendungsserver zu verteilen. Es bleibt Ihren Ansprüchen und Anforderungen an die IT-Umgebung überlassen, wie Sie Ihre d.3ecm-Umgebung organisieren.

#### **Beispiel 1**

Die zentralen Apps wurden auf einem Anwendungsserver installiert, während die produktspezifischen Apps auf einem anderen Anwendungsserver installiert wurden.

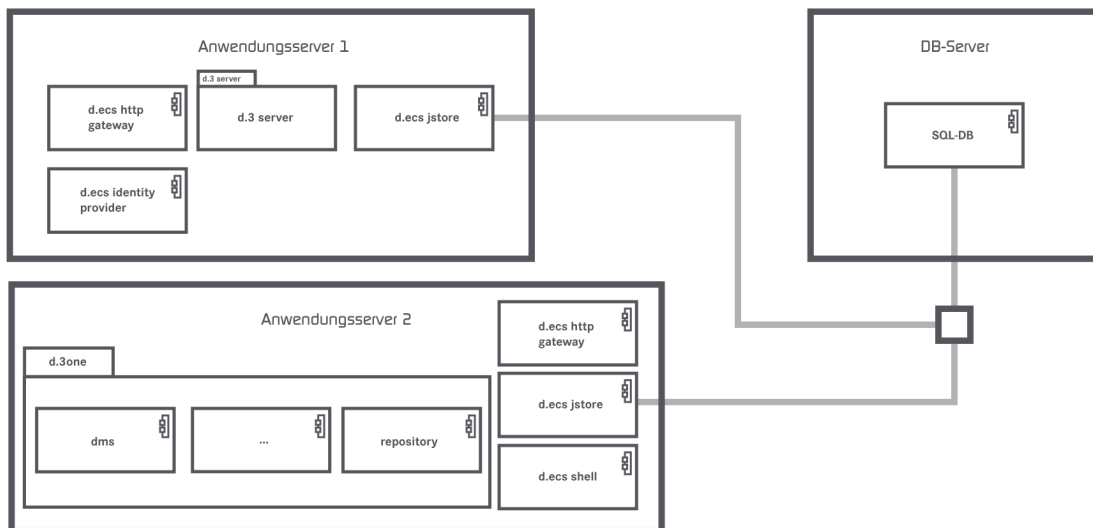
## d.3ecm-Umgebung



### Beispiel 2

Die zentralen Apps wurden auf zwei Anwendungsservern verteilt, und die d.ecs http gateway-App ist in der d.3ecm-Umgebung zweimal vorhanden.

## d.3ecm-Umgebung



Wenn Sie Fragen zum Clusterbetrieb oder zur Skalierung haben, wenden Sie sich an Ihren d.velop-Ansprechpartner.

### 1.1.3. Wissenswertes zu d.3one-Lizenzen

Mit d.3one als Integration können Anwender d.3-Funktionalitäten einfach in anderen Anwendungen verwenden, z.B.:

- Browser
- Microsoft Outlook
- Microsoft Office
- HCL Notes
- SAP ERP
- Kundenspezifische Integrationen

Jede Integration muss für jeden Anwender erworben werden. Die Anzahl der Anwender der einzelnen Produkte kann innerhalb einer Installation von d.3one unterschiedlich sein; z.B. können 200 Anwender d.3one im Browser verwenden, aber nur 50 Anwender d.3one in Microsoft Outlook. Im Gegensatz zu einer d.3ecm-Systemumgebung ist d.3one eine separate Integrationsanwendung.

Wenn ein Anwender d.3one im Browser oder als Integration verwendet, werden lizenzrelevante Informationen aus dem d.3-Repository abgerufen. Mit jedem Zugriff bucht jeder d.3one-Anwender eine Benutzerlizenz in der d.3ecm-Systemumgebung ab. Stellen Sie sicher, dass für alle Anwender, die die d.3ecm-Systemumgebung direkt oder indirekt verwenden, genug Basislizenzen vorhanden sind. Wir empfehlen, einheitlich Named-User-Lizenzen zu verwenden.

### Anmerkung

Achten Sie vor dem Installieren von d.3one oder den Integrationen darauf, dass genug d.3-Clientzugriffslizenzen (d.3-CALs) vorhanden sind. Wir empfehlen ein durchgängiges Named-User-Lizenzmodell, in dem für jeden d.3one-Anwender genug d.3-Clientzugriffslizenzen vorhanden sind.

Abhängig vom erworbenen Produkt stehen Ihnen für die E-Mail-Integrationen verschiedene Funktionen zur Verfügung.

Bei weiteren Fragen zur Lizenzierung von d.3one wenden Sie sich an Ihren d.velop-Ansprechpartner.

Siehe auch: [Detailinformationen zu Named-User-Lizenzen](#)

## 1.1.4. Wissenswertes zum lizenzabhängigen Funktionsumfang der d.3one-Integrationen

Mit d.ecs content crawler werden auch die d.3one-Integrationen für Microsoft Outlook und HCL Notes ausgeliefert. Sie können das Add-In oder das Widget bei Bedarf an Ihre Anwender verteilen. Weitere Informationen finden Sie in den Administrationshandbüchern von d.3one in Microsoft Outlook und d.3one in IBM Notes.

Der Funktionsumfang der Integrationen richtet sich nach den erworbenen Lizenzen. Mithilfe der folgenden Liste können Sie nachvollziehen, welche Funktionen Ihnen für die entsprechenden Lizenzen zur Verfügung stehen.

### Keine Lizenz

- Wiederherstellen eines Elements aus einem d.3-Repository
- Offline Store oder Offline Speicher

### Basislizenz

- Wiederherstellen eines Elements aus einem d.3-Repository
- Offline Store oder Offline Speicher
- Speichern von E-Mails und Anlagen mit dem Kontextmenü
- Suchen im d.3-Repository

### Volle Lizenz

- Wiederherstellen eines Elements aus einem d.3-Repository
- Offline Store oder Offline Speicher
- Speichern von E-Mails und Anlagen mit dem Kontextmenü
- Suchen im d.3-Repository
- Speichern von Elementen in Akten mit Drag & Drop
- Senden und gleichzeitiges Speichern von Elementen in einem d.3-Repository mit der **Senden und ablegen**-Funktion
- Öffnen von E-Mail-Inhalten in anderen Anwendungen mit der **Gehe zu**-Funktion
- Aufgaben und Nachrichten
- Kontextsensitives Suchen mit der **Suche nach**-Funktion
- Verwenden der d.3one-Funktionen
- Öffnen von d3l-Verweisdateien
- Versenden eines Elements per E-Mail als Originaldatei oder PDF-Datei
- Erstellen einer neuen Version eines Dokuments mit Änderungstext
- Aktualisieren von Dokumenteigenschaften
- Anzeigen von Dokumenten während der Bearbeitung
- Anzeigen von Eigenschaften einer archivierten E-Mail
- Exportieren der Eigenschaften von mehreren Elementen
- Exportieren von Dokumenten als PDF-Datei

### 1.1.5. Wissenswertes zur Architektur und Arbeitsweise von d.ecs content crawler

Damit Sie die Funktionen von d.ecs content crawler besser verstehen können und Ihre Systemumgebung anpassen können, finden Sie in diesem Artikel Informationen zum Aufbau und der Arbeitsweise von d.ecs content crawler.

Anhand des folgenden Schaubilds können Sie nachvollziehen, wie Profile oder Konfigurationen für die Journalarchivierung von d.ecs content crawler verarbeitet werden:



d.ecs content crawler verarbeitet Profile, die Sie nach Ihren Bedürfnissen konfigurieren können. Mithilfe der Profile legen Sie fest, welche Maildatenbanken, Postfächer oder Journalpostfächer von d.ecs content crawler verarbeitet werden. Darüber hinaus können Sie z.B. individuell festlegen, wie viele Profile oder Dokumente maximal verarbeitet werden.

In d.ecs content crawler verarbeitet ein Profile-Controller ein Konfigurationsdokument und ermittelt die notwendige Anzahl von Maildatenbanken. Für jede Maildatenbank oder jedes Postfach wird eine Profile-Worker-Instanz erzeugt. Wenn mehr Postfächer verarbeitet werden müssen als Verarbeitungsinstanzen vorhanden sind, werden die Postfächer gleichmäßig auf die Instanzen verteilt. Die Journalkonfiguration zählt auch als Profil.

Die Profile-Worker-Instanz ermittelt die zu archivierenden Dokumente anhand der im Profil festgelegten Regeln. Pro Durchlauf wird die Anzahl von Dokumenten ermittelt.

Jede Profile-Worker-Instanz erzeugt die notwendige Anzahl Document-Worker. Die ermittelte Anzahl von zu archivierenden Dokumenten je Datenbank wird gleichmäßig auf die vorhandenen Document-Worker verteilt.

Basierend auf einer zuvor erstellten Zuordnung (Mapping) speichern die Document-Worker die Dokumente mithilfe der Groupware-App und der DMS-App im d.3-Repository mit den entsprechenden E-Mail-Eigenschaften und d.3-Eigenschaften.

Siehe auch: [Beispielaufbau einer d.ecs content crawler-Konfiguration](#)

## 1.2. Installieren und Deinstallieren

In diesem Thema finden Sie Informationen zum Installieren, Aktualisieren und Deinstallieren von d.ecs content crawler und den notwendigen Komponenten.

### 1.2.1. Systemvoraussetzungen

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

Wenn Sie Microsoft Exchange Online verwenden, werden archivierte E-Mails in den Postfächern (Stubs) nicht volltextindiziert. Die Stubs werden bei einer Volltextsuche von Microsoft Outlook nicht gefunden. Die Stubs werden weiterhin wie gewohnt in den Ordnern angezeigt. Die Volltextindizierung erfolgt, wenn die Microsoft Outlook-Kategorie anstatt der Archiv-Nachrichtenklasse angegeben wird.

Damit Ihre Anwender weiterhin mit einer lokal installierten Microsoft Outlook-Anwendung nach archivierten Inhalten suchen können, haben Sie folgende Möglichkeiten:

- Aktivieren Sie den Cachemodus in Microsoft Outlook.
- Verwenden Sie die erweiterte Suche in Microsoft Outlook (**Start > E-Mail filtern > Weitere Filter > Suchtools > Erweiterte Suche**).
- Stellen Sie Ihren Anwendern einen Ordner für die Startseite bereit, mit dem im d.3-Repository nach den archivierten E-Mails gesucht wird (direkte Verknüpfung zur Ergebnisliste).

### 1.2.2. Vorbereiten der Installation von d.ecs content crawler

Bevor Sie d.ecs content crawler installieren, müssen Sie die Installation vorbereiten. Folgende Aufgaben müssen Sie vor der Installation von d.ecs content crawler erledigen:

- Installieren und konfigurieren Sie den d.3one-Anwendungsserver mit den entsprechenden Groupware-App-Komponenten.
- Installieren Sie die d.velop-Infrastrukturkomponenten. Informationen zum Installieren der zentralen Infrastruktur-Apps finden Sie im Konfigurationsleitfaden für d.velop-Infrastrukturkomponenten. Wenn Sie Kerberos verwenden möchten, müssen Sie vor dem Installieren von Kerberos d.ecs identity provider installieren und konfigurieren.
- Stellen Sie sicher, dass die Rechte **Statustransfer Bearbeitung** und **Statustransfer Freigabe** in der Administration von d.3 erteilt sind.
- Erstellen Sie eine Testumgebung für E-Mail-Archivierungsprojekte. Konfigurieren Sie die Testumgebung so, dass Sie Fehler im Produktivsystem nachstellen können. Eine Testumgebung kann Ihnen helfen, neue Funktionen zu überprüfen, bevor Sie eine neue Version für das Produktivsystem installieren.

## Wissenswertes zum Verwenden von d.ecs content crawler mit HCL Domino

Wenn Sie d.ecs content crawler mit HCL Domino verwenden, empfehlen wir, den d.ecs domino-Service nicht auf dem produktiven Mailserver oder einem hoch frequentierten HCL Domino-Server zu installieren. Erstellen Sie einen eigenen Server oder verwenden Sie einen wenig ausgelasteten Server, um den produktiven Betrieb sicherzustellen.

### Warnung

Das Verwenden des d.ecs domino-Dienstes kann sich negativ auf die Funktionsweise von HCL Domino Server auswirken. Wir raten daher dringend davon ab, den d.ecs domino-Dienst für ein unternehmenskritisches HCL Domino-System zu verwenden. Stellen Sie HCL Domino Server als eigenständigen Server bereit, um E-Mails mit dem d.ecs domino-Dienst zu verarbeiten. Sie können den d.ecs domino-Dienst z.B. auch mit dem d.3one-Anwendungsserver verwenden.

## Erteilen von Berechtigungen für Microsoft Exchange Server

Zum Sicherstellen der Microsoft Exchange Server-Konnektivität müssen Sie ein Benutzerkonto angeben, das Zugriffsrecht auf alle Microsoft Exchange Server-Postfächer in Ihrer Organisation hat. Stellen Sie sicher, dass das Zertifikat zur URL gültig ist.

Das Benutzerkonto für den EWS-Connector (Exchange Web Services, Exchange-Webdienst) sollte dasselbe Benutzerkonto sein, mit dem Sie d.3one installieren.

Sie müssen sicherstellen, dass das Benutzerkonto über die erforderlichen Berechtigungen für Microsoft Exchange Server verfügt, insbesondere das Recht **Exchange-Identitätswechsel** (Rolle **Exchange Impersonation**). Mit diesem Recht können Aktionen auf allen Postfächern im Namen der entsprechenden Besitzer ausgeführt werden.

Sie benötigen für das Benutzerkonto zum Identitätswechsel nur dann ein Microsoft Exchange-Postfach, wenn Sie d.ecs content crawler verwenden. Für d.3one in Microsoft Outlook ist kein Microsoft Exchange-Postfach für den Identitätswechsel notwendig.

Sie können die Berechtigungen mit dem folgenden PowerShell-Befehl ändern:

```
New-ManagementRoleAssignment -Name:impersonationAssignmentName -
Role:ApplicationImpersonation
```

Wenn Sie dem Benutzerkonto nur Rechte auf bestimmte Postfächer erteilen möchten, können Sie mit einem Filter für einen regulären, gefilterten Empfängerbereich (**RecipientRestrictionFilter**) die Berechtigungen einschränken.

Sie können z.B. einen PowerShell-Befehl angeben, um einen Exchange-Identitätswechsel für das Dienstkonto auf die Postfächer 1 und 2 zu erteilen.

### Beispiel

```
New-ManagementScope -Name d3oneImpersonationScope
-RecipientRestrictionFilter { (Name -eq "Mailbox1") -or (Name -eq
"Mailbox2") }
New-ManagementRoleAssignment -Name d3oneImpersonation -Role
ApplicationImpersonation -User "serviceAccount" -CustomRecipientWriteScope
d3oneImpersonationScope
```

Alternativ können Sie den Exchange-Identitätswechsel in Office 365 oder Microsoft Exchange Online unter **Exchange Admin Center > Berechtigungen** konfigurieren.

Weitere Informationen zum Filtern finden Sie auf der Microsoft Docs-Website in der Dokumentation von Exchange Server 2013 unter "Grundlegendes zu Verwaltungsrollenbereichs-Filtern".

## Zuweisen von Einschränkungrichtlinien für den Dienstbenutzer in Microsoft Exchange Server

Damit d.3one in Microsoft Outlook in Verbindung mit Microsoft Exchange Server funktioniert, müssen Sie für den Dienstbenutzer mit der Rolle **ApplicationImpersonation** auf dem Server mit Microsoft Exchange Server eine gesonderte Einschränkungrichtlinie (Throttling Policy) erstellen und zuweisen.

### Für Microsoft Exchange Version 2010

Erstellen Sie die folgende Richtlinie in der Microsoft Exchange-Verwaltungskonsolle.

```
New-ThrottlingPolicy d3onepolicy
Set-ThrottlingPolicy d3onepolicy -RCAMaxConcurrency $null
-RCAPercentTimeInAD $null -RCAPercentTimeInCAS $null
-RCAPercentTimeInMailboxRPC $null -EWSMaxConcurrency $null
```

```
-EWSPercentTimeInAD $null -EWSPercentTimeInCAS $null
-EWSPercentTimeInMailboxRPC $null -EWSMaxSubscriptions $null
-EWSFastSearchTimeoutInSeconds $null -EWSFindCountLimit $null
-CPAMaxConcurrency $null -CPAPercentTimeInCAS $null
-CPAPercentTimeInMailboxRPC $null -CPUStartPercent $null
```

Weisen Sie die Richtlinie dem Dienstbenutzer zu.

```
Set-Mailbox "user name" -ThrottlingPolicy d3onepolicy"
```

### Ab Microsoft Exchange Version 2013

Erstellen Sie die folgende Richtlinie in der Microsoft Exchange-Verwaltungskonsole.

```
New-ThrottlingPolicy -Name d3onepolicy -ThrottlingPolicyScope Regular
-IsServiceAccount -MessageRateLimit unlimited -RcaCutoffBalance Unlimited
-RcaMaxBurst unlimited -RcaRechargeRate unlimited -RcaMaxConcurrency
unlimited -RecipientRateLimit unlimited -EwsMaxConcurrency
unlimited -CpaMaxConcurrency unlimited -EwsCutoffBalance unlimited
-EwsMaxSubscriptions unlimited
```

Weisen Sie die Richtlinie dem Dienstbenutzer zu.

```
Set-ThrottlingPolicyAssociation -Identity "user name" -ThrottlingPolicy
d3onepolicy
```

### 1.2.3. Installieren von d.ecs content crawler

Sie installieren die Software ausschließlich mit d.velop software manager. Wird eine Anwendung für verschiedene Produkte benötigt, werden die zugehörigen Softwarepakete ebenfalls automatisch installiert.

Weitere Informationen zum Installieren der Software finden Sie im d.velop software manager-Handbuch.

Installieren Sie die d.ecs content crawler-App auf dem d.3one-Anwendungsserver. Bei einer Basisinstallation (maximal zehn Postfächer) oder einer Testumgebung können Sie den Windows-Dienst von d.ecs content crawler auch auf dem d.3one-Anwendungsserver installieren. Bei größeren Systemen mit erhöhter Auslastung empfehlen wir, d.ecs content crawler auf dedizierten Servern zu installieren.

Für das Setup von d.ecs content crawler installieren Sie folgende Komponenten:

- d.ecs groupware
- d.ecs mail converter
- d.ecs content crawler-App
- d.ecs domino service setup
- DGI2HTML
- DGI2EML

Zusätzlich zu d.ecs content crawler werden die Integrationen für Microsoft Outlook und HCL Notes ausgeliefert. Der Funktionsumfang der Integrationen ist abhängig von den erworbenen Lizenzen. Sie können bei Bedarf die Integrationen an Ihre Anwender verteilen. Weitere Informationen zum Verteilen der Integrationen finden Sie in den Administrationshandbüchern von d.3one in Microsoft Outlook und d.3one in IBM Notes.

Bei einer Neuinstallation kann es vorkommen, dass Daten einer vorherigen Installation noch eingetragen sind. Diese Daten wurden bei der vorherigen Deinstallation nicht gelöscht. Ändern Sie ggf. die Daten entsprechend.

### 1.2.4. Deinstallieren von d.ecs content crawler

Sie können die Software, die Sie mit d.velop software manager installiert haben, nur mit d.velop software manager wieder deinstallieren. Falls es bei der zu deinstallierenden Software Abhängigkeiten zu anderen Softwarepaketen gibt, müssen Sie diese Konflikte entsprechend auflösen.

Weitere Informationen zum Deinstallieren finden Sie im d.velop software manager-Handbuch.

### 1.2.5. Rollback einer Installation von d.ecs content crawler

Sie können von der Software, die Sie mit d.velop software manager installiert haben, eine frühere Version wiederherstellen. Bei diesem Prozess wird die Software nur auf eine vorherige Version zurückgesetzt.

Weitere Informationen zur Wiederherstellung einer früheren Version finden Sie im d.velop software manager-Handbuch.

### 1.2.6. Freigeben des Standardports für d.ecs content crawler

- Standardmäßig wird der Port für d.ecs content crawler dynamisch ermittelt. Sie können jedoch auch einen Port festlegen.

### 1.2.7. Installieren von Updates für d.ecs content crawler

Sie installieren Updates für d.ecs content crawler standardmäßig mit d.velop software manager.

Wenn in Ihrer Systemumgebung eine frühere Version statt der unmittelbar vorherigen Version installiert ist, wenden Sie sich an Ihren d.velop-Ansprechpartner.

## 1.3. Konfigurieren von d.ecs content crawler

In diesem Thema finden Sie Informationen zum Konfigurieren von d.ecs content crawler und den notwendigen Komponenten.

### 1.3.1. Vorbereiten der Authentifizierung der Groupware-App mit OAuth 2.0 in Azure Active Directory

Wenn Sie Microsoft Office 365 in Verbindung mit der Groupware-App verwenden, legen Sie fest, dass die Groupware-App mit OAuth 2.0 authentifiziert wird. Diese Art der Authentifizierung wird von Microsoft empfohlen.

Für die Authentifizierung mit OAuth 2.0 müssen Sie zunächst die Konfiguration in Azure Active Directory anpassen. Im Anschluss passen Sie die Einstellungen in der Groupware-App entsprechend an.

Sie müssen folgende Vorbereitungen für die Authentifizierung mit OAuth 2.0 in Azure Active Directory vornehmen:

- **Registrieren der Groupware-App in Azure Active Directory:** Fügen Sie eine neue App-Registrierung für die Groupware-App hinzu. Wählen Sie als unterstützte Kontotypen **Nur Konten in diesem Organisationsverzeichnis** aus. Geben Sie die Basisadresse der d.3one-Systemumgebung als Umleitungs-URI an.
- **Konfigurieren der API-Berechtigungen:** Fügen Sie für die API-Berechtigungen folgende Berechtigung hinzu: **Use Exchange Web Services with full access to all mailboxes (full\_access\_as\_app)**
- **Erzeugen eines geheimen Clientschlüssels:** Erstellen Sie einen neuen geheimen Clientschlüssel. Kopieren Sie den Schlüssel direkt in die Zwischenablage, um den Schlüssel im Anschluss in der Groupware-App einzufügen.
- **Ermitteln der Anwendungs-ID und der Verzeichnis-ID:** Kopieren Sie die IDs aus der Zusammenfassung der App-Registrierung der Groupware-App in die Zwischenablage, um die IDs im Anschluss in der Groupware-App einzufügen.

Erstellen Sie außerdem eine Zugriffsrichtlinie für die Groupware-App in Microsoft 365. Weitere Informationen finden Sie in unserer Knowledge Base in folgendem Artikel: <https://kb.d-velop.de/s/article/000001683>

Im Anschluss müssen Sie für die Authentifizierung mit OAuth 2.0 die Einstellungen in der Groupware-App entsprechend anpassen.

### 1.3.2. Vorbereiten der Authentifizierung der Groupware-App mit OAuth 2.0 und Microsoft Graph in Azure Active Directory

Wenn Sie Microsoft Office 365 in Verbindung mit der Groupware-App und Microsoft Graph verwenden, stellen Sie sicher, dass die Groupware-App mit OAuth 2.0 authentifiziert wird. Diese Art der Authentifizierung wird von Microsoft empfohlen.

#### Anmerkung

Folgende Funktionen werden nicht von der Microsoft Graph-Schnittstelle unterstützt:

- Zugriff auf öffentliche Ordner
- Zugriff auf das Online-Archiv
- Importieren und Exportieren der vollständigen Daten der Nachrichtenklassen **Aufgaben (IPM.Task)** und **Verteilerliste (IPM.DistList)**
- Vorgeben der Farbe einer Kategorie (die Farbe muss von jedem Anwender selbst festgelegt werden)

Wenn Sie d.ecs content crawler verwenden, gelten zusätzlich folgende Einschränkungen:

- Die Journalarchivierung wird nicht unterstützt.
- Aus der d.velop documents-Ergebnisliste können nur E-Mail-Elemente wiederhergestellt werden.

Für die Authentifizierung mit OAuth 2.0 müssen Sie zunächst die Konfiguration in Azure Active Directory anpassen. Im Anschluss passen Sie die Einstellungen in der Groupware-App entsprechend an.

Sie müssen folgende Vorbereitungen für die Authentifizierung mit OAuth 2.0 in Azure Active Directory vornehmen:

- **Registrieren der Groupware-App in Azure Active Directory:** Fügen Sie eine neue App-Registrierung für die Groupware-App hinzu. Legen Sie fest, welche Konten auf die API zugreifen können. Geben Sie die Basisadresse der d.velop documents-Systemumgebung als Umleitungs-URI an.
- **Konfigurieren der API-Berechtigungen:** Fügen Sie für folgende API-Berechtigungen aus dem Bereich **Microsoft Graph > Anwendungsberechtigungen** hinzu:
  - **Group.Read.All**
  - **GroupMember.Read.All**
  - **Mail.ReadWrite**
  - **MailboxSettings.Read**
  - **MailboxSettings.ReadWrite** (Diese Berechtigung ist für das Verwenden einer Farbe je Kategorie erforderlich.)
  - **Member.Read.Hidden**
  - **User.Read.All**

## Warnung

Zum 31.12.2026 ändert Microsoft die MSGraph-API. Um in Zukunft Extended-Properties in E-Mails zu schreiben, wird eine zusätzliche Berechtigung (**Mail-Advanced.ReadWrite.All**) benötigt. Dies hat u.a. signifikanten Einfluss auf d.ecs content crawler und d.ecs groupware.

Wenn die neue Berechtigung in der Appregistrierung nicht festgelegt ist, können keine E-Mails mehr bearbeitet werden.

- **Erteilen der Administrationszustimmung:** Wählen Sie für die entsprechenden API-Berechtigungen **Administratorzustimmung für <Mandantename> erteilen** aus.
- **Erzeugen eines geheimen Clientschlüssels:** Erstellen Sie einen neuen geheimen Clientschlüssel. Kopieren Sie den Schlüssel direkt in die Zwischenablage, um den Schlüssel im Anschluss in der Groupware-App einzufügen.
- **Ermitteln der Anwendungs-ID und der Verzeichnis-ID:** Kopieren Sie die IDs aus der Zusammenfassung der Appregistrierung der Groupware-App in die Zwischenablage, um die IDs im Anschluss in der Groupware-App einzufügen.

Erstellen Sie außerdem eine Zugriffsrichtlinie für die Groupware-App in Microsoft 365. Weitere Informationen finden Sie im Artikel [Wie erstelle ich eine Zugriffsrichtlinie \(Application Access Policy\) für d.ecs groupware in Microsoft 365?](#) (Knowledge Base).

Im Anschluss müssen Sie für die Authentifizierung mit OAuth 2.0 die Einstellungen in der Groupware-App entsprechend anpassen.

### 1.3.3. Angeben der Registrierungsinformationen aus Azure Active Directory für die Authentifizierung mit OAuth 2.0

Wenn Sie die Groupware-App in Azure Active Directory registriert haben und die notwendigen IDs und den geheimen Clientschlüssel kopiert haben, müssen Sie die Einstellungen in der Groupware-App entsprechend anpassen.

#### So geht's

1. Öffnen Sie das Feature **Konfiguration** auf der Startseite und navigieren Sie in der Kategorie **Dokumentenmanagement** zu **E-Mails**.
2. Wählen Sie unter **E-Mail-Verwaltung** den Eintrag **Microsoft Exchange** aus.
3. Wählen Sie in der Perspektive **Verbindungseinstellungen** unter **Exchange-Webdienste-Authentifizierungsmethode** den Eintrag **OAuth 2.0 (Microsoft Office 365)** aus.
4. Geben Sie unter **Office 365 Verzeichnis-ID** die Verzeichnis-ID ein, die Sie zuvor in Azure Active Directory in die Zwischenablage kopiert haben.
5. Geben Sie unter **Office 365 Anwendungs-ID für d.ecs groupware** die Anwendungs-ID ein, die Sie zuvor in Azure Active Directory in die Zwischenablage kopiert haben.
6. Geben Sie unter **Office 365 API-Zugriffsschlüssel für Exchange-Webdienste** den geheimen Client-schlüssel ein, die Sie zuvor in Azure Active Directory in die Zwischenablage kopiert haben.
7. Fügen Sie den Benutzer für den Identitätswechsel in den Exchange-Webdiensten ein.
8. Speichern Sie Ihre Angaben und starten Sie die Groupware-App neu.

### 1.3.4. Festlegen von mehreren Verbindungen zum Microsoft Exchange-Server mit Microsoft Exchange (on-premises)

Sie können die Verbindung zum Microsoft Exchange-Server festlegen und mehrere unterschiedliche Exchange-Server mit der Groupware-App verbinden.

Beachten Sie für die Verbindung mit Microsoft Exchange Server, dass das SSL-Zertifikat qualifiziert und gültig ist.

Folgende Bedingungen gelten für den Benutzer für den Identitätswechsel:

- Für Exchange Online in Microsoft 365: Der Benutzer benötigt ein Postfach (EWS und OAuth 2.0).
- Microsoft Exchange-Server (on-premises): Der Benutzer benötigt ein Postfach (EWS und Basic), wenn auf öffentliche Ordner zugegriffen wird.
- Geben Sie als Benutzernamen die SMTP-Adresse an, um den Zugriff auf öffentliche Ordner zu gewährleisten.

Sie können als weitere Microsoft Exchange-Verbindung zwischen Microsoft Exchange (on-premises) und Exchange Online auswählen. Für Microsoft Exchange (on-premises) ist nur Microsoft EWS zulässig. Exchange Online kann Microsoft EWS oder Microsoft Graph nutzen.

Wenn Sie eine Microsoft Exchange-Konfiguration löschen möchten, stellen Sie sicher, dass die Konfiguration nicht mehr verwendet wird.

Angenommen, Sie möchten die Verbindungseinstellungen für den Microsoft Exchange-Server festlegen und als weitere Verbindung Microsoft Exchange (on-premises) hinzufügen.

### So geht's

1. Öffnen Sie das Feature **Konfiguration** auf der Startseite und navigieren Sie in der Kategorie **Dokumentenmanagement** zu **E-Mails**.
2. Wählen Sie unter **E-Mail-Verwaltung** den Eintrag **Microsoft Exchange** aus.
3. Wechseln Sie in die Perspektive **Verbindungseinstellungen**.
4. Wählen Sie **Microsoft Exchange Dienste aktivieren** aus.
5. Geben Sie alle notwendigen Parameter für die erste Verbindung ein.
6. Klicken Sie auf das Plusymbol, um die Parameter als eine zusätzliche Verbindung hinzuzufügen.
7. Geben Sie die akzeptierten Domänen des Microsoft Exchange-Servers an. Trennen Sie die Domänen durch ein Komma.
8. Wählen Sie unter **Exchange-API** als Schnittstelle **Microsoft EWS** aus.
9. Geben Sie unter **Exchange-Webdienste-Server** den vollqualifizierten Namen Ihres Exchange-Servers (on-premises) im Format <Name des Servers>.<Name der Domäne> an.
10. Wählen Sie Ihren Port unter **Exchange-Webdienste-Port** aus. Der Standardwert ist **443**.
11. Legen Sie die entsprechende Version unter **Exchange Web Service-Version** fest. Der Standardwert ist **Autodetect**.
12. Legen Sie die Authentifizierungsmethode für die die Exchange-Webdienste fest. Bei Microsoft Exchange (on-premises) ist nur **Basic** zulässig.
13. Tragen Sie den Benutzer zum Identitätswechsel und das Kennwort ein.
14. Wählen Sie bei Bedarf die Option **Postfächer per AutoErmittlung öffnen (hybride Umgebungen)** aus.

Siehe auch:

- [Festlegen von mehreren Verbindungen zum Microsoft Exchange-Server mit Exchange Online und Microsoft EWS](#)
- [Festlegen von mehreren Verbindungen zum Microsoft Exchange-Server mit Exchange Online und Microsoft Graph](#)

### 1.3.5. Festlegen von mehreren Verbindungen zum Microsoft Exchange-Server mit Exchange Online und Microsoft EWS

#### Warnung

Microsoft deaktiviert zum 01.10.2026 die Exchange-Webdienste (EWS) für alle externen Anwendungen in Exchange Online. Diese Deaktivierung hat auch Auswirkungen auf die d.velop-Komponenten d.ecs groupware und d.ecs content crawler. Beide Anwendungen können nicht mehr per EWS auf Exchange Online zugreifen. Stattdessen ist ein Wechsel auf die Microsoft Graph-Schnittstelle notwendig.

Sie können die Verbindung zum Microsoft Exchange-Server festlegen und mehrere unterschiedliche Exchange-Server mit der Groupware-App verbinden.

Beachten Sie für die Verbindung mit Microsoft Exchange Server, dass das SSL-Zertifikat qualifiziert und gültig ist.

Folgende Bedingungen gelten für den Benutzer für den Identitätswechsel:

- Für Exchange Online in Microsoft 365: Der Benutzer benötigt ein Postfach (EWS und OAuth 2.0).
- Microsoft Exchange-Server (on-premises): Der Benutzer benötigt ein Postfach (EWS und Basic), wenn auf öffentliche Ordner zugegriffen wird.
- Geben Sie als Benutzernamen die SMTP-Adresse an, um den Zugriff auf öffentliche Ordner zu gewährleisten.

Sie können als weitere Microsoft Exchange-Verbindung zwischen Microsoft Exchange (on-premises) und Exchange Online auswählen. Für Microsoft Exchange (on-premises) ist nur Microsoft EWS zulässig. Exchange Online kann Microsoft EWS oder Microsoft Graph nutzen.

Wenn Sie eine Microsoft Exchange-Konfiguration löschen möchten, stellen Sie sicher, dass die Konfiguration nicht mehr verwendet wird.

Angenommen, Sie möchten die Verbindungseinstellungen für Exchange Online festlegen und als zusätzliche Verbindung Microsoft EWS verwenden.

### So geht's

1. Öffnen Sie das Feature **Konfiguration** auf der Startseite und navigieren Sie in der Kategorie **Dokumentenmanagement** zu **E-Mails**.
2. Wählen Sie unter **E-Mail-Verwaltung** den Eintrag **Microsoft Exchange** aus.
3. Wechseln Sie in die Perspektive **Verbindungseinstellungen**.
4. Wählen Sie **Microsoft Exchange Dienste aktivieren** aus.
5. Geben Sie alle notwendigen Parameter für die erste Verbindung ein.
6. Klicken Sie auf das Plusymbol, um die Parameter als eine zusätzliche Verbindung hinzuzufügen.
7. Geben Sie die akzeptierten Domänen des Microsoft Exchange-Servers an. Trennen Sie die Domänen durch ein Komma.
8. Wählen Sie unter **Exchange-API** als Schnittstelle **Microsoft EWS** aus.
9. Klicken Sie unter **Exchange-Webdienste-Server** auf **Microsoft 365**. Dadurch trägt das System outlook.office365.com ein.
10. Tragen Sie den Exchange-Webdienste-Port und die entsprechende Version unter **Exchange Web Service-Version** fest. Der Standardwert ist **Autodetect**.
11. Legen Sie die Authentifizierungsmethode für die Exchange-Webdienste fest. Bei **OAuth 2.0 (Microsoft 365)** tragen Sie die Microsoft 365 Verzeichnis-ID, Microsoft 365 Anwendungs-ID für d.ecs groupware, den Microsoft 365 API-Zugriffsschlüssel für Exchange-Webdienste und den Benutzer für den Identitätswechsel in Exchange-Webdienste aus Azure Active Directory ein. Bei **Basic** geben Sie den Benutzernamen für den Identitätswechsel und das Kennwort ein.

Siehe auch:

- [Festlegen von mehreren Verbindungen zum Microsoft Exchange-Server mit Microsoft Exchange \(on-premises\)](#)
- [Festlegen von mehreren Verbindungen zum Microsoft Exchange-Server mit Exchange Online und Microsoft Graph](#)

### 1.3.6. Festlegen von mehreren Verbindungen zum Microsoft Exchange-Server mit Exchange Online und Microsoft Graph

#### Warnung

Microsoft deaktiviert zum 01.10.2026 die Exchange-Webdienste (EWS) für alle externen Anwendungen in Exchange Online. Diese Deaktivierung hat auch Auswirkungen auf die d.velop-Komponenten d.ecs groupware und d.ecs content crawler. Beide Anwendungen können nicht mehr per EWS auf Exchange Online zugreifen. Stattdessen ist ein Wechsel auf die Microsoft Graph-Schnittstelle notwendig.

Sie können die Verbindung zum Microsoft Exchange-Server festlegen und mehrere unterschiedliche Exchange-Server mit der Groupware-App verbinden.

Beachten Sie für die Verbindung mit Microsoft Exchange Server, dass das SSL-Zertifikat qualifiziert und gültig ist.

Folgende Bedingungen gelten für den Benutzer für den Identitätswechsel:

- Für Exchange Online in Microsoft 365: Der Benutzer benötigt ein Postfach (EWS und OAuth 2.0).
- Microsoft Exchange-Server (on-premises): Der Benutzer benötigt ein Postfach (EWS und Basic), wenn auf öffentliche Ordner zugegriffen wird.
- Geben Sie als Benutzernamen die SMTP-Adresse an, um den Zugriff auf öffentliche Ordner zu gewährleisten.

Sie können als weitere Microsoft Exchange-Verbindung zwischen Microsoft Exchange (on-premises) und Exchange Online auswählen. Für Microsoft Exchange (on-premises) ist nur Microsoft EWS zulässig. Exchange Online kann Microsoft EWS oder Microsoft Graph nutzen.

Wenn Sie eine Microsoft Exchange-Konfiguration löschen möchten, stellen Sie sicher, dass die Konfiguration nicht mehr verwendet wird.

Angenommen, Sie möchten die Verbindungseinstellungen für Exchange Online festlegen und als zusätzliche Verbindung Microsoft Graph verwenden.

#### So geht's

1. Öffnen Sie das Feature **Konfiguration** auf der Startseite und navigieren Sie in der Kategorie **Dokumentenmanagement** zu **E-Mails**.
2. Wählen Sie unter **E-Mail-Verwaltung** den Eintrag **Microsoft Exchange** aus.
3. Wechseln Sie in die Perspektive **Verbindungseinstellungen**.
4. Wählen Sie **Microsoft Exchange Dienste aktivieren** aus.
5. Geben Sie alle notwendigen Parameter für die erste Verbindung ein.
6. Klicken Sie auf das Plusymbol, um die Parameter als eine zusätzliche Verbindung hinzuzufügen.
7. Geben Sie die akzeptierten Domänen des Microsoft Exchange-Servers an. Trennen Sie die Domänen durch ein Komma.
8. Wählen Sie unter **Exchange-API** als Schnittstelle **Microsoft Graph** aus.
9. Tragen Sie die Microsoft 365 Verzeichnis-ID, Microsoft 365 Anwendungs-ID für d.ecs groupware, den Microsoft 365 API-Zugriffsschlüssel aus Azure Active Directory ein. Die Exchange-Verbindung wird unter outlook.office365.com (akzeptierte Domänen) eingetragen.

Siehe auch:

- [Festlegen von mehreren Verbindungen zum Microsoft Exchange-Server mit Microsoft Exchange \(on-premises\)](#)
- [Festlegen von mehreren Verbindungen zum Microsoft Exchange-Server mit Exchange Online und Microsoft EWS](#)

### 1.3.7. Herstellen einer Verbindung zwischen d.3one-Anwendungsserver und d.ecs domino

Damit d.3one in IBM Notes ordnungsgemäß funktioniert, müssen Sie die Kommunikation zwischen dem HCL Domino-Server, den Client-PCs mit HCL Notes und dem d.3one-Anwendungsserver sicherstellen. Sie legen auf dem HCL Domino-Server, auf dem d.ecs domino installiert ist, die Verbindungsdaten fest. Zum Festlegen der Verbindungsdaten müssen Sie mit einem Windows-Administratorkonto angemeldet sein.

Angenommen, Sie möchten für die Kommunikation zwischen den Servern die Verbindungsdaten auf dem HCL Domino-Server festlegen.

#### So geht's

1. Öffnen Sie im Datenverzeichnis die Datenbank **d3onecfg.nsf** mit HCL Notes oder einem Browser und navigieren Sie zu **Settings**. Stellen Sie sicher, dass die Datei **d3onecfg.nsf** im Hauptverzeichnis der Datenbanken gespeichert ist. Die Datei darf nicht in einem Unterverzeichnis gespeichert sein.
2. Geben Sie auf der Registerkarte **d.3one Server** den Hostnamen des Servers an, auf dem d.3one installiert ist (Basisadresse). Sie müssen den vollqualifizierten Domännennamen (FQDN) des d.3one-Servers angeben, damit die Kerberos-Authentifizierung in der Windows-Domäne ordnungsgemäß funktioniert, z.B. **d.3one.contoso.com**.
3. Geben Sie den Port für den d.3one-Anwendungsserver an.
4. Wechseln Sie zur Registerkarte **d.ecs domino** und wählen Sie unter **Log level** die Protokollebene von d.ecs domino aus.
5. Geben Sie unter **Log path** den Pfad zur Protokolldatei an.
6. Geben Sie unter **Log file** den Dateinamen der Protokolldatei an.
7. Geben Sie unter **Work path** den Dateipfad an, in dem die temporären Dateien von d.ecs domino gespeichert werden (z.B. zum Konvertieren von E-Mails). Wenn Sie keinen Pfad angeben, wird der Systemordner **Temp** verwendet.
8. Geben Sie unter **SSL Port** den Port für d.ecs domino für die verschlüsselte Verbindung an. Standardmäßig ist der Port **8182**.
9. Wechseln Sie zur Registerkarte **Certificate** und geben Sie unter **Keystore file path** den Dateipfad vom Java-Keystore an. Der Java-Keystore speichert den zu verwendenden Schlüssel für die sichere Verbindung.
10. Geben Sie unter **Keystore password** das Passwort für den Java-Keystore an.
11. Geben Sie bei Bedarf unter **Key password** das Passwort für den im Java-Keystore gespeicherten Schlüssel an.

Wenn Ihre Anwender ihre Maildatenbanken von unterschiedlichen Servern abrufen, müssen Sie eventuell die Datenbank auf den Mailservern replizieren, damit Ihre Einstellungen für d.3one auf dem Server auch für die Client-PCs mit HCL Notes verwendet werden können.

Nachdem Sie die Verbindungsdaten festgelegt haben, müssen Sie die Verbindungsdaten ebenfalls in d.3one festlegen.

### 1.3.8. Festlegen der d.ecs domino-Verbindungsdaten in d.3one

Wenn Sie die Verbindungsdaten für d.ecs domino auf dem HCL Domino-Server festgelegt haben, müssen Sie für die Verbindung zwischen d.3one-Server und d.ecs domino die Verbindungsdaten ebenfalls in d.3one festlegen.

#### So geht's

1. Öffnen Sie das Feature **Konfiguration** auf der Startseite und navigieren Sie in der Kategorie **Dokumentenmanagement** zu **E-Mails**.
2. Wählen Sie unter **E-Mail-Verwaltung** den Eintrag **IBM Domino** aus.
3. Wählen Sie **IBM Domino Dienste aktivieren** aus.

4. Geben Sie unter **d.ecs domino service-Server** den Hostnamen des Client-PCs an, auf dem d.ecs domino installiert ist.
5. Geben Sie unter **d.ecs domino service-Port** den Port für d.ecs domino an. Standardmäßig ist der Port **8182**.
6. Speichern Sie Ihre Angaben und starten Sie die Groupware-App neu.

### 1.3.9. Festlegen der allgemeinen Einstellungen von d.ecs content crawler

Nachdem Sie d.ecs content crawler installiert haben, müssen Sie d.ecs content crawler konfigurieren. Sie können d.ecs content crawler für die regelbasierte Verarbeitung von E-Mails oder die Journalarchivierung konfigurieren. Darüber hinaus können Sie die Verarbeitungsgeschwindigkeit anpassen.

#### Warnung

Wir empfehlen, d.link for lotus notes nicht parallel zu d.ecs content crawler zu verwenden, um eventuelle Probleme im Postfach zu vermeiden.

Die allgemeinen Einstellungen von d.ecs. content crawler finden Sie im Feature **Konfiguration** auf der Startseite in der Kategorie **Dokumentenmanagement** unter **E-Mails**, indem Sie unter **E-Mail-Archivierung** den Eintrag **Archivierungsoptionen** auswählen. Alternativ können Sie das Feature **d.ecs content crawler** verwenden.

In den allgemeinen Einstellungen können Sie z.B. die maximale Anzahl von gleichzeitig zu verarbeitenden Profilen festlegen. Standardmäßig werden bereits Werte vorgegeben. Sie können bei Bedarf die Werte individuell anpassen.

#### Anmerkung

Wenn Sie die Microsoft Graph-Schnittstelle verwenden, halbieren Sie die maximale Anzahl der gleichzeitig zu verarbeitenden Profile und die Instanzen pro Profil. Microsoft hat für die Microsoft Graph-Schnittstelle eine strikte Einschränkungsrichtlinie (Throttling Policy) definiert, die nicht verändert werden kann.

Wenn Sie die allgemeinen Einstellungen für d.ecs content crawler abgeschlossen haben, starten Sie d.ecs content crawler in d.3 process manager neu.

Wenn Microsoft Exchange Server oder HCL Domino Server eine gewisse Zeit nicht erreichbar sind, z.B. wegen eines Wartungsfensters für Updates oder zur Datensicherung, starten Sie d.ecs content crawler in d.3 process manager neu, sobald der Mailserver wieder erreichbar ist.

### 1.3.10. Konfigurieren des Datenbankservers

d.ecs content crawler erstellt für jede zu verarbeitende E-Mail einen Job, der alle notwendigen Informationen enthält. Zum Verwalten der Jobs müssen Sie eine Datenbank festlegen.

Die Datenbanktabellen werden mit dem Präfix **GWCR\_** erstellt. Sie können für d.ecs content crawler die Datenbank eines d.3-Repositorys verwenden.

#### Anmerkung

Wenn Sie eine interne Datenbank verwenden möchten, können Sie d.ecs content crawler nicht mehr verteilt installieren. Es darf nur eine Instanz bei d.ecs http gateway registriert sein und ausgeführt werden.

Angenommen, Sie möchten zum Verwalten von Jobs einen Datenbankserver konfigurieren.

#### So geht's

1. Öffnen Sie das Feature **Konfiguration** auf der Startseite und navigieren Sie in der Kategorie **Dokumentenmanagement** zu **E-Mails**.

2. Wählen Sie unter **E-Mail-Archivierung** den Eintrag **Archivierungsoptionen** aus.
3. Wechseln Sie in die Perspektive **Datenbank**.
4. Wählen Sie den entsprechenden Datenbanktyp aus.
5. Geben Sie unter **Server** den entsprechenden Hostnamen oder die IP-Adresse des Datenbanksservers an.
6. Geben Sie den Namen der Datenbank an, die Sie verwenden möchten.
7. Geben Sie den Namen des Datenbankbenutzers an.
8. Geben Sie das Passwort des Benutzers an und speichern Sie Ihre Angaben.

### 1.3.11. Konfigurieren einer Journalarchivierung

Mit d.ecs content crawler steht Ihnen die Möglichkeit zur Journalarchivierung von bestimmten Elementen mit Microsoft Exchange und HCL Domino zur Verfügung. Sie können z.B. Journal-E-Mails oder auch Besprechungsanfragen mit der Journalarchivierung speichern. Davon ausgenommen sind z.B. Termine, wenn Sie in der Groupware-App die Option **Ablageformat EML anstatt DGIX** aktiviert haben. Sie finden die Option im Feature **Konfiguration** in der Kategorie **Dokumentenmanagement** unter **E-Mails**, wenn Sie unter **E-Mail-Verwaltung** den Eintrag **Microsoft Exchange** auswählen und in die Perspektive **Verarbeitungseinstellungen** wechseln.

Darüber hinaus können Sie die Compliance-Archivierung ohne aktiviertes Journaling für Microsoft Exchange 2016 und Microsoft Exchange Online verwenden.

Für das rechtssichere und revisionskonforme Speichern von E-Mails aus dem Journal Ihres E-Mail-Systems können Sie `db | journal archiver` verwenden anstatt `d.ecs content crawler` insgesamt zu lizenzieren. Um die Journalarchivierung verwenden und konfigurieren zu können, müssen Sie `db | journal archiver` oder `db | mailbox archiver` für Ihr E-Mail-System lizenziert haben.

### Festlegen der allgemeinen Einstellungen für die Journalarchivierung

Mit d.ecs content crawler können Sie das Journaling für Microsoft Exchange oder HCL Domino aktivieren.

Angenommen, Sie möchten die Journalarchivierung für Microsoft Exchange verwenden.

#### So geht's

1. Öffnen Sie das Feature **Konfiguration** auf der Startseite und navigieren Sie in der Kategorie **Dokumentenmanagement** zu **E-Mails**.
2. Wählen Sie unter **E-Mail-Archivierung** den Eintrag **Archivierungsoptionen** aus.
3. Wechseln Sie in die Perspektive **Verarbeitungseinstellungen**.
4. Aktivieren Sie das Journaling für Microsoft Exchange.
5. Wählen Sie das Repository aus, in das die Journal-E-Mails gespeichert werden sollen.
6. Geben Sie unter **Journalpostfach** die SMTP-Adresse des Postfachs an, in dem die Journal-E-Mails gespeichert werden, z.B. `journal@<Domänenname>.com`. Wenn Sie mehrere Postfächer angeben möchten, trennen Sie die Einträge mit einem Komma.
7. Wählen Sie für die Zeitsteuerung die Tage und die Laufzeit aus.
8. Speichern Sie Ihre Angaben.

Wenn Sie die Konfiguration für die Journalarchivierung ändern, starten Sie im Anschluss den Dienst `d.ecs content crawler` neu.

### Konfigurieren der Compliance-Archivierung ohne aktiviertes Journaling für Microsoft Exchange 2016 und Microsoft Exchange Online

Das Compliance-Archivieren wird nur im Zusammenhang mit Microsoft Exchange 2016 und Microsoft Exchange Online unterstützt. Wenn Sie eine frühere Version von Microsoft Exchange Server verwenden, werden Ihre Konfigurationen ignoriert.

Wenn Sie die Compliance-Archivierung ohne aktiviertes Journaling verwenden möchten, müssen Sie Folgendes beachten:

- Sie müssen in Microsoft Exchange Server das Beweissicherungsverfahren aktivieren. Wenn Sie das Beweissicherungsverfahren aktivieren, wird bei jeder Veränderung eines Elements eine Kopie im Ordner **Versions** erstellt. Stellen Sie sicher, dass der Ordner nicht unnötig mit Kopien befüllt wird.

### Warnung

d.ecs content crawler prüft nicht, ob das Beweissicherungsverfahren in Microsoft Exchange aktiviert ist. Wenn das Beweissicherungsverfahren deaktiviert ist, werden die Elemente nach einer festgelegten Zeit automatisch von Microsoft Exchange Server gelöscht oder der Benutzer dieses Elements wird dauerhaft gelöscht.

Weitere Informationen finden Sie auf der Microsoft Docs-Website in der Exchange Server 2019-Dokumentation unter "Ordner 'erneut herstellbare Elemente' in Exchange Server".

- Sie müssen die Einstellungen für ein Profil in d.ecs content crawler anpassen. Geben Sie als Quellsystem **Microsoft Exchange** an und wählen Sie die Option **Archivieren von gelöschten Elementen aktivieren** aus. In diesem Fall werden auch E-Mails berücksichtigt, die unter **Wiederherstellbare Elemente** in den Ordnern **Löschvorgänge (Deletions)** oder **Endgültige Löschvorgänge (Purges)** gespeichert sind. Die Elemente aus den entsprechenden Ordnern werden basierend auf Ihren Konfigurationen des Profils verarbeitet.
- Die Elemente werden nicht automatisch von d.ecs content crawler gelöscht. Das automatische Löschen müssen Sie bei Bedarf im Profil festlegen.

Wenn Sie die Konfiguration für die Journalarchivierung ändern, starten Sie im Anschluss den Dienst d.ecs content crawler neu.

## Konfigurieren der Journalarchivierung für HCL Domino

Bei der Journalarchivierung für HCL Domino müssen Sie Folgendes beachten:

- Der Archivierungsservice kann maximal eine Journaldatenbank bearbeiten. Wenn Sie mehr als eine Journaldatenbank verarbeiten möchten, müssen Sie mehrere d.ecs content crawler-Apps bzw. mehrere Groupware-Apps (d.3one-Anwendungsserver) installieren.
- Stellen Sie sicher, dass in der Administration von HCL Domino Server im Feld **Form** eine der folgenden Kategorien (Dokumentarten) angegeben ist: **Message, Memo, Reply, Notice, Appointment, Report, NonDelivery Report, Recall Response, Recall Request, Return Receipt** oder **Personal Stationery**. Nur solche Kategorien dürfen an die Journaldatenbank übermittelt werden.
- Um die Eigenschaften von E-Mails den d.3-Eigenschaften zuordnen zu können, müssen Sie eine Zuordnung erstellen. Wir empfehlen, eine separate Kategorie für Journal-E-Mails zu verwenden, da sonst dieselbe Zuordnung zum Speichern von E-Mails in HCL Notes auch in d.3one verwendet wird.

## Konfigurieren der Journalarchivierung für Microsoft Exchange

Bei der Journalarchivierung für Microsoft Exchange müssen Sie Folgendes beachten:

- Die Journalarchivierung kann auch Dokumente archivieren, die direkt zugestellt werden und keinen Umschlag haben. Wir empfehlen, das Journaling für Microsoft Exchange so zu konfigurieren, dass nur E-Mails von Microsoft Exchange akzeptiert werden (Microsoft Exchange PowerShell Commandlet **Set-Mailbox** in Verbindung mit **AcceptMessagesOnlyFromSendersOrMembers**).
- Innerhalb des Journals werden nur E-Mails mit den Nachrichtenklassen **IPM.Note\***, **IPM.Schedule.Meeting\***, **IPM.Report.Recall\***, **IPM.Outlook.Recall\*** und **REPORT.IPM\*** verarbeitet. E-Mails, die von diesen Vorgaben abweichen, werden in den Ordner **d.3ecm unprocessable** des Journalpostfachs verschoben.
- Um die Eigenschaften von E-Mails den d.3-Eigenschaften zuordnen zu können, müssen Sie eine Zuordnung erstellen. Bei einer Zuordnung werden die Werte nicht aus der Umschlagsmail ermittelt, sondern

aus dem zu speichernden Dokument. Wir empfehlen, eine separate Kategorie (Dokumentart) für Journal-E-Mails zu verwenden, da sonst dieselbe Zuordnung zum Speichern von E-Mails in Microsoft Outlook auch in d.3one verwendet wird.

Microsoft Office 365 (Microsoft Exchange Online) unterstützt derzeit nur externe Postfächer als Journalpostfach. Externe Postfächer sind Postfächer, die keine Microsoft Office 365-Postfächer sind. Für die Journalarchivierung mit d.ecs content crawler muss das externe Postfach mithilfe der Exchange-Webdienste (EWS) erreichbar sein. Es spielt keine Rolle, ob es sich um ein Cloud-Postfach oder On-Premises-Postfach handelt.

## Speichern von Besprechungsanfragen

Sie können aus dem Journaling zusätzlich zu E-Mails auch andere Elemente speichern. Für diese Elemente können Sie bei der Zuordnung die Quelle **Kalendereintrag/Besprechung** auswählen.

Folgende Elemente können Sie zusätzlich zu E-Mails speichern:

- Besprechungsanfragen
- Antworten auf Besprechungsanfragen (**Zusage, Absage, Unter Vorbehalt**)
- Absagen von Besprechungen

Folgende Werte können zusätzlich übernommen werden:

- Alle SMTP-Adressen (Teilnehmer, Organisator) oder alle Teilnehmernamen
- Startzeitpunkt und Endzeitpunkt
- Name des Organisators
- Namen der erforderlichen Teilnehmer, optionalen Teilnehmer, Räume oder Ressourcen
- Ort
- SMTP-Adresse des Organisators
- SMTP-Adressen der erforderlichen oder optionalen Teilnehmer, Räume oder Ressourcen
- SMTP-Adressen aller Teilnehmer

### 1.3.12. Konfigurieren einer regelbasierten Archivierung

Sie können mit d.ecs content crawler E-Mails regelbasiert archivieren, indem Sie Profile erstellen. In den Profilen geben Sie Quellen, Regeln und Verarbeitungsschritte an, um festzulegen, wie die Elemente verarbeitet werden sollen.

Sie können Quellen, Regeln und Verarbeitungsschritte auch direkt beim Profilerstellen mithilfe der entsprechenden Kontextaktionen konfigurieren, ohne die Konfiguration des Profils verlassen zu müssen.

Wenn Sie ein Profil zum regelbasierten Archivieren erstellen möchten, müssen Sie eine Kategorie erstellen und für diese Kategorie eine Zuordnung definieren. Sie können die Kategorie und die Zuordnung vor dem Profilerstellen in der Konfiguration der Groupware-App und dem Feature **Zuordnungen** erstellen. Alternativ können Sie beim Erstellen einer Verarbeitungsschrittsammlung mithilfe der entsprechenden Kontextaktionen in die Konfiguration wechseln, ohne die Konfiguration der Verarbeitungsschritte verlassen zu müssen.

## Aktivieren der regelbasierten Archivierung

Um E-Mails regelbasiert zu archivieren, müssen Sie die Option in d.ecs content crawler aktivieren.

### So geht's

1. Öffnen Sie das Feature **Konfiguration** auf der Startseite und navigieren Sie in der Kategorie **Dokumentenmanagement** zu **E-Mails**.
2. Wählen Sie unter **E-Mail-Archivierung** den Eintrag **Archivierungsoptionen** aus.
3. Wechseln Sie in die Perspektive **Verarbeitungseinstellungen**.
4. Aktivieren Sie die Option für die regelbasierte Verarbeitung und speichern Sie Ihre Angaben.

## Erstellen eigener Quellen für Zuordnungen

Standardmäßig stehen Ihnen mit den Integrationen und d.ecs content crawler bereits konfigurierte Standardquellen zum Erstellen von Zuordnungen zur Verfügung. Sie können aber auch eigene Quellen mit zusätzlichen benutzerdefinierten Feldern definieren.

Für die Journalarchivierung müssen Sie keine Quellen definieren, da Sie die entsprechende Standardquelle verwenden können.

### Anmerkung

Wenn eine Quelle für eine Konfiguration verwendet wird, können Sie die Quelle nicht mehr ändern oder löschen.

Angenommen, Sie möchten für eine Zuordnung eine eigene Quelle definieren.

### So geht's

1. Öffnen Sie das Feature **Konfiguration** auf der Startseite und navigieren Sie in der Kategorie **Dokumentenmanagement** zu **E-Mails**.
2. Wählen Sie unter **E-Mail-Verwaltung** den Eintrag **Quellen** aus.
3. Wählen Sie in der Übersicht der Quellen die Kontextaktion **Neue Quelle erstellen** aus.
4. Geben Sie einen eindeutigen Namen für die Quelle an.
5. Wählen Sie eine Basisquelle aus, aus der die Quelle grundlegende Informationen beziehen soll.
6. Wählen Sie bei Bedarf **Benutzerdefiniertes Feld bearbeiten oder hinzufügen** aus, um zusätzliche benutzerdefinierte Felder für die Quelle zu definieren.
7. Geben Sie den Namen des benutzerdefinierten Feldes so an, wie der Name im Quellsystem vorkommt.
8. Geben Sie einen Anzeigenamen für das benutzerdefinierte Feld an.
9. Wählen Sie unter **Typ** einen Dateityp für das benutzerdefinierte Feld aus.
10. Klicken Sie auf **Hinzufügen**.

Im Anschluss können Sie bei Bedarf benutzerdefinierte Felder hinzufügen, bearbeiten, entfernen oder Sie speichern Ihre Angaben, um die Quelle für eine Zuordnung zu verwenden.

Siehe auch:

- [Detailinformationen zu Quellen](#)
- [Detailinformationen zu Kategorien](#)
- [Detailinformationen zu Zuordnungen](#)

## Erstellen eigener Kategorien für eine Zuordnung

Um eine Zuordnung zu erstellen, müssen Sie mindestens eine Kategorie definieren.

Für die Journalarchivierung müssen Sie keine Kategorien definieren, da Sie die entsprechende Standardkategorie verwenden können.

### Anmerkung

Wenn eine Kategorie für eine Konfiguration verwendet wird, dürfen Sie die Kategorie nicht löschen.

Angenommen, Sie möchten für eine Zuordnung eine eigene Kategorie definieren.

### So geht's

1. Öffnen Sie das Feature **Konfiguration** auf der Startseite und navigieren Sie in der Kategorie **Dokumentenmanagement** zu **E-Mails**.

2. Wählen Sie unter **E-Mail-Verwaltung** den Eintrag **Kategorien** aus.
3. Wählen Sie in der Übersicht der Kategorien die Kontextaktion **Neue Kategorie erstellen** aus.
4. Geben Sie einen eindeutigen Namen für die Kategorie an und speichern Sie Ihre Angaben.

Siehe auch:

- [Detailinformationen zu Kategorien](#)
- [Detailinformationen zu Quellen](#)
- [Detailinformationen zu Zuordnungen](#)

## Erstellen eines Profils

Um z.B. E-Mails aus Ihren Postfächern regelbasiert zu archivieren, benötigen Sie ein Profil. Bevor Sie ein Profil erstellen können, benötigen Sie mindestens Folgendes:

- Eine konfigurierte Verbindung zum Quellsystem (Microsoft Exchange oder HCL Domino)
- Eine Zuordnung mit einer Quelle und einer Kategorie

Alle weiteren notwendigen Komponenten des Profils (Quellensammlung, Regelsammlung, Verarbeitungsschrittsammlung) können Sie ebenfalls vorab oder direkt aus den Profileinstellungen heraus erstellen.

Angenommen, Sie möchten ein Profil erstellen.

### So geht's

1. Öffnen Sie das Feature **Konfiguration** auf der Startseite und navigieren Sie in der Kategorie **Dokumentenmanagement** zu **E-Mails**.
2. Wählen Sie unter **E-Mail-Archivierung** den Eintrag **Profile** aus.
3. Klicken Sie auf das Plus-Symbol, um ein neues Profil hinzuzufügen.
4. Geben Sie einen eindeutigen Namen und eine Beschreibung für das Profil an.
5. Legen Sie unter **Quellsystem** fest, welches E-Mail-System das Profil verarbeiten soll, z.B. **Microsoft Exchange**.
6. Wählen Sie eine entsprechende Microsoft Exchange-Verbindung aus, wenn Sie unter **Quellsystem** den Eintrag **Microsoft Exchange** ausgewählt haben.

### Anmerkung

Sie können auch mehrere konfigurierte Microsoft Exchange-Server eintragen. Damit lassen sich mit demselben Profil Postfächer verarbeiten, die teilweise in Microsoft Exchange On-Premises und in Exchange Online konfiguriert sind (Hybrid-Szenario).

Weitere Informationen hierzu erhalten Sie in den folgenden Kapiteln:

- [Festlegen von mehreren Verbindungen zum Microsoft Exchange-Server mit Microsoft Exchange \(on-premises\)](#)
  - [Festlegen von mehreren Verbindungen zum Microsoft Exchange-Server mit Exchange Online und Microsoft EWS](#)
  - [Festlegen von mehreren Verbindungen zum Microsoft Exchange-Server mit Exchange Online und Microsoft Graph](#)
7. Wählen Sie eine Quellensammlung für das Profil aus. Alternativ können Sie mit **Quellensammlung erstellen** eine neue Quellensammlung hinzufügen.
  8. Wählen Sie eine Regelsammlung für das Profil aus. Alternativ können Sie mit **Regelsammlung erstellen** eine neue Quellensammlung hinzufügen.
  9. Wählen Sie eine Verarbeitungsschrittsammlung für das Profil aus. Alternativ können Sie mit **Verarbeitungsschrittsammlung erstellen** eine neue Quellensammlung hinzufügen.
  10. Wählen Sie aus, ob es sich um ein priorisiertes Profil handelt.
  11. Wählen Sie für die Zeitsteuerung des Profils die Tage und die Laufzeiten aus.

12. Speichern Sie Ihre Angaben.

Siehe auch:

- [Detailinformationen zu Profilen](#)
- [Detailinformationen zu Zuordnungen](#)
- [Erstellen eigener Quellen für Zuordnungen](#)
- [Erstellen eigener Kategorien für eine Zuordnung](#)
- [Erstellen einer Quellensammlung](#)
- [Erstellen einer Regelsammlung](#)
- [Erstellen einer Verarbeitungsschrittsammlung](#)
- [Konfigurieren des Datenbankservers](#)
- [Festlegen der allgemeinen Einstellungen von d.ecs content crawler](#)

## Erstellen einer Quellensammlung

Zum Erstellen eines Profils benötigen Sie eine Quellensammlung.

Angenommen, Sie möchten eine neue Quellensammlung erstellen.

So geht's

1. Öffnen Sie das Feature **Konfiguration** auf der Startseite und navigieren Sie in der Kategorie **Dokumentenmanagement** zu **E-Mails**.
2. Wählen Sie unter **E-Mail-Archivierung** den Eintrag **Quellen** aus.
3. Klicken Sie auf das Plusymbol, um eine neue Quellensammlung hinzuzufügen.
4. Geben Sie einen eindeutigen Namen und eine Beschreibung für die Quellensammlung an.
5. Fügen Sie eine Quelle hinzu, z.B. den Typ **Benutzer**.
6. Geben Sie einen Namen für die Quelle an, z.B. **Administrator**.
7. Klicken Sie auf **Hinzufügen**.
8. Fügen Sie bei Bedarf weitere Quellen hinzu und speichern Sie Ihre Angaben.

Im Anschluss steht Ihnen die neue Quellensammlung zum Profilerstellen zur Verfügung.

Siehe auch: [Detailinformationen zu Quellensammlungen](#)

## Erstellen einer Regelsammlung

Zum Erstellen eines Profils benötigen Sie eine Regelsammlung.

### Anmerkung

Zur Verarbeitung von E-Mails müssen Sie mindestens die Regel **Nicht archivierte Dokumente** oder **Archivierte Dokumente** konfigurieren.

Angenommen, Sie möchten eine neue Regelsammlung erstellen.

So geht's

1. Öffnen Sie das Feature **Konfiguration** auf der Startseite und navigieren Sie in der Kategorie **Dokumentenmanagement** zu **E-Mails**.
2. Wählen Sie unter **E-Mail-Archivierung** den Eintrag **Regeln** aus.
3. Klicken Sie auf das Plusymbol, um eine neue Regelsammlung hinzuzufügen.
4. Wählen Sie die Kontextaktion zum Hinzufügen einer neuen Regelsammlung aus.
5. Geben Sie einen eindeutigen Namen und eine Beschreibung für die Regelsammlung an.
6. Fügen Sie eine Regel hinzu, z.B. **Archivierte Dokumente**.
7. Klicken Sie auf **Hinzufügen**.
8. Fügen Sie bei Bedarf weitere Regeln hinzu und speichern Sie Ihre Angaben.

Im Anschluss steht Ihnen die neue Regelsammlung zum Profilerstellen zur Verfügung.

Siehe auch: [Detailinformationen zu Regelsammlungen](#)

## Erstellen einer Verarbeitungsschrittsammlung

Zum Erstellen von Profilen benötigen Sie eine Verarbeitungsschrittsammlung.

Angenommen, Sie möchten für eine neue Verarbeitungsschrittsammlung den Verarbeitungsschritt **Dokument archivieren** hinzufügen.

### So geht's

1. Öffnen Sie das Feature **Konfiguration** auf der Startseite und navigieren Sie in der Kategorie **Dokumentenmanagement** zu **E-Mails**.
2. Wählen Sie unter **E-Mail-Archivierung** den Eintrag **Verarbeitungsschritte** aus.
3. Klicken Sie auf das Plus-Symbol, um eine neue Verarbeitungsschrittsammlung hinzuzufügen.
4. Geben Sie einen eindeutigen Namen und eine Beschreibung für die Verarbeitungsschrittsammlung an.
5. Fügen Sie den Verarbeitungsschritt **Dokument archivieren** hinzu.
6. Wählen Sie ein Repository aus.
7. Wählen Sie eine Quelle aus.
8. Wählen Sie eine Kategorie aus.
9. Fügen Sie bei Bedarf eine Nachbearbeitungsaktion hinzu, um z.B. festzulegen, dass Anhänge verknüpft werden sollen.
10. Wählen Sie bei Bedarf eine profilbezogene Dublettenprüfung aus.
11. Aktivieren Sie bei Bedarf **dfs | case manager-Daten verarbeiten**.
12. Klicken Sie auf **Hinzufügen**.
13. Fügen Sie bei Bedarf weitere Verarbeitungsschritte hinzu und speichern Sie Ihre Angaben.

Im Anschluss steht Ihnen die neue Verarbeitungsschrittsammlung zum Profilerstellen zur Verfügung.

Siehe auch: [Detailinformationen zu Verarbeitungsschrittsammlungen](#)

### 1.3.13. Konfigurieren eines Servicebenutzers

Damit Sie mit d.ecs content crawler arbeiten können, benötigen Sie einen Servicebenutzer. Mit diesem Benutzer werden z.B. die Dokumente im d.3-Repository gespeichert.

Der Servicebenutzer muss folgenden Voraussetzungen erfüllen:

- Der Benutzer muss der administrativen Gruppe zugeordnet sein, die Sie in d.ecs identity provider als administrative Gruppe festgelegt haben.
- Der Benutzer muss in der Administration von d.3 Rechte zum Lesen von Dokumenten im Status **Lesen Bearbeitung**, **Lesen Prüfung** oder **Lesen Freigabe** haben.
- Der Benutzer muss in der Administration von d.3 das Recht zum Importieren eines Dokuments haben.

### 1.3.14. Konfigurieren von Error-Jobs

Durch externe Abhängigkeiten können z.B. Netzwerkausfälle auftreten. Um den ordnungsgemäßen Betrieb sicherzustellen, werden für alle Aktionen von d.ecs content crawler Error-Jobs erstellt. Bei Fehlern erhalten die Jobs einen entsprechenden Status.

Sie können festlegen, wie Error-Jobs verarbeitet werden. Sie können z.B. festlegen, wie oft Error-Jobs neu gestartet werden sollen, um manuell nach der Fehlerursache zu suchen und die Jobs manuell neu zu starten. Darüber hinaus können Sie ein Intervall für den Neustart der Error-Jobs bestimmen. Sie können die Optionen für die maximale Anzahl von Neustarts und das Intervall kombinieren.

Angenommen, Sie möchten festlegen, dass Error-Jobs maximal siebenmal neu gestartet werden. Außerdem möchten Sie einen bestimmten Tag und eine bestimmte Uhrzeit festlegen, wann Error-Jobs neu gestartet werden sollen.

#### So geht's

1. Öffnen Sie das Feature **Konfiguration** auf der Startseite und navigieren Sie in der Kategorie **Dokumentenmanagement** zu **E-Mails**.
2. Wählen Sie unter **E-Mail-Archivierung** den Eintrag **Archivierungsoptionen** aus.
3. Wechseln Sie in die Perspektive **Fehlerbehandlung**.
4. Aktivieren Sie die Option für den automatischen Neustart von Error-Jobs.
5. Geben Sie für die maximale Anzahl von Neustarts den Wert **7** an.
6. Aktivieren Sie **Error-Jobs bei Neustart des Dienstes zurücksetzen**.
7. Wählen Sie den entsprechenden Tag aus.
8. Klicken Sie auf **Uhrzeit hinzufügen**.
9. Geben Sie den entsprechenden Wert an.
10. Klicken Sie auf **Hinzufügen** und speichern Sie Ihre Angaben.

### 1.3.15. Konfigurieren der Änderungsprotokollierung

Die Änderungsprotokollierung zeichnet Änderungen im System zentral auf. Sie können bei Bedarf Detailinformationen zu den jeweiligen Änderungen anzeigen.

#### Aktivieren der Änderungsprotokollierung

Sie möchten die Protokollierung für Änderungen aktivieren. Beachten Sie, dass das Deaktivieren der Änderungsprotokollierung ebenfalls protokolliert wird.

#### So geht's

1. Öffnen Sie das Feature **Konfiguration** auf der Startseite und navigieren Sie in der Kategorie **Dokumentenmanagement** zu **E-Mails**.
2. Wählen Sie unter **E-Mail-Archivierung** den Eintrag **Archivierungsoptionen** aus.
3. Wechseln Sie in die Perspektive **Fehlerbehandlung**.
4. Aktivieren Sie die Option **Änderungsprotokollierung**.
5. Speichern Sie Ihre Angaben.

#### Anzeigen der Änderungsprotokollierung

Sie möchten die Details von protokollierten Änderungen anzeigen.

#### So geht's

1. Wählen Sie das Feature **d.ecs content crawler** auf der Startseite aus.
2. Klicken Sie auf **Änderungsprotokollierung**.
3. Klicken Sie auf einen entsprechenden Eintrag, um die Detailansicht anzuzeigen.

## 1.4. Tipps und Tricks

In diesem Thema finden Sie Informationen zu Arbeitserleichterungen und nützliche Hinweise zu Funktionen.

### 1.4.1. Aktivieren von HTTPS für eine sichere Kommunikation zwischen d.ecs http gateway und den App-Instanzen (optional)

Die Kommunikation der d.3one-Integrationen mit dem Browser und d.ecs http gateway ist generell mit HTTPS verschlüsselt. Die d.ecs http gateway-App kommuniziert aber mit der d.ecs content crawler-App unverschlüsselt mit HTTP. Ausgenommen sind Apps, die in Internetinformationsdiensten (IIS) gehostet werden. Für diese Apps ist die Kommunikation bereits mithilfe des TLS-Protokolls (Transport Layer Security-Protokolls) verschlüsselt.

Sie können die Kommunikation zwischen der d.ecs http gateway-App und d.ecs content crawler ebenfalls mit einem Zertifikat verschlüsseln, das das TLS-Protokoll verwendet. Das verwendete Protokoll entspricht dem Sicherheitsstandard, wobei SSL (Secure Sockets Layer) synonym zu TLS verwendet wird.

Um die Kommunikation zu verschlüsseln, müssen Sie TLS für d.ecs content crawler aktivieren einen festen Port zuweisen. Darüber hinaus benötigen Sie den Hashwert des Zertifikats und die Anwendungskennung, um das Zertifikat mit dem Port zu verknüpfen.

### Ermitteln des Hashwerts des zu verknüpfenden Zertifikats

Wenn Sie für die d.ecs content crawler-App einen Port festgelegt haben, müssen Sie den Hashwert des Zertifikats ermitteln, das Sie verknüpfen möchten.

Zusätzlich zum Hashwert benötigen Sie eine Anwendungskennung (App-ID). Sie können als Anwendungskennung jede gültige GUID im Format `XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX` verwenden. Mit dem Hashwert und der Anwendungserkennung können Sie das Zertifikat mit dem Port der App verknüpfen.

Sie können dasselbe Zertifikat verwenden, das Sie in IIS verwenden. Wenn Sie ein anderes Zertifikat verwenden möchten, können Sie mithilfe der Eigenschaften des Zertifikats den Hashwert (Fingerabdruck) ermitteln. Entfernen Sie unbedingt alle Leerzeichen.

Angenommen, Sie möchten den Hashwert des Zertifikats ermitteln.

#### So geht's

1. Starten Sie die Windows-Eingabeaufforderung als Administrator.
2. Geben Sie den Befehl `netsh http show sslcert ipport=0.0.0.0:<Port>` ein. Ersetzen Sie `<Port>` durch die Portnummer, die Sie bei der Installation von d.3one angegeben haben (standardmäßig `3401`).
3. Kopieren Sie den Wert für **Zertifikatshash**, z.B. in einen Texteditor.

### Festlegen des Ports in der d.ecs content crawler-App

Damit Sie die Kommunikation zwischen den Apps verschlüsseln können, müssen Sie in der d.ecs content crawler-App TLS aktivieren und der App einen festen Port zuweisen.

#### So geht's

1. Öffnen Sie den Ordner **bin** im Installationsverzeichnis der d.ecs content crawler-App (z.B.: `C:\d3\d.3 content crawler\bin`).
2. Öffnen Sie die Datei **dvelop.GroupwareCrawler.App.exe.config** mit einem Texteditor.
3. Geben Sie im Bereich **appSettings** für **protocol** den Wert **https** an (z.B.: `<add key="protocol" value="https">`).
4. Geben Sie für **port lower bound** und **port upper bound** einen festen Wert an (z.B.: `<add key="port lower bound" value="4010" /><add key="port upper bound" value="4010" />`).
5. Speichern Sie die Datei.
6. Starten Sie den Dienst **d.3content crawler App** neu.

### Verknüpfen von Zertifikat und Port der d.ecs content crawler-App

Wenn Sie einen Port festgelegt haben und das Zertifikat ermittelt haben, können Sie das Zertifikat mit dem Port der d.ecs content crawler-App verknüpfen.

#### So geht's

1. Starten Sie die Windows-Eingabeaufforderung als Administrator.
2. Geben Sie den Befehl `netsh http add urlacl url=https://*:<Port>/ user=<User>`. Ersetzen Sie `<Port>` durch die Portnummer und `<User>` durch den Benutzer, mit dem die App ausgeführt wird.
3. Geben Sie den Befehl `netsh http add sslcert ipport=0.0.0.0:<Port> certstorename=<storename> certhash=<hash> appid={<appid>}` ein. Ersetzen Sie `<storename>` durch den Zertifikatsspeicher,

<Port> durch die Portnummer, <hash> durch den gespeicherten Hashwert und <appid> durch die Anwendungskennung.

4. Bestätigen Sie den Befehl.

Wenn die Portverknüpfung erfolgreich war, können Sie die Portverknüpfung in der Windows-Eingabeaufforderung mit dem Befehl **netsh http show sslcert** anzeigen. Sie können die Portverknüpfung auch mit dem Befehl **netsh http show sslcert ipport=0.0.0.0:<Port>** direkt anzeigen. Ersetzen Sie <Port> durch die Portnummer.

Starten Sie im Anschluss die entsprechenden Apps neu, um sicherzustellen, dass die Apps sich mit HTTPS statt mit HTTP bei der d.ecs http gateway-App registrieren.

### Beispiel

```
netsh http show sslcert ipport=0.0.0.0:3401
netsh add urlacl url=https://*:4000/ user=SYSTEM netsh http add urlacl
url=https://*:4000/ user=SYSTEM
netsh http add sslcert ipport=0.0.0.0:4000 certstorename=Root
certhash=e31c06568e4b222a92c8434eaa770b26f09a31a3 appid={2131f4cd-
d05b-4308-9af1-9caa44b2c74a}
```

Siehe auch: [Prüfen der Registrierung in d.ecs http gateway](#)

## 1.4.2. Anpassen des Protokollierungsgrads in d.ecs content crawler

Sie können den Protokollierungsgrad in der Groupware-App und der d.ecs content crawler-App an Ihre Bedürfnisse anpassen.

In d.ecs content crawler können Sie zusätzlich ein erweitertes Logging aktivieren, um im Fehlerfall detailliertere Informationen zu erhalten. Wenn Sie das erweiterte Logging aktivieren, können Sie Informationen zu einem Job anzeigen und das zugehörige Dokument schneller identifizieren.

Angenommen, Sie möchten mithilfe von d.ecs content crawler alle Meldungen im zentralen d.3-Log anzeigen und das erweiterte Logging aktivieren.

### So geht's

1. Öffnen Sie das Feature **Konfiguration** auf der Startseite und navigieren Sie in der Kategorie **Dokumentenmanagement** zu **E-Mails**.
2. Wählen Sie unter **E-Mail-Archivierung** den Eintrag **Archivierungsoptionen** aus.
3. Wechseln Sie in die Perspektive **Fehlerbehandlung**.
4. Wählen Sie unter **Protokollierungsstufe** den Eintrag **All** aus.
5. Aktivieren Sie **Erweitertes Logging** und speichern Sie Ihre Angaben.

Siehe auch: [Detailinformationen zur Protokollierung](#)

## 1.4.3. Vorbereiten der Prüfung von Duplikaten

Sie können mithilfe der Groupware-App vermeiden, dass unnötige Duplikate im d.3-Repository gespeichert werden.

Damit das Prüfen von Duplikaten ordnungsgemäß funktioniert, müssen Sie sicherstellen, dass die Elemente im Repository in den entsprechenden d.3-Status importiert und gespeichert werden. Wenn Sie z.B. beim Erstellen einer Zuordnung für das Element **E-Mail** das Importieren und Speichern in einen Status ermöglichen möchten, müssen Sie in der Konfiguration von d.3 admin für folgende Parameter den Wert **Nein** festlegen:

- **IGNORE\_DUPS\_IN\_A**: Zum Überprüfen von Elementen, die direkt in den Status **Archiv** gespeichert werden.

- **IGNORE\_DUPS\_IN\_B\_P**: Zum Überprüfen von Elementen, die direkt in den Status **Bearbeitung** oder **Prüfung** gespeichert werden.

Weitere Informationen zu den Parametern und dem Prüfen von Duplikaten finden Sie im Handbuch von d.3 admin.

#### 1.4.4. Aktivieren der Prüfung von Duplikaten

Sie können vermeiden, dass unnötige Duplikate im d.3-Repository gespeichert werden, indem Sie das Prüfen von Duplikaten in der Groupware-App aktivieren. Sie können die Funktion für d.3one und für d.ecs content crawler aktivieren.

##### So geht's

1. Öffnen Sie das Feature **Konfiguration** auf der Startseite und navigieren Sie in der Kategorie **Dokumentenmanagement** zu **E-Mails**.
2. Wählen Sie unter **E-Mail-Verwaltung** den Eintrag **Verwaltungsoptionen** aus.
3. Wählen Sie in der Perspektive **Groupware-Einstellungen** die entsprechende Option zum Prüfen der Duplikate aus.
4. Speichern Sie Ihre Angaben.

#### 1.4.5. Konfigurieren einer Berechtigungsprüfung

Beim Speichern von E-Mails im d.3-Repository werden alle Empfänger und der Absender der E-Mail in ein d.3-Systemfeld geschrieben (**dvelop.groupware.mail.restrictions**). Sie können mit d.3 server Version 8 eine Berechtigungsprüfung mithilfe von sogenannten Restrictionsets festlegen. Vorhandene Gruppen in der Empfängerliste werden rückwirkend aufgelöst.

##### Anmerkung

Wenn die X.500-Adresse von internen Empfängern oder dem internen Absender nicht aufgelöst werden kann, wird eine Fehlermeldung in das Log geschrieben. Darüber hinaus wird das d3.-Systemfeld **dvelop.groupware.mail.restrictions.resolve.error** mit dem Wert **1** gefüllt, damit Sie das betroffene Dokument einfach identifizieren und korrigieren können.

Darüber hinaus werden beim Speichern aus der E-Mail-Anwendung folgende Werte in d.3-Systemfelder geschrieben, die Sie für Ihre Berechtigungsprüfung verwenden können:

- **dvelop.groupware.messageID**: Die Nachrichten-ID der E-Mail. Die ID wird auch beim Speichern von Anlagen eingetragen.
- **dvelop.groupware.attachmentid**: Die ID der Anlage beim Speichern einer einzelnen Anlage.
- **dvelop.groupware.recoverableItem**: Wenn in Microsoft Exchange das gespeicherte Dokument auf einer als gelöscht markierten E-Mail basiert, ist der Wert **1**.
- **dvelop.groupware.attachments.count**: Beim Speichern einer E-Mail wird die Anzahl der Anlagen eingetragen.
- **dvelop.groupware.attachments.name**: Der Dateiname der Anlage, wenn eine E-Mail gespeichert wird.
- **dvelop.groupware.attachments.extension**: Die Dateierweiterung inklusive Punkt der Anlage, wenn eine E-Mail gespeichert wurde.
- **dvelop.groupware.attachments.index**: Der interne Index der Anlagen beim Speichern von E-Mails. Geben Sie den Parameter an, wenn ein Retrieval-Link erstellt werden soll.
- **dvelop.groupware.attachments.size**: Die Dateigröße der Anlagen beim Speichern der E-Mail.
- **dvelop.groupware.attachments.type**: Die Darstellung des Typs der entsprechenden Anlage. Beim Wert **EMBEDDED** handelt es sich um eine eingebettete Anlage. Beim Wert **FILE** handelt es sich bei der Anlage um eine angehängte Datei.
- **dvelop.groupware.mail.restrictions**: Eine Tabelle, in der alle Empfänger und der Absender der E-Mail eingetragen werden (Berechtigungssteuerung).

- **dvelop.groupware.cm.token:** Wenn die Option **db | case manager-Daten verarbeiten** in d.ecs content crawler aktiviert ist, wird das db | case manager-Token eingetragen.
- **dvelop.groupware.mail.conversationid:** Die Konversations-ID (Message Header: **Thread-Index**).

Folgende Systemfelder werden nur geschrieben, wenn das Prüfen von Duplikaten deaktiviert ist.

- **dvelop.groupware.exchange.mailbox.objectguid:** Die eindeutige Objekt-GUID des d.3one-Benutzers, der das Element im d.3-Repository gespeichert hat.
- **dvelop.groupware.exchange.mailbox.userguid:** Die eindeutige Objekt-GUID des Postfachbenutzers aus d.ecs identity provider.
- **d.velop.groupware.exchange.mailbox.name:** Der Name des Microsoft Exchange-Postfachs, in dem die gespeicherte E-Mail zu finden ist.

#### 1.4.6. Aktivieren der Funktion zum gleichzeitigen Wiederherstellen von mehreren E-Mails

Sie können mit d.ecs content crawler mehrere E-Mails gleichzeitig wiederherstellen.

Beim Wiederherstellen werden die Typen DGIX, MSG, NZIP und EML unterstützt. Wenn das Zielsystem HCL Domino ist, können Sie beim Wiederherstellen nur E-Mails auswählen, die mit dem Domino-Service gespeichert wurden.

Um E-Mails wiederherstellen zu können, müssen Sie die Option in d.ecs content crawler aktivieren.

##### So geht's

1. Öffnen Sie das Feature **Konfiguration** auf der Startseite und navigieren Sie in der Kategorie **Dokumentenmanagement** zu **E-Mails**.
2. Wählen Sie unter **E-Mail-Archivierung** den Eintrag **Archivierungsoptionen** aus.
3. Wechseln Sie in die Perspektive **Verarbeitungseinstellungen**.
4. Aktivieren Sie im Bereich **Wiederherstellung** die Option **E-Mails wiederherstellen**.

#### 1.4.7. Wiederherstellen von mehreren E-Mails aus der Ergebnisliste einer Suche

Wenn Sie die Option zum Wiederherstellen von E-Mails aktiviert haben, können Sie mithilfe der Suche in d.3one mehrere E-Mails gleichzeitig aus der Ergebnisliste einer Suche wiederherstellen. Im Anschluss definieren Sie ein Ziel für die wiederherzustellenden E-Mails.

Wenn Sie HCL Domino als Zielsystem auswählen, geben Sie als Datenbank den Namen der physischen HCL Notes-Datenbank an (**mail\user1.nsf**).

Wenn Sie Microsoft Exchange als Zielsystem auswählen, geben Sie als Zielpostfach eine SMTP-Adresse oder einen Benutzernamen an. In Microsoft Exchange können Sie auch Makros als Zielordner angeben. Sie können bei Bedarf die Option **Microsoft Exchange In-Situ-Archiv aktivieren**, wenn der Import der E-Mails in das In-Situ-Archiv erfolgen soll.

Angenommen, Sie möchten mehrere E-Mails aus einer Ergebnisliste wiederherstellen.

##### So geht's

1. Führen Sie eine Suche im Feature **Suche** aus, die die wiederherzustellenden E-Mails enthält.
2. Wählen Sie die Kontextaktion **E-Mails wiederherstellen** aus.
3. Markieren Sie einzelne oder alle E-Mails aus der Ergebnisliste und klicken Sie auf **E-Mails wiederherstellen**.
4. Geben Sie eine Beschreibung für den Job an.
5. Wählen Sie ein Zielsystem aus.
6. Geben Sie ein Zielpostfach oder eine Zieldatenbank an.
7. Geben Sie einen Zielordner an. Der Unterordner wird automatisch erstellt.

8. Starten Sie die Wiederherstellung.

Für jede wiederherzustellende E-Mail wird ein Job in dem Profil **Restore** erstellt.

### 1.4.8. Überwachen von d.ecs content crawler mit d.ecs monitor

Wenn Sie d.ecs monitor zum Überwachen von d.ecs content crawler verwenden möchten, müssen Sie in den entsprechenden d.3ecm-Systemumgebungen jeweils d.ecs monitor agent installieren. Wenn d.ecs monitor agent bereits in Ihrer d.3ecm-Systemumgebung vorhanden ist, wird der Agent automatisch erkannt und d.ecs monitor agent sendet die Statusinformationen an d.ecs monitor.

Mit d.ecs monitor erhalten Sie allgemeine Informationen zum Status von d.ecs content crawler, z.B. zur CPU-Auslastung, dem Speicherverbrauch oder der Anzahl der Threads. Die d.ecs content crawler-App sendet zusätzlich die Anzahl der fehlerhaften Jobs an d.ecs monitor. Sie können die Jobs unter **Überwachungsobjekt** anzeigen. Standardmäßig wird bei 100 Jobs mit fehlerhaftem Status ein Alarm in d.ecs monitor ausgelöst. Sie können den Wert bei Bedarf anpassen.

Weitere Informationen zu d.ecs monitor finden Sie im Administrationshandbuch von d.ecs monitor.

### 1.4.9. Überwachen der Journalarchivierung

Wenn die Journalfunktion überwacht werden soll, empfehlen wir, das Journalpostfach der E-Mail-Anwendung einzubeziehen. Sie können nicht verarbeitete E-Mails schneller erkennen und Maßnahmen ergreifen.

Alternativ können Sie regelmäßig PowerShell-Skripte ausführen.

### 1.4.10. Festlegen eines anderen Ports und HTTP-Protokolls

Standardmäßig wird der Port der App dynamisch ermittelt. Sie können den Port und das HTTP-Protokoll bei Bedarf auch ändern.

#### So geht's

1. Erstellen Sie im Installationsverzeichnis der App einen Ordner mit dem Namen **conf**.
2. Erstellen Sie eine Datei mit dem Namen **appsettings.config**.
3. Geben Sie den Port an, indem Sie für die obere und untere Grenze jeweils denselben Wert eintragen.
4. Geben Sie einen Wert für **protocol** ein, z.B. **http** oder **https**.
5. Starten Sie die App neu.

```
<?xml version="1.0" encoding="utf-8"?>
<appSettings>
  <add key="port lower bound" value="4000" />
  <add key="port upper bound" value="4200" />
  <add key="protocol" value="http" />
</appSettings>
```

Sie können jedoch auch die Suche nach einem freien Port konfigurieren:

- **port lower bound**: Gibt die untere Grenze an, oberhalb derer die App nach einem freien Port suchen soll.
- **port upper bound**: Gibt die obere Grenze an, unterhalb derer die App nach einem freien Port suchen soll.
- **protocol**: Gibt das Protokoll an, über das die App die Verbindungen aufbauen soll. Die möglichen Werte sind **http** oder **https**.

## 1.5. Häufig gestellte Fragen

In diesem Thema finden Sie Antworten auf häufig gestellte Fragen.

### 1.5.1. Aus welchen Ordnern werden gelöschte Elemente archiviert, wenn ich das Beweissicherungsverfahren oder In-Situ Speicher aktiviert habe?

Wenn Sie das Beweissicherungsverfahren oder In-Situ-Speicher aktiviert haben, werden beim Archivieren von gelöschten Elementen die Ordner **Löschvorgänge (Deletions)** und **Endgültige Löschvorgänge (Purges)** archiviert. Die Ordner werden nicht aus dem Archivordner archiviert.

Weitere Informationen finden Sie auf der Microsoft Docs-Website in der Exchange Server 2019-Dokumentation unter "Ordner 'erneut herstellbare Elemente' in Exchange Server".

### 1.5.2. Für welche Nachrichtenklassen kann ich das Journaling, die Postfacharchivierung oder das manuelle Speichern mit dem Microsoft Outlook-Add-In verwenden?

Mit der folgenden Liste können Sie anhand der IDs nachvollziehen, für welche Nachrichtenklassen Sie das Journaling oder die Postfacharchivierung in d.ecs content crawler verwenden können. Darüber hinaus erfahren Sie, welche Nachrichtenklassen das manuelle Speichern in der d.3one-Integration in Microsoft Outlook unterstützen.

#### IPM.Activity

- Name: Journaleinträge
- Journaling: Nein
- Postfacharchivierung: Nein
- Manuelles Speichern: Nein

#### IPM.Appointment

- Name: Termine
- Journaling: Ja
- Postfacharchivierung: Nein
- Manuelles Speichern: Nein

#### IPM.Contact

- Name: Kontakte
- Journaling: Nein
- Postfacharchivierung: Nein
- Manuelles Speichern: Nein

#### IPM DistList

- Name: Verteilerliste (werden als ZIP-Container mit einzelnen vCards gespeichert)
- Journaling: Ja (als Anlage einer E-Mail)
- Postfacharchivierung: Ja (als Anlage einer E-Mail)
- Manuelles Speichern: Ja (als Anlage einer E-Mail, gilt nicht beim Speichern als Anlage)

#### IPM.Document

- Name: Dokumente
- Journaling: Nein
- Postfacharchivierung: Nein
- Manuelles Speichern: Nein

#### IPM.OLE.Class

- Name: Vom Serienmuster abweichende Ausnahmeelemente

- Journaling: Nein
- Postfacharchivierung: Nein
- Manuelles Speichern: Nein

#### **IPM**

- Name: Elemente, für die das angegebene Formular nicht gefunden wurde
- Journaling: Nein
- Postfacharchivierung: Nein
- Manuelles Speichern: Nein

#### **IPM.Note**

- Name: E-Mails
- Journaling: Ja
- Postfacharchivierung: Ja
- Manuelles Speichern: Ja

#### **IPM.Note.IMC.Notification**

- Name: Berichte von Internet Mail Connector (Microsoft Exchange Server-Gateway ins Internet)
- Journaling: Ja
- Postfacharchivierung: Ja
- Manuelles Speichern: Ja

#### **IPM.Note.Rules.Oof.Template.Microsoft**

- Name: Abwesenheitsvorlagen
- Journaling: Ja
- Postfacharchivierung: Nein
- Manuelles Speichern: Ja

#### **IPM.Post**

- Name: Bereitstellen von Notizen in einem Ordner
- Journaling: Ja
- Postfacharchivierung: Nein
- Manuelles Speichern: Nein

#### **IPM.StickyNote**

- Name: Erstellen von Notizen
- Journaling: Nein
- Postfacharchivierung: Nein
- Manuelles Speichern: Nein

#### **IPM.Recall.Report**

- Name: Berichte für Nachrichtenrückruf
- Journaling: Nein
- Postfacharchivierung: Nein
- Manuelles Speichern: Nein

#### **IPM.Outlook.Recall**

- Name: Rückrufen gesendeter Nachrichten aus dem Posteingang des Empfängers
- Journaling: Nein

- Postfacharchivierung: Nein
- Manuelles Speichern: Nein

**IPM.Remote**

- Name: Remotemail-Nachrichtenkopf
- Journaling: Nein
- Postfacharchivierung: Nein
- Manuelles Speichern: Nein

**IPM.Note.Rules.ReplyTemplate.Microsoft**

- Name: Abwesenheitsvorlagen
- Journaling: Ja
- Postfacharchivierung: Nein
- Manuelles Speichern: Ja

**IPM.Report**

- Name: Statusberichte zu Elementen
- Journaling: Ja
- Postfacharchivierung: Nein
- Manuelles Speichern: Nein

**IPM.Resend**

- Name: Erneutes Senden einer fehlerhaften Nachricht
- Journaling: Ja
- Postfacharchivierung: Nein
- Manuelles Speichern: Nein

**IPM.Schedule.Meeting.Canceled**

- Name: Besprechungsabsagen
- Journaling: Ja
- Postfacharchivierung: Nein
- Manuelles Speichern: Nein

**IPM.Schedule.Meeting.Request**

- Name: Besprechungsanfragen
- Journaling: Ja
- Postfacharchivierung: Nein
- Manuelles Speichern: Nein

**IPM.Schedule.Meeting.Resp.Neg**

- Name: Antworten zur Ablehnung von Besprechungsanfragen
- Journaling: Ja
- Postfacharchivierung: Nein
- Manuelles Speichern: Nein

**IPM.Schedule.Meeting.Resp.Pos**

- Name: Antworten zur Zusage von Besprechungsanfragen
- Journaling: Ja
- Postfacharchivierung: Nein

- Manuelles Speichern: Nein

#### **IPM.Schedule.Meeting.Resp.Tent**

- Name: Antworten zur Zusage von Besprechungsanfragen
- Journaling: Ja
- Postfacharchivierung: Nein
- Manuelles Speichern: Nein

#### **IPM.Note.Secure**

- Name: Digital unterzeichnete Notizen an andere Personen
- Journaling: Ja
- Postfacharchivierung: Ja
- Manuelles Speichern: Ja

#### **IPM.Note.Secure.Sign**

- Name: Verschlüsselte Notizen an andere Personen
- Journaling: Ja
- Postfacharchivierung: Ja
- Manuelles Speichern: Ja

#### **IPM.Task**

- Name: Aufgaben
- Journaling: Ja
- Postfacharchivierung: Nein
- Manuelles Speichern: Nein

#### **IPM.TaskRequest.Decline**

- Name: Antworten zur Annahme einer Aufgabenanfrage
- Journaling: Ja
- Postfacharchivierung: Nein
- Manuelles Speichern: Nein

#### **IPM.TaskRequest**

- Name: Aufgabenanfragen
- Journaling: Ja
- Postfacharchivierung: Nein
- Manuelles Speichern: Nein

#### **IPM.TaskRequest.Update**

- Name: Aktualisierung von Anfragen
- Journaling: Ja
- Postfacharchivierung: Nein
- Manuelles Speichern: Nein

#### **IPM.conflict.message**

- Journaling: Ja
- Postfacharchivierung: Nein
- Manuelles Speichern: Nein

#### **IPM.sharing**

- Journaling: Ja
- Postfacharchivierung: Nein
- Manuelles Speichern: Nein

#### **Report.report.ipm.note.ipnrm.ndr**

- Journaling: Ja
- Postfacharchivierung: Nein
- Manuelles Speichern: Nein

#### **IPM.Schedule.Meeting.Notification**

- Journaling: Ja
- Postfacharchivierung: Nein
- Manuelles Speichern: Nein

### **1.5.3. Warum wird die Option zum Archivieren von gelöschten Elementen beim Profilerstellen nicht angezeigt?**

Beim Erstellen eines Profils steht Ihnen die Option **Archivieren von gelöschten Elementen aktivieren** nur dann zur Verfügung, wenn Sie **Microsoft Exchange** als Quellsystem auswählen. Die Option wird ab Microsoft Exchange 2016 von d.ecs content crawler unterstützt.

### **1.5.4. Was ist der Unterschied zwischen dem Löschen und Zurücksetzen von Jobs?**

Im Feature d.ecs content crawler können Sie unter **Statistikübersicht** in den Bereich **Jobübersicht** navigieren, um Jobs zu markieren und bei Bedarf mit den entsprechenden Kontextaktionen zu löschen oder zurückzusetzen. Wenn Sie ein Profil löschen möchten, stellen Sie sicher, dass keine Jobs mehr für dieses Profil in der Datenbank vorhanden sind.

Wenn Sie die markierten Jobs löschen, werden die Jobs aus der Datenbank gelöscht und die zugrundeliegenden Dokumente zurückgesetzt.

Wenn Sie die markierten Jobs zurücksetzen, werden die Jobs und die zugrundeliegenden Dokumente zurückgesetzt. Im Anschluss werden diese Jobs direkt wieder mit dem Profil verarbeitet.

### **1.5.5. Was ist eine Named-User-Lizenz?**

Eine Named-User-Lizenz ist genau einem Anwender für ein Produkt oder eine Integration zugeordnet. Durch die Zuordnung ist eine Lizenz für einen Anwender reserviert und die Lizenz kann von keinem anderen Anwender verwendet werden.

Named-User-Lizenzen werden für jede d.3one-Integration beim ersten Starten für den Anwender und die d.3one-Integration zugewiesen. Wenn sich z.B. ein Anwender an d.3one im Browser oder der Integration anmeldet, wird eine Lizenz für diesen Anwender und für dieses Produkt in d.ecs license server reserviert.

Siehe auch: [Detailinformationen zu d.3one-Lizenzen](#)

### **1.5.6. Was sind Kategorien?**

Sie können Ihre Anwender bei der täglichen Arbeit unterstützen, indem Sie Kategorien zum Speichern von Elementen definieren. Standardmäßig wird keine Kategorie vorgegeben. Sie können aber eigene Kategorien administrativ erstellen.

Mithilfe von Kategorien können Sie Quellen (z.B. E-Mails oder Anlagen) nicht nur mit den d.3-Kategorien (Dokumentarten) für das Speichern im Repository klassifizieren, sondern Sie können mit der Groupware-App eigene Kategorien definieren, in denen die Elemente gespeichert werden. Mit einer Kategorie können Sie eine Quelle mehreren d.3-Kategorien zuordnen.

Sie können die Kategorien individuell anpassen, da die Kategorien unabhängig vom Repository und der Quelle sind.

### Anmerkung

Sie können Kategorien Farben zuweisen (verfügbar ab Version 1.32.0 von d.ecs groupware). Wenn Sie die Microsoft Graph-Schnittstelle verwenden und die Berechtigung **MailboxSettings.ReadWrite** in der Azure Active Directory-App-Registrierung erteilt haben, wird im Postfach automatisch die Farbe für die Kategorie verwendet. Wenn die Berechtigung nicht erteilt ist, wird die Kategorie weiterhin ohne Farbzuzuordnung erstellt und ein Warnhinweis im Protokoll (Log) ausgegeben.

Siehe auch:

- [Erstellen von Kategorien](#)
- [Detailinformationen zu Quellen](#)
- [Detailinformationen zu Zuordnungen](#)

### 1.5.7. Was sind Profile?

Um die regelbasierte Archivierung zu verwenden, erstellen Sie Profile. Ein Profil verfügt über drei zentrale Komponenten: Quellen, Regeln und Verarbeitungsschritte.

Quellen, Regeln und Verarbeitungsschritte werden zu Sammlungen zusammengefasst. Mit diesen Sammlungen können Sie festlegen, welche Elemente basierend auf welchen Regeln archiviert und ggf. nachverarbeitet werden.

Damit die Eigenschaften von E-Mails den entsprechenden d.3-Eigenschaften zugeordnet werden können, müssen Sie eine Zuordnung (Mapping) erstellen.

Siehe auch:

- [Erstellen von Profilen](#)
- [Detailinformationen zu Quellensammlungen](#)
- [Detailinformationen zu Regelsammlungen](#)
- [Detailinformationen zu Verarbeitungsschrittsammlungen](#)

### 1.5.8. Was sind Quellen?

Mithilfe von Zuordnungen können Sie ein beliebiges Quellsystem (z.B. eine E-Mail-Anwendung oder ein ERP-System) mit einem d.3-Repository verknüpfen.

Ein Quellsystem kann mehrere Quellen definieren, z.B. E-Mails und Anlagen. Die Quellen beschreiben ein Element im Quellsystem mit den spezifischen Eigenschaften und Kategorien.

Bei Archivierungsprofilen sind Quellen Datentöpfe, aus denen Elemente gelesen werden wie z.B. Benutzern, Gruppen, oder öffentlichen Ordnen von Microsoft Exchange.

Im Kontext der Groupware-App sind Quellen die zu verarbeitenden Elemente, z.B. E-Mails oder Anlagen. Die App ermittelt die Eigenschaften der Quelle (z.B. Absender, Betreff oder Empfänger) und generiert die zu speichernde Nutzdatei.

Mithilfe einer Zuordnung können Sie die Eigenschaften einer Quelle mit bestimmten d.3-Eigenschaftsfeldern (Repositoryfeldern) verknüpfen. Sie können eigene Quellen für Zuordnungen definieren.

Sie können darüber hinaus die Quellen weiter klassifizieren, indem Sie Kategorien erstellen. Mit den Kategorien sind Sie von den Kategorien (Dokumentarten) im d.3-Repository unabhängig.

Mit den E-Mail-Integrationen und d.ecs content crawler stehen Ihnen Standardquellen zum Erstellen von Zuordnungen zur Verfügung:

- **Standard - Microsoft Exchange-E-Mail**
- **Standard - Microsoft Exchange-Anlage**
- **Standard - Microsoft Exchange-Journal-E-Mail**
- **Standard - IBM Notes-E-Mail**
- **Standard - IBM Notes-Anlage**
- **Standard - IBM Notes-Journal-E-Mail**
- **Standard - Termin/Besprechung**

Siehe auch:

- [Erstellen von Quellen](#)
- [Detailinformationen zu Kategorien](#)
- [Detailinformationen zu Zuordnungen](#)

### 1.5.9. Was sind Quellensammlungen?

Für die regelbasierte Archivierung müssen Sie in jedem Profil die Quellen angeben, die archiviert werden sollen. Die Quellen sind Postfächer oder Maildatenbanken, aus denen Elemente archiviert werden. Eine Quellensammlung kann aus mehreren Quellen bestehen. Um die zu archivierenden Postfächer oder Maildatenbanken für ein Profil anzugeben, erstellen und konfigurieren Sie eine Quellensammlung.

Je nach hinzugefügter Quelle gelten bestimmte Besonderheiten, z.B.:

- **Benutzer:**
  - Die Postfächer werden automatisch anhand des angegebenen Benutzernamens ermittelt.
  - Da das Adressbuch durchsucht wird, werden eventuell für einen Eintrag mehrere Postfächer von unterschiedlichen Benutzern gefunden.
- **Gruppe:**
  - Die Postfächer werden automatisch anhand der angegebenen Gruppe ermittelt.
  - Gruppen in Gruppen werden ebenfalls aufgelöst.
  - Bei Microsoft Exchange müssen Sie die SMTP-Adresse der Gruppe angeben. Die Gruppe muss im Microsoft Exchange-Adressbuch sichtbar sein, damit sie aufgelöst werden kann.
- **Microsoft Exchange Öffentlicher Ordner:**
  - Die Postfächer werden anhand des angegebenen Dateipfads ermittelt.
  - Wenn Sie verhindern möchten, dass Unterordner ebenfalls archiviert werden, wählen Sie die Regel **Ordner einschränkung** aus.
- **Microsoft Exchange In-Situ-Archiv:**
  - Die Postfächer werden anhand des angegebenen Microsoft Exchange In-Situ-Archiv ermittelt.
  - Bei Microsoft Exchange müssen Sie die SMTP-Adresse des In-Situ-Archivs angeben.
  - Stellen Sie sicher, dass die In-Situ-Archivierung für das Postfach aktiviert ist.

Siehe auch:

- [Erstellen von Quellensammlungen](#)
- [Detailinformationen zu Profilen](#)
- [Detailinformationen zu Regelsammlungen](#)
- [Detailinformationen zu Verarbeitungsschrittsammlungen](#)

### 1.5.10. Was sind Regelsammlungen?

In jedem Profil müssen Sie einen Satz von Regeln angeben. Anhand der Regeln wird ermittelt, welche Elemente archiviert werden. Mehrere Regeln sind mit UND-Verknüpfungen verbunden und werden zu einer Regelsammlung zusammengefasst. Um die Archivierungsregeln für ein Profil festzulegen, erstellen und konfigurieren Sie eine Regelsammlung.

Je nach hinzugefügter Regel gelten bestimmte Besonderheiten, z.B.:

- **Ordner einschränkung:**
  - Sie können Einschlussordner oder Ausschlussordner für Microsoft Exchange oder HCL Domino festlegen.
  - Eine Regel kann nur Einschlussregeln oder Ausschlussregeln enthalten.
  - Geben Sie Unterordner mit einem Backslash (\) an. Wenn Sie z.B. einen Unterordner **Rechnungen** ebenfalls archivieren möchten, geben Sie als Einschlussordner **Posteingang\Rechnungen** an.
  - Mit der Option **Unterordner berücksichtigen** können Sie pro Ordner festlegen, dass auch die Unterordner archiviert werden. Wenn Sie z.B. keine Elemente aus dem Ordner **Gelöschte Elemente** oder den Unterordnern archivieren möchten, geben Sie als Ausschlussordner **Gelöschte Elemente** an und aktivieren **Unterordner berücksichtigen**.
  - Sie können für HCL Domino den Posteingang mit dem Makro **\$Inbox** referenzieren. Ihre erstellten Ordner können Sie mit den entsprechenden Namen ebenfalls mit dem Makro referenzieren.
  - Für Microsoft Exchange stehen Ihnen ebenfalls verschiedene Makros zur Verfügung. Beim Einschließen von Unterordnern entsteht eventuell eine erhöhte Last auf dem Microsoft Exchange Server oder dem HCL Domino Server.
- **Externe Regelprüfung:**
  - Sie können festlegen, dass ein Element mit einer externen Anwendung geprüft wird statt mit einer zuvor erstellten Regel. Geben Sie die URI für die Regelprüfung an.
  - Die externe Regelprüfung wird immer als letzter Schritt nach allen vorherigen Regeln ausgeführt. Weitere Informationen z.B. zum Aufbau der HTTP-Aufrufe und der zu übermittelnden Daten finden Sie in den Themen zum Konfigurieren der externen Regelprüfung.
- **Prüfung auf Betreff:**
  - Es wird anhand des Inhalts des Betreffs geprüft, welche Elemente archiviert werden. Sie können E-Mails anhand des Betreffs einschließen oder ausschließen.
  - Wenn Sie Suchbegriffe angeben, beachten Sie, dass die Groß- und Kleinschreibung berücksichtigt wird.
  - Wenn Sie die Option **Alle Übereinstimmungen** aktivieren, müssen alle Suchbegriffe im Betreff vorkommen (UND-Verknüpfung).
  - Wenn Sie die Option **Mindestens eine Übereinstimmung** aktivieren, muss mindestens ein Suchbegriff im Betreff vorkommen (ODER-Verknüpfung).
- **Regulärer Ausdruck auf Betreff anwenden:** Sie können festlegen, dass Betreffs von E-Mails mithilfe eines regulären Ausdrucks ein- oder ausgeschlossen werden. Aktivieren Sie zum Ausschließen von Elementen die Option **Nicht verarbeiten**.
- **Nur externe Mails:** Es werden nur Elemente ermittelt, die mindestens einen externen Empfänger oder Sender haben. Sender oder Empfänger gelten als intern, wenn sie die Domäne enthalten. Wenn das Element ausschließlich interne Adressen enthält, wird das Element nicht verarbeitet.
- **S/MIME-verschlüsselte Dokumente auslassen:** Sie können mit dieser Regel festlegen, dass S/MIME-verschlüsselte E-Mails von der Verarbeitung ausgeschlossen werden. Nur Absender und Empfänger können diese E-Mails im Klartext lesen. Hierfür wird Microsoft Outlook (Desktop-Version) benötigt. Wenn Sie diese Regel nicht verwenden und S/MIME-verschlüsselte E-Mails archivieren, sind diese E-Mails unter Umständen nicht mehr lesbar. Eine Rendition kann in diesem Fall ebenfalls nicht erzeugt werden.
- **DRM-geschützte Dokumente auslassen (nur Microsoft Exchange):** Sie können mit dieser Regel festlegen, dass DRM-geschützte E-Mails von der Verarbeitung ausgeschlossen werden. DRM-geschützte E-Mails werden durch einen externen Microsoft-Dienst mit digitalen Berechtigungen (z.B. nicht Weiterleiten, nicht Drucken etc.) versehen. Nur Absender und Empfänger können diese E-Mails im Klartext lesen. Hierfür wird Microsoft Outlook (Desktop-Version) benötigt. Wenn Sie diese Regel nicht verwenden und DRM-geschützte E-Mails archivieren, sind diese E-Mails unter Umständen nicht mehr lesbar. Eine Rendition kann in diesem Fall ebenfalls nicht erzeugt werden.

Siehe auch:

- [Erstellen von Regelsammlungen](#)
- [Detailinformationen zu Profilen](#)

- [Detailinformationen zu Quellensammlungen](#)
- [Detailinformationen zu Verarbeitungsschrittsammlungen](#)
- [Detailinformationen zur externen Regelprüfung](#)
- [Detailinformationen zur externen Regelprüfung mit d.ecs script](#)

### 1.5.11. Was sind Verarbeitungsschrittsammlungen?

In jedem Profil müssen Sie die Verarbeitungsschritte angeben, um festzulegen, wie die archivierten Elemente weiterverarbeitet werden. Um festzulegen, welche Schritte beim Weiterverarbeiten angewendet werden sollen, erstellen und konfigurieren Sie eine Verarbeitungsschrittsammlung.

Je nach hinzugefügtem Verarbeitungsschritt gelten bestimmte Besonderheiten, z.B.:

- **Dokument archivieren:**
  - Alle ermittelten Elemente werden archiviert.
  - Sie können zusätzlich die Nachverarbeitung der Elemente festlegen.
  - Wir empfehlen, die Option zum Löschen nur für das Überwachen von Funktionspostfächern.
  - Sie können bereits archivierte Elemente zu einem späteren Zeitpunkt löschen, indem Sie ein Profil mit der Nachbearbeitungsaktion zum Löschen erstellen.
  - Wenn Sie die Option **dfs | case manager-Daten verarbeiten** aktivieren, wird eventuell die Verarbeitungsgeschwindigkeit der E-Mail-Archivierung beeinflusst. Verwenden Sie die Option nur für die Funktionspostfächer von dfs | case manager. Sie können diesen Verarbeitungsschritt nicht mit der Regel **Archivierte Dokumente** verwenden.
- **In Dateisystem speichern:**
  - Alle ermittelten Elemente werden im EML-Format in das Dateisystem übertragen.
  - Sie können bei Bedarf **Keine Unterordner** aktivieren, um festlegen, dass nur die Ordner auf der obersten Ebene archiviert werden.
  - Wenn Sie die Option für die Verarbeitung von PEC-E-Mails aktivieren, werden die angehängte EML-E-Mails in das Dateisystem übertragen und die Anlagen separat gespeichert. Sie können diesen Verarbeitungsschritt nicht mit der Regel **Archivierte Dokumente** verwenden.
  - Sie können bei der Pfadangabe einen statischen oder dynamischen Pfad verwenden. Beim statischen Pfad tragen Sie den vollständigen Pfad im Feld Pfad ein. Beim dynamischen Pfad tragen Sie an einer beliebigen Stelle im Pfad das Makro **<SMTPADDRESS>** ein, z.B. **C:\export\<<SMTPADDRESS>**. Erstellen Sie für das Makro einen regulären Ausdruck, der aus einer SMTP-Adresse einen Textteil ermitteln kann. Der Textteil wird an der Stelle des Makros **<SMTPADDRESS>** ersetzt. Beispiel:
    - Pfad: **C:\export\<<SMTPADDRESS>**
    - Input: **Mustermann@Domain.com**
    - Regulärer Ausdruck: **(?<=@)[^.]+(?=\.)**
    - Outputpfad: **C:\export\Domain**
  - Wenn Sie HCL Domino verwenden, ermittelt das System aus Performancegründen nicht die SMTP-Adresse, sondern stellt den Namen der E-Mail-Datenbankbank bereit. Bauen Sie daher einen regulären Ausdruck für einen dynamischen Pfad wie folgt auf:
    - Pfad: **C:\export\<<SMTPADDRESS>**
    - Input: **mail\bbnutze**
    - Regulärer Ausdruck: **[a-zA-Z]{8}**
    - Outputpfad: **C:\export\bbnutze**
- **Ablage über d.velop inbound:**
  - Die Option **PDF-Anlagen an d.velop inbound übergeben** extrahiert Anlagen im PDF-Format und übergibt die Anlagen an d.velop inbound.
  - Sie können die Option **Gesamte Mail an d.velop inbound übergeben** nur verwenden, wenn Sie d.velop inbound in der d.velop cloud abonniert haben.
- **Nachbearbeitungsaktion:**
  - Sie können festlegen, wie bereits archivierte Elemente weiterverarbeitet werden.

- Anlagen werden nur dann entfernt und durch HTTP-Links ersetzt, wenn die Anlage eindeutig entfernt werden kann. Bei bestimmten E-Mail-Formaten ist nicht immer eindeutig, ob die Anlagen entfernt werden können, z.B. bei MIME-Formaten. Die entsprechenden E-Mails werden trotzdem komplett im d.3-Repository gespeichert.
- Um alle E-Mails zu entlasten und eine passende Formatierung bereitzustellen, prüfen Sie die Einstellungen Ihres Mailgateways.
- Sie können diesen Verarbeitungsschritt nicht zusammen mit der Regel **Nicht archivierte Dokumente** verwenden.
- Wenn Sie mehrere Verarbeitungsschritte auswählen, ergeben sich folgende Abhängigkeiten:
  - Sie können nur einen Verarbeitungsschritt mit aktiver Nachbearbeitung erstellen. Der Verarbeitungsschritt mit Nachbereitung wird immer als letzter Schritt nach allen vorherigen Verarbeitungsschritten ausgeführt.
  - Sie können die Option **Ablage über d.velop inbound** nur einmal auswählen.
  - Sie können nur eine Nachbearbeitungsaktion auswählen.
  - Sie können die Optionen **Dokument archivieren** und **In Dateisystem speichern** mehrfach für unterschiedliche Parameter verwenden.

Siehe auch:

- [Erstellen von Verarbeitungsschrittsammlungen](#)
- [Detailinformationen zu Profilen](#)
- [Detailinformationen zu Quellensammlungen](#)
- [Detailinformationen zu Regelsammlungen](#)

### 1.5.12. Was sind Zuordnungen?

Mit einer Zuordnung (Mapping) verknüpfen Sie ein Quellsystem (z.B. eine E-Mail-Anwendung) mit einem Ziel (einem d.3-Repository).

Jede E-Mail hat standardmäßig bestimmte Eigenschaften, z.B. Absender, Empfänger oder Betreff. Sie können die Standardeigenschaften einer d.3-Kategorie und den zugehörigen d.3-Eigenschaften zuordnen. Wenn Sie entsprechende Zuordnungen erstellen, müssen Ihre Anwender diese Eigenschaften nicht mehr manuell angeben.

Weitere Informationen zum Erstellen und Verwalten von Zuordnungen finden Sie im Administrationshandbuch von d.3one.

Siehe auch:

- [Detailinformationen zu Quellen](#)
- [Erstellen von Quellen](#)
- [Detailinformationen zu Kategorien](#)
- [Erstellen von Kategorien](#)

### 1.5.13. Welche Authentifizierungsmöglichkeiten habe ich beim Konfigurieren eines Datenbankservers?

Als Authentifizierungsmechanismus wird lediglich die SQL Server-Authentifizierung unterstützt. Andere Optionen wie z.B. die Windows-Authentifizierung stehen Ihnen nicht zur Verfügung.

### 1.5.14. Welche Jobs werden verarbeitet, wenn ich ein Profil für die regelbasierte Archivierung ändere?

Wenn Sie Profile für das regelbasierte Archivieren verändern, werden die Änderungen beim nächsten Durchlauf von d.ecs content crawler ohne Neustart übernommen.

Jobs werden sofort mit der neuen Profilkonfiguration verarbeitet.

### 1.5.15. Welche Quelleigenschaften sind welchen Feldnamen in HCL Notes oder Microsoft Outlook zugeordnet?

In dieser Liste finden Sie Informationen zu den Quelleigenschaften zum Erstellen von Zuordnungen. Sie können anhand der Liste nachvollziehen, welche Quelleigenschaften welchen Feldnamen in Microsoft Outlook und HCL Notes zugeordnet sind.

#### Alle Empfängernamen (An, Cc, Bcc)

- HCL Notes: Berechneter Wert
- Microsoft Outlook: Berechneter Wert
- Bedeutung: Liste aller Empfänger (An, CC und BCC) als Anzeigename (wenn vorhanden)

#### SMTP-Adressen von allen Empfängern (An, Cc, Bcc)

- HCL Notes: Berechneter Wert
- Microsoft Outlook: **RecipientTable**
- Bedeutung: Liste aller Empfänger (An, CC und BCC) als E-Mail-Adressen (wenn vorhanden). Wenn in Domino Directory die Internet-E-Mail-Adresse nicht vorhanden ist, wird der Wert aus der E-Mail verwendet.

#### Textkörper

- HCL Notes: **Body**
- Microsoft Outlook: **PR-BODY**
- Bedeutung: Definierter Textinhalt aus dem E-Mail-Inhalt. Bei verschlüsselten E-Mails kann der Textinhalt nicht gelesen werden und wird daher leer übermittelt. Bei verschlüsselten E-Mails kann der Text nicht ausgelesen werden. Eine Zuordnung wird deswegen immer zu einem leeren Wert führen.

#### Erstellt am

- HCL Notes: Dokumenteigenschaft **Created**
- Microsoft Outlook: **PR\_CREATION\_TIME**
- Bedeutung: Erstelldatum der E-Mail

#### Erhalten am

- HCL Notes: **DeliveredDate**
- Microsoft Outlook: **PR\_MESSAGE\_DELIVERY\_TIME**
- Bedeutung: Zustelldatum der E-Mail

#### Zeitpunkt der letzten Änderung

- HCL Notes: **\$Revisions**
- Microsoft Outlook: **PR\_LAST\_MODIFICATION\_TIME**
- Bedeutung: Datum der letzten Änderung der E-Mail

#### Nachrichten-ID

- HCL Notes: **\$MessageID**
- Microsoft Outlook: **PR\_INTERNET\_MESSAGE\_ID**
- Bedeutung: Eindeutige Message-ID der E-Mail

#### Nachrichtengröße in Bytes

- HCL Notes: Berechneter Wert
- Microsoft Outlook: **Size**
- Bedeutung: Größe der E-Mail

### Empfängernamen

- HCL Notes: **SendTo**
- Microsoft Outlook: Berechneter Wert
- Bedeutung: Liste der Empfänger als Anzeigename (wenn vorhanden)

### SMTP-Adressen der Empfänger

- HCL Notes: **SendTo**
- Microsoft Outlook: Berechneter Wert
- Bedeutung: Liste der Empfänger als E-Mail-Adressen

### Empfängernamen (Bcc)

- HCL Notes: **BlindCopyTo**
- Microsoft Outlook: **RecipientTable**
- Bedeutung: Liste der Blindkopie-Empfänger als Anzeigenamen (wenn vorhanden)

### SMTP-Adressen der Empfänger (Cc)

- HCL Notes: **CopyTo**
- Microsoft Outlook: **RecipientTable**
- Bedeutung: Liste der Kopie-Empfänger als E-Mail-Adressen

### Alle SMTP-Adressen (Von, An, Cc, Bcc)

- HCL Notes: Berechneter Wert
- Microsoft Outlook: **RecipientTable**
- Bedeutung: Liste aller SMTP-Adressen

### Absendername

- HCL Notes: **From**
- Microsoft Outlook: **PR\_SENDER\_NAME**
- Bedeutung: Name des Absenders

### SMTP-Adresse des Absenders

- HCL Notes: **From**
- Microsoft Outlook: **PR\_SENDER\_EMAIL\_ADDRESS**
- Bedeutung: SMTP-Adresse des Absenders

### Betreff

- HCL Notes: **Subject**
- Microsoft Outlook: **PR\_SUBJECT**
- Bedeutung: Betreffzeile der E-Mail

### Gesendet am

- HCL Notes: **PostedDate**
- Microsoft Outlook: **PR\_CLIENT\_SUBMIT\_TIME**
- Bedeutung: Versanddatum der E-Mail

### Anzahl der Anlagen

- HCL Notes: Berechneter Wert
- Microsoft Outlook: Berechneter Wert

- Bedeutung: Anzahl der Anlagen

#### Gesendet im Auftrag von (SMTP-Adresse)

- Microsoft Outlook: **PR\_RCVD\_REPRESENTING**
- Bedeutung: SMTP-Adresse des stellvertretenden Absenders

#### Gesendet im Auftrag von (Name)

- Microsoft Outlook: **PR\_RECEIVED\_BY**
- Bedeutung: Name des stellvertretenden Absenders

#### Zeitpunkt (empfangen/gesendet/erstellt)

- HCL Notes: Berechneter Wert
- Microsoft Outlook: Berechneter Wert
- Bedeutung: Zustelldatum (Delivery) (wenn vorhanden). Wenn das Zustelldatum nicht vorhanden ist, wird entweder das Absendedatum (Submit) oder das Erzeugungsdatum (Create) verwendet. Das Erzeugungsdatum ist immer vorhanden.

#### Postfach-ID

- Microsoft Outlook: **MBADGUID**
- Bedeutung: Postfach-ID im Active Directory. Die Postfach-ID kann z.B. für die Berechtigungssteuerung verwendet werden.

#### Postfachname

- Microsoft Outlook: Berechneter Wert
- Bedeutung: Name des Microsoft Exchange-Postfachs (standardmäßig die SMTP-Adresse)

#### Ordnername (letzte Ebene)

- HCL Notes: Berechneter Wert
- Microsoft Outlook: Berechneter Wert
- Bedeutung: Ordner, in dem sich die E-Mail befindet. Bei HCL Notes-E-Mails kann der Ordnerpfad nur ermittelt werden, wenn die Ordnerreferenzen in der Maildatenbank aktiviert wurden und die E-Mail nach dem Aktivieren erhalten oder verschoben wurde. Verwenden Sie bei der Zuordnung von Ordnernamen keine Backslashes (\). Backslashes werden für die Zuordnung von **Ordnerpfad (gesplittet)** benötigt.

#### Ordnerpfad

- HCL Notes: **\$FolderRefs**
- Microsoft Outlook: **PR\_FOLDER\_PATH**
- Bedeutung: Kompletter Ordnerpfad, in dem sich die E-Mail befindet.

#### Ordnerpfad (gesplittet)

- HCL Notes: Berechneter Wert
- Microsoft Outlook: Berechneter Wert
- Bedeutung: Liste der Ordner, berechnet aus dem Ordnerpfad, in dem sich die E-Mail befindet.

Für Anlagen:

#### Dateiname

- HCL Notes: Berechneter Wert

- Microsoft Outlook: **PR\_ATTACH\_FILENAME**
- Bedeutung: Originaldateiname der Anlage

#### Dateigröße in Bytes

- HCL Notes: Berechneter Wert
- Microsoft Outlook: **PR\_ATTACH\_SIZE**
- Bedeutung: Größe der Datei in Bytes

#### Dateierweiterung

- HCL Notes: Berechneter Wert
- Microsoft Outlook: **PR\_ATTACH\_EXTENSION**
- Bedeutung: Erweiterung der Datei

Für die Benutzerinformationen wählen Sie mit dem Anzeigenamen **Postfach-SAM-Accountname** den Anmeldename des Windows-Benutzer aus, der dem Postfach zugeordnet ist. Der SAM-Accountname kann nur ermittelt werden, wenn Sie ein Active Directory in d.ecs identity provider konfiguriert haben. Darüber hinaus müssen Sie mithilfe der SMTP-Adresse des Postfachs einen Benutzer bestimmen, was bei Microsoft Office 365 in manchen Fällen nicht möglich ist.

### 1.5.16. Wie archiviere ich PST-Dateien regelbasiert?

Das Verarbeiten von PST-Dateien wird von d.ecs content crawler indirekt unterstützt. Wir empfehlen, eine PST-Datei in ein In-Situ-Archiv zu importieren. Orientieren Sie sich am von Microsoft vorgesehenen Weg. Sie können das In-Situ-Archiv mit d.ecs content crawler archivieren.

Um ein In-Situ-Archiv zu archivieren, müssen Sie als Quelle einer Quellensammlung **Microsoft Exchange In-Situ-Archiv** auswählen und das zu verarbeitende Postfach angeben. Die weitere Verarbeitung entspricht der Verarbeitung von anderen Quellentypen. Sie können alle Regeln und Verarbeitungsschritte an Ihre Bedürfnisse anpassen.

Weitere Informationen zu In-Situ-Archiven finden Sie auf der Microsoft Docs-Website in der Exchange Server 2019-Dokumentation unter "In-Place-Archivierung in Exchange Server".

Weitere Informationen zum Importieren von PST-Dateien finden Sie auf der Microsoft Docs-Website in der Exchange Server 2019-Dokumentation unter "Verfahren für Postfach Importe aus PST-Dateien in Exchange Server".

### 1.5.17. Wie archiviere ich rechtskonform mit Microsoft Exchange Online ohne ein externes Postfach?

Wenn Sie mit Microsoft Exchange Online rechtskonform ohne externes Postfach archivieren möchten, können Sie beim regelbasierten Archivieren in d.ecs content crawler die Option **Archivieren von gelöschten Elementen** aktivieren. In diesem Fall benötigen Sie das Lösungspaket `db | mailbox archiver`.

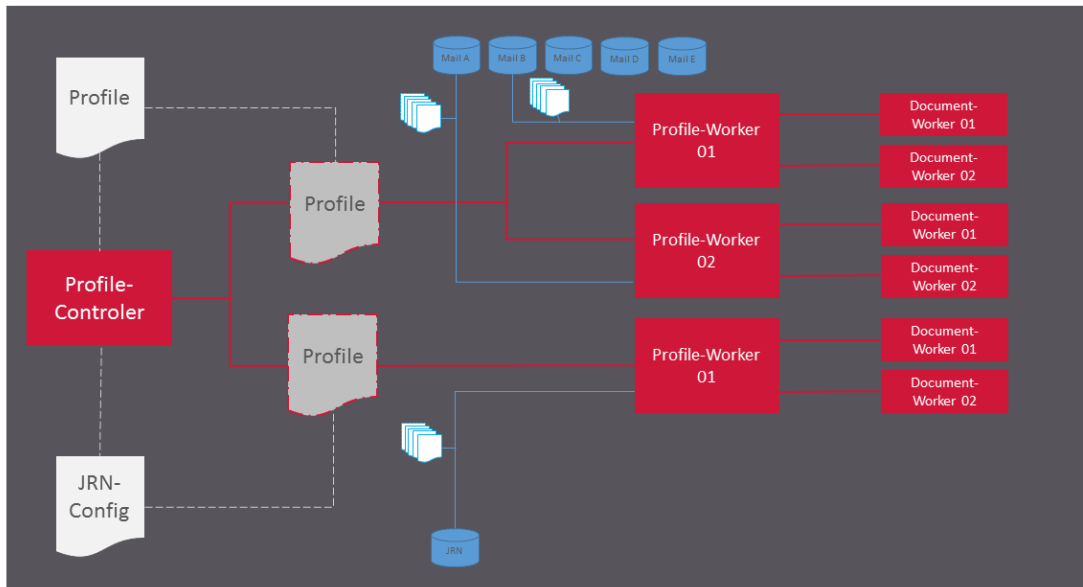
### 1.5.18. Wie kann eine d.ecs content crawler-Konfiguration aufgebaut sein? (Anwendungsbeispiel)

Sie können die Konfiguration von d.ecs content crawler für das regelbasierte Archivieren von Elementen und die Journalarchivierung an Ihre Bedürfnisse anpassen.

#### Beispiel

Ein Kunde möchte fünf Postfächer regelbasiert in einem d.3-Repository archivieren. Darüber hinaus möchte der Kunde die Journalarchivierung für ein Journal-Postfach verwenden.

Anhand des folgenden Schaubilds können Sie nachvollziehen, wie die Beispielkonfiguration aussehen kann:



d.velop

Der Administrator erstellt eine Zuordnung für die Eigenschaften der zu archivierenden E-Mails und bestimmten d.3-Eigenschaften. Darüber hinaus erstellt der Administrator ein Profil für das regelbasierte Archivieren und eine Konfiguration für die Journalarchivierung.

Für die Journalarchivierung wird innerhalb von d.ecs content crawler ein Profile-Worker erstellt. Für den Profile-Worker werden zwei Document-Worker erstellt. Der Profile-Worker verarbeitet das Journalpostfach.

Für das Profil zum regelbasierten Archivieren werden zwei Profile-Worker erstellt. Je Profile-Worker werden zwei Document-Worker erstellt. Die Profile-Worker verarbeiten die fünf Postfächer basierend auf den Regeln des erstellten Profils.

Je Durchlauf werden 100 Dokumente verarbeitet, die gleichmäßig auf die Document-Worker verteilt werden. Die Document-Worker speichern basierend auf der Zuordnung die Dokumente im d.3-Repository mit den entsprechenden Eigenschaften.

### 1.5.19. Wie kann ich d.ecs content crawler ohne d.3one-Anwendungsserver verwenden?

Sie können d.ecs content crawler auch ohne einen d.3one-Anwendungsserver verwenden. In diesem Fall werden die Elemente in das Dateisystem exportiert. In diesem Modus haben Sie Zugriff auf das komplette Regelwerk.

Um diesen Modus verwenden zu können, müssen Sie trotzdem die d.velop-Infrastrukturkomponenten installieren.

Folgende Einschränkungen gelten für diesen Modus:

- Das Speichern von Elementen in ein d.3-Repository ist nicht möglich.
- Beim Speichern von Elementen in ein d.3-Repository ist das Ersetzen von Anlagen durch Links nicht möglich.
- Bei der Nachverarbeitung von Elementen ist nur das komplette Löschen des Elements möglich.

### 1.5.20. Wie kann ich Detailinformationen zu Jobs anzeigen und filtern?

Sie können im Feature d.ecs content crawler im Bereich **Statistikübersicht** Informationen über Ihre Jobs anzeigen. Wenn Sie die auf die Zahl der Jobs im entsprechenden Status klicken, erhalten Sie unter

**Jobübersicht** genauere Informationen zu den entsprechenden Jobs im jeweiligen Status. Sie können die Jobs bei Bedarf filtern.

Im Bereich **Gesamtstatus** können Sie Informationen z.B. zu ausstehenden Jobs oder seit dem letzten Neustart fertiggestellten Jobs anzeigen.

Im Bereich **Profilstatus** können Sie eine Auswertung pro Profil anzeigen.

### 1.5.21. Wie kann ich regelbasiert das Verknüpfen von eingebetteten Anlagen festlegen, wenn ich HCL Domino verwende?

Wenn Sie HCL Domino verwenden und die Nachbearbeitungsaktion **Anhänge und eingebettete Dateien verknüpfen** für eine Verarbeitungsschrittsammlung verwenden möchten, werden in diesem Fall keine eingebetteten Dateien durch HTTP-Links ersetzt. Diese Nachbearbeitungsaktion wird nur für reguläre Anlagen unterstützt.

### 1.5.22. Wie konfiguriere ich eine E-Mail-Archivierung für unterschiedliche Domänen?

Wenn Sie die E-Mail-Archivierung für unterschiedliche Domänen in Ihrer Organisation konfigurieren, empfehlen wir einen eigenen d.3one-Anwendungsserver für die Verarbeitung je Domäne.

### 1.5.23. Wie konfiguriere ich eine externe Regelprüfung?

In kundenspezifischen Einzelfällen reichen die Standardregeln von d.ecs content crawler eventuell nicht aus, um ein Objekt zu prüfen und für das Weiterverarbeiten zu markieren. In diesem Fall können Sie die externe Regelprüfung verwenden. Sie können mithilfe einer einfachen HTTP-Schnittstelle individuelle Regeln erstellen, um ein Objekt beliebig detailliert zu prüfen.

#### Warnung

Sie können mit d.ecs content crawler bei der Regelauswertung ein externes Skript verwenden. Die d.velop AG übernimmt keinerlei Haftung und Gewährleistung für das aufgerufene Skript und/oder die Ergebnisse, die durch die Ausführung des Skripts entstehen können.

Die externe Regelprüfung muss eine Anwendung sein, die HTTP-Aufrufe entgegennehmen, auswerten und senden kann.

Der Ablauf einer externen Regelprüfung sieht wie folgt aus:

1. d.ecs content crawler erstellt bereits Jobs und ermittelt Objekte. d.ecs content crawler überträgt die Jobs und Objekte an die externe Regelprüfung.
2. Die externe Regelprüfung nimmt die HTTP-Aufrufe entgegen und sendet eine Bestätigung zurück.
3. Bestätigte Jobs werden in einen Wartezustand versetzt. Fehler werden ebenfalls entsprechend markiert.
4. Die externe Regelprüfung führt die Regeln für die Objekte aus und meldet das Ergebnis mithilfe der entsprechenden Rückrufe an d.ecs content crawler zurück.
5. Wenn eine Rückmeldung erfolgt, wird der entsprechende Job markiert und mit dem nächsten Durchlauf weiterverarbeitet oder die Verarbeitung wird abgebrochen.

Die Kommunikation erfolgt ausschließlich mit HTTP-POST-Aufrufen. Daten werden als **application/json** übermittelt.

Im Folgenden finden Sie weitere wichtige Informationen zum Aufbau der HTTP-Aufrufe und der zu übermittelnden Daten für die externe Regelprüfung.

#### POST-Daten für die Übertragung von d.ecs content crawler an die externe Regelprüfung

```
{
  "uri": "http://server.domain.com:2000/",
```

```

"groupwareItemIdentifizier": null,
"jobId": null,
"successCallback": null,
"errorCallback": null,
"isTest": true
}

```

- **uri**: Die URI der externen Regelprüfung.
- **groupwareItemIdentifizier**: Die ID des Objekts, das an die externe Regelprüfung übermittelt wird. Die IDs für HCL Domino-Objekte und Microsoft Exchange-Objekte sind unterschiedlich.
- **jobId**: Die ID des Jobs, der an die externe Regelprüfung übermittelt wird.
- **successCallback**: Die URI des Rückrufs bei einem Erfolg. Der Rückruf muss aufgerufen werden, wenn die externe Regelprüfung erfolgreich abgeschlossen wurde.
- **errorCallback**: Die URI des Rückrufs bei einem Fehler. Der Rückruf muss aufgerufen werden, wenn bei der externen Regelprüfung ein Fehler aufgetreten ist, der eine Weiterverarbeitung verhindert. Der Rückruf soll im Job protokolliert werden.
- **isTest**: Beim Wert **true** dienen die übermittelten Daten lediglich dem Verbindungstest. Beim Wert **false** gehören die Daten zu einem Job und werden verarbeitet. Da der Wert **false** der Standardwert ist, können Sie den Wert auch auslassen.

### GroupwareItemIdentifizier (HCL Domino)

```

{
  "type": "DOMINO",
  "server": "dominoserver/domain",
  "database": "mail/mailuser.nsf",
  "replicaId": "C1257CB700273AAF",
  "noteId": "39CA",
  "universalId": "84A717A82EDD701DC12580ED0051F49D",
  "attachmentIdentifizier": null
}

```

- **type**: Legt fest, ob ein Objekt einem HCL Domino-System oder einem Microsoft Exchange-System angehört.
- **server**: Der Name des HCL Domino Servers, auf dem sich die Datenbank und das Objekt befinden. Verwenden Sie die übliche Kurzschreibweise **<Server>/<Domäne>**.
- **database**: Der Pfadname und Dateiname der Datenbank, in der das Objekt enthalten ist. Die Angaben sind immer relativ zum Data-Verzeichnis des HCL Domino Servers.
- **replicaId**: Die Replikant-ID der Datenbank.
- **noteId**: Die Note-ID des Objekts innerhalb der Datenbank.
- **universalId**: Die Universal-ID des Objekts innerhalb der Datenbank.
- **attachmentIdentifizier**: Wenn Sie diesen Eintrag füllen, wird mit diesem Eintrag ein Attachment innerhalb eines Objekts identifiziert. Da dieser Eintrag in d.ecs content crawler nicht angewendet wird, ist der Wert immer **null**.

### GroupwareItemIdentifizier (Microsoft Exchange)

```

{
  "type": "EXCHANGE",
  "exchangeStoreType": 0,
  "mailbox": "ttes@so.training",
  "parentFolderId": null,
  "entryId":
"AAMkADQyMzc0YTZmLWIyM2QtNDFkOC04MDJhLWRmZDUxMTAxMDMyZQBGAIAAAAZMnZybIySRbt
8MxDtMGQbBwCUhE5mmOtWRbVwYoiZpwRcAAAAZwNIAAAhPwfg1f9rTqKq29vpQTqcAAATGKY5AAA
="

```

```

    "attachmentId": -1,
    "entryIdFormat": 1,
    "isDeletedElement": false
  }

```

- **type:** Legt fest, ob ein Objekt einem HCL Domino-System oder einem Microsoft Exchange-System angehört.
- **exchangeStoreType:** Der Typ des Postfachs. Beim Wert **0** handelt es sich um das primäre Postfach des Benutzers. Beim Wert **1** handelt es sich um das Archiv-Postfach des Benutzers. Beim Wert **2** handelt es sich um den öffentlichen Ordner.
- **mailbox:** Das Postfach, in dem das Objekt enthalten ist. Das Format ist die SMTP-Adresse.
- **parentFolderId:** Die ID des Ordners, in dem das Objekt enthalten ist.
- **entryId:** Die ID des Objektes innerhalb des Postfachs.
- **attachmentId:** Wenn Sie diesen Eintrag füllen, wird mit diesem Eintrag ein Attachment innerhalb eines Objekts identifiziert. Da dieser Eintrag in d.ecs content crawler nicht angewendet wird, ist der Wert immer **-1**.
- **entryIdFormat:** Das Format der Eintrags-ID. Beim Wert **0** handelt es sich um das MAPI-Format. Beim Wert **1** handelt es sich um das EWS-Format. Mithilfe der Exchange-Webdienste können Eintrags-IDs im MAPI-Format in das EWS-Format umgewandelt werden.
- **isDeletedElement:** Gibt an, ob das Objekt im Ordner **Recoverable Items** enthalten ist. Standardmäßig ist das irrelevant.

#### POST-Daten für die Übertragung der externen Regelprüfung an d.ecs content crawler

```

{
  "uri": "http://server.domain.com:2000/",
  "groupwareItemIdentifier":
  "{ \"type\": \"DOMINO\", \"server\": \"dominoserver/
domain\", \"database\": \"mail/
mailuser.nsf\", \"replicaId\": \"C1257CB700273AAF\", \"noteId\": \"39CA\", \"universaId\": \"84A717A82EDD701DC12580ED0051F49D\", \"attachmentIdentifier\": null
} ",
  "jobId": "dfd1a0ef-bbee-477a-936f-d43342abfe75",
  "status": 4,
  "statusMessage": "Task for externally checking job dfd1a0ef-
bbee-477a-936f-d43342abfe75 successfully created"
}

```

- **uri:** Die URI der externen Regelprüfung.
- **groupwareItemIdentifier:** Die ID des Objekts, das an die externe Regelprüfung übermittelt wird. Die IDs für HCL Domino-Objekte und Microsoft Exchange-Objekte sind unterschiedlich.
- **jobId:** Die ID des Jobs, der an die externe Regelprüfung übermittelt wird.
- **status:** Der Status, den die externe Regelprüfung an d.ecs content crawler zurückmeldet. Folgende Werte sind möglich:
  - **0 Unknown:** Diesen Wert dürfen Sie nicht verwenden. Der Wert dient der internen Prüfung.
  - **1 Continue:** Dieser Wert gibt an, dass die Weiterverarbeitung des Jobs durch d.ecs content crawler erfolgen kann.
  - **2 Abort:** Dieser Wert gibt an, dass die Weiterverarbeitung des Jobs durch d.ecs content crawler abgebrochen werden soll und dass das Objekt zurückgesetzt werden soll.
  - **3 Error:** Dieser Wert gibt an, dass ein Fehler bei der externen Regelprüfung aufgetreten ist.
  - **4 Received:** Dieser Wert gibt an, dass die externe Regelprüfung die Daten von d.ecs content crawler entgegengenommen hat und auf Rückmeldung der externen Regelprüfung wartet.
  - **999 TestSuccess:** Dieser Wert wird für den Verbindungstest benötigt und gibt an, dass eine Verbindung zur externen Regelprüfung erfolgreich aufgebaut wurde.
- **statusMessage:** Eine optionale Meldung, die in der Übersicht der Jobs von d.ecs content crawler angezeigt wird. Insbesondere im Fehlerfall sollten Sie einen Wert angeben.

Wenn ein Objekt durch eine externe Regel nicht verarbeitet wird, muss das Objekt ein entsprechendes Flag erhalten und in einen Ordner verschoben werden, der nicht überwacht wird. Bei der nächsten Verarbeitung durch d.ecs content crawler wird dieses Objekt nicht erneut verarbeitet.

In Microsoft Exchange müssen Sie die benannte Eigenschaft **DXJOB** (Typ: **PT\_UNICODE**) mit dem Wert **SCP** füllen.

In HCL Domino müssen Sie das Feld **D3IMPORT** (Typ: **Text**) mit dem Wert **SCP** füllen.

### 1.5.24. Wie konfiguriere ich eine externe Regelprüfung mit d.ecs script?

In kundenspezifischen Einzelfällen kann es vorkommen, dass zusätzlich zu den Standardregeln von d.ecs content crawler Regeln benötigt werden, um ein Objekt zu prüfen und für das Weiterverarbeiten zu markieren. In diesem Fall können Sie d.ecs script verwenden. In d.ecs script können Sie für Ihren Anwendungsfall eigene Skripte erstellen.

Der Ablauf einer externen Regelprüfung sieht wie folgt aus:

1. d.ecs content crawler erstellt bereits Jobs und ermittelt Objekte. d.ecs content crawler überträgt die Jobs und Objekte an d.ecs script.
2. d.ecs script führt das Skript aus, das im Regelwerk von d.ecs content crawler angegeben ist. In dem Skript muss als Ergebnis eine Rückmeldung darüber erfolgen, ob das entsprechende Objekt verarbeitet werden soll.
3. Wenn eine Rückmeldung erfolgt, wird der entsprechende Job markiert und mit dem nächsten Durchlauf weiterverarbeitet oder die Verarbeitung wird abgebrochen.

Im Folgenden finden Sie weitere wichtige Informationen zum Aufbau der HTTP-Aufrufe und der zu übermittelnden Daten für die externe Regelprüfung mit d.ecs script.

Folgendes Objekt wird von d.ecs content crawler im JSON-Format an d.ecs script übermittelt und kann in einem Skript zur Regelprüfung verwendet werden:

```
{
  "GroupwareItemIdentifizier" : null,
  "JobId" : null,
  "Status" : 0,
  "StatusMessage" : null
}
```

- **GroupwareItemIdentifizier:** Die ID des Objekts, das an d.ecs script übermittelt wird. Die Regelprüfung muss das Objekt ermitteln und bereitstellen. Die IDs für HCL Domino-Objekte und Microsoft Exchange-Objekte sind unterschiedlich.
- **JobId:** Die ID des Jobs, der an d.ecs script übermittelt wird.
- **Status:** Der Status, der mithilfe der weiteren Verarbeitung das Objekt bestimmt. Sie müssen den Status im Skript festlegen. Folgende Werte sind möglich:
  - **1 Continue:** Dieser Wert gibt an, dass die Weiterverarbeitung des Jobs durch d.ecs content crawler erfolgen kann.
  - **2 Abort:** Dieser Wert gibt an, dass die Weiterverarbeitung des Jobs durch d.ecs content crawler abgebrochen werden soll und dass das Objekt zurückgesetzt werden soll.
  - **3 Error:** Dieser Wert gibt an, dass ein Fehler im Skript aufgetreten ist.
  - **4 Deleted:** Dieser Wert gibt an, dass das Objekt im Skript gelöscht wurde. Der Job wird ebenfalls direkt gelöscht.
- **StatusMessage:** Eine optionale Meldung, die in der Jobs-Übersicht von d.ecs content crawler angezeigt wird. Sie können die Meldung im Skript festlegen, um nähere Informationen zum Status mitzuteilen.

#### GroupwareItemIdentifizier (HCL Domino)

```
{
  "type": "DOMINO",
```

```

"server": "dominoserver/domain",
"database": "mail/mailuser.nsf",
"replicaId": "C1257CB700273AAF",
"noteId": "39CA",
"universalId": "84A717A82EDD701DC12580ED0051F49D",
"attachmentIdentifier": null
}

```

- **type:** Legt fest, ob ein Objekt einem HCL Domino-System oder einem Microsoft Exchange-System angehört.
- **server:** Der Name des HCL Domino Servers, auf dem sich die Datenbank und das Objekt befinden. Verwenden Sie die übliche Kurzschreibweise **<Server>/<Domäne>**.
- **database:** Der Pfadname und Dateiname der Datenbank, in der das Objekt enthalten ist. Die Angaben sind immer relativ zum Data-Verzeichnis des HCL Domino Servers.
- **replicaId:** Die Replik-ID der Datenbank.
- **noteId:** Die Note-ID des Objekts innerhalb der Datenbank.
- **universalId:** Die Universal-ID des Objekts innerhalb der Datenbank.
- **attachmentIdentifier:** Wenn Sie diesen Eintrag füllen, wird mit diesem Eintrag ein Attachment innerhalb eines Objekts identifiziert. Da dieser Eintrag in d.ecs content crawler nicht angewendet wird, ist der Wert immer **null**.

#### GroupwareItemIdentifier (Microsoft Exchange)

```

{
  "type": "EXCHANGE",
  "exchangeStoreType": 0,
  "mailbox": "ttes@so.training",
  "parentFolderId": null,
  "entryId":
"AAMkADQyMzc0YTZmLWIyM2QtNDFkOC04MDJhLWRmZDUxMTAxMDMyZQBGAZMnZybiYSRbt
8MxDtMGQbBwCUhE5mmOtWRbVwYoiZpwRcAAAAZwNIAAAhPwfg1f9rTqKq29vpQTqcAAATGKY5AAA
=",
  "attachmentId": -1,
  "entryIdFormat": 1,
  "isDeletedElement": false
}

```

- **type:** Legt fest, ob ein Objekt einem HCL Domino-System oder einem Microsoft Exchange-System angehört.
- **exchangeStoreType:** Der Typ des Postfachs. Beim Wert **0** handelt es sich um das primäre Postfach des Benutzers. Beim Wert **1** handelt es sich um das Archiv-Postfach des Benutzers. Beim Wert **2** handelt es sich um den öffentlichen Ordner.
- **mailbox:** Das Postfach, in dem das Objekt enthalten ist. Das Format ist die SMTP-Adresse.
- **parentFolderId:** Die ID des Ordners, in dem das Objekt enthalten ist.
- **entryId:** Die ID des Objektes innerhalb des Postfachs.
- **attachmentId:** Wenn Sie diesen Eintrag füllen, wird mit diesem Eintrag ein Attachment innerhalb eines Objekts identifiziert. Da dieser Eintrag in d.ecs content crawler nicht angewendet wird, ist der Wert immer **-1**.
- **entryIdFormat:** Das Format der Eintrags-ID. Beim Wert **0** handelt es sich um das MAPI-Format. Beim Wert **1** handelt es sich um das EWS-Format. Mithilfe der Exchange-Webdienste können Eintrags-IDs im MAPI-Format in das EWS-Format umgewandelt werden.
- **isDeletedElement:** Gibt an, ob das Objekt im Ordner **Recoverable Items** enthalten ist. Standardmäßig ist das irrelevant.

#### Beispielskript (alle Objekte verarbeiten)

```
param([string]$scriptDto)

$dto = $scriptDto | ConvertFrom-Json

$dto.Status = 1

$obj = @{ }

$obj.ReturnCode = 0
$obj.ScriptDto = $dto | ConvertTo-Json

return $ResultObj = (New-Object PSObject -Property $obj)
```

Wenn ein Objekt durch eine externe Regel nicht verarbeitet wird, muss das Objekt ein entsprechendes Flag erhalten und in einen Ordner verschoben werden, der nicht überwacht wird. Bei der nächsten Verarbeitung durch d.ecs content crawler wird dieses Objekt nicht erneut verarbeitet.

In Microsoft Exchange müssen Sie die benannte Eigenschaft **DXJOB** (Typ: **PT\_UNICODE**) mit dem Wert **SCP** füllen.

In HCL Domino müssen Sie das Feld **D3IMPORT** (Typ: **Text**) mit dem Wert **SCP** füllen.

### 1.5.25. Wie öffne ich die Konfiguration der Anbindung für Microsoft Exchange oder HCL Domino?

Sie können die Konfiguration der Anbindung für Microsoft Exchange oder HCL Domino unter <Basisadresse>/groupware aufrufen.

### 1.5.26. Wie öffne ich die Konfiguration von d.ecs content crawler, wenn das Feature auf der Startseite nicht angezeigt wird?

Wenn Ihnen das Feature **d.ecs content crawler** auf der Startseite nicht zur Verfügung steht, können Sie die Konfiguration unter <Basisadresse>/groupwarecrawler aufrufen.

### 1.5.27. Wie prüfe ich Duplikate von verschlüsselten oder signierten E-Mails?

Für verschlüsselte E-Mails wird kein Prüfen von Duplikaten durchgeführt.

### 1.5.28. Wie prüfe ich nach dem Verknüpfen von Zertifikat und Port, ob sich die Apps bei d.ecs http gateway mit HTTPS registrieren?

Wenn Sie zum Verschlüsseln der Kommunikation der Apps ein Zertifikat mit einem Port verknüpft haben, können Sie in der Administration von d.ecs http gateway prüfen, wie sich die Apps bei der d.ecs http gateway-App registrieren.

#### So geht's

1. Rufen Sie die Administration der d.ecs http gateway-App mit **https://<Computername>:4280/httpgateway/ui** auf oder wählen Sie im Windows-Startmenü in der d.velop-Programmgruppe den Eintrag **d.ecs http gateway admin** aus.
2. Klicken Sie im Bereich **Apps** auf die entsprechende App.
3. Klicken Sie auf die entsprechende App, um die Eigenschaften der App anzuzeigen.
4. Prüfen Sie unter **Destination URL**, ob die URL mit HTTPS beginnt.

Siehe auch: [Verknüpfen von Zertifikat und Port für die Inter-App-Kommunikation mit HTTPS](#)

### 1.5.29. Wie verhindere ich, dass verschlüsselte E-Mails archiviert werden?

Sie können verschlüsselte E-Mails vom automatischen Archivieren ausschließen. Fügen Sie die entsprechende Regel einer Regelsammlung hinzu.

### Anmerkung

Die Anlagen einer verschlüsselten E-Mail können nicht von der E-Mail losgelöst werden, auch wenn Sie in der Verarbeitungsschrittsammlung die Nachbearbeitungsoption **Anhänge verknüpfen** aktiviert haben. Die verschlüsselte E-Mail wird komplett mit Anlagen archiviert.

### 1.5.30. Wie verschiebe ich Datenbankeinträge zu Jobs manuell, wenn die Jobs nach dem Ändern meiner Datenbank noch vorhanden sind?

Wenn Sie beim Konfigurieren des Datenbankservers Änderungen an Ihrer verwendeten Datenbank vorgenommen haben, sind die Jobs eventuell noch in der Datenbank vorhanden. In diesem Fall müssen Sie die Datenbankeinträge manuell verschieben.

Beenden Sie d.ecs content crawler. Im Anschluss können Sie alle Tabellen mit dem Präfix **GWCR\_** in die neue Datenbank verschieben.

Siehe auch: [Konfigurieren des Datenbankservers](#)

### 1.5.31. Wie werden E-Mails ohne Jobs von d.ecs content crawler verarbeitet?

E-Mails im Status **Prepared-Rule** oder **Error** ohne dazugehörigen Job werden automatisch zurückgesetzt, um erneut verarbeitet zu werden. Zuvor wird geprüft, ob die E-Mails verschoben wurden.

### 1.5.32. Wie werden E-Mails von d.ecs content crawler verarbeitet, wenn die E-Mails verschoben wurden?

Wenn E-Mails während der Verarbeitung verschoben werden, erhalten die E-Mails in Microsoft Exchange Server eine neue ID. d.ecs content crawler meldet, dass das Element nicht gefunden werden kann. Der dazugehörige Job wird als Fehler gewertet (Fehlernummer 40).

In einem asynchronen Prozess wird zyklisch nach Jobs mit der Fehlernummer 40 gesucht und versucht, die dazugehörige E-Mail zu finden. Wenn die E-Mail gefunden wird, wird der Job korrigiert, zurückgesetzt und das Element wird verarbeitet. Wenn das Element nicht gefunden wird, wird der Job gelöscht.

### 1.5.33. Wozu dient die Protokollierung?

Für die Protokollierung schreibt die d.3one-Integration in das zentrale d.3-Log. Wenn ein Fehler auftritt, werden alle erforderlichen Informationen protokolliert, damit Sie die Fehlerursache schnell identifizieren können.

Standardmäßig protokolliert die Integration nur Fehler. Wenn Sie weitere Informationen benötigen, können Sie den Protokollierungsgrad an Ihre Bedürfnisse anpassen.

Siehe auch: [Anpassen des Protokollierungsgrads in d.ecs content crawler](#)

### 1.5.34. Wie ordne ich eine d.3-Repository-ID einer Repository-ID zu?

Wenn Sie mehrere Repositories konfiguriert haben, die dieselbe d.3-Repository-ID haben, können Sie bei Bedarf in der Groupware-App eine d.3-Repository-ID einer Repository-ID zuordnen.

#### So geht's

1. Öffnen Sie das Feature **Konfiguration** auf der Startseite und navigieren Sie in der Kategorie **Dokumentenmanagement** zu **E-Mails**.
2. Wählen Sie unter **E-Mail-Verwaltung** den Eintrag **Verwaltungsoptionen** aus.
3. Wechseln Sie in die Perspektive **Repositoryzuordnung**.
4. Geben Sie die entsprechende d.3-Repository-ID ein.
5. Wählen Sie die Repository-ID aus, die Sie der d.3-Repository-ID zuordnen möchten.
6. Klicken Sie auf **Hinzufügen** und speichern Sie Ihre Angaben.

### 1.5.35. Wie setze ich den Zähler für Jobs zurück?

Sie können im Feature **d.ecs content crawler** im Bereich **Statistikübersicht** Informationen über Ihre Jobs und die erstellten Profile anzeigen. Im Kontextmenü eines Profils können Sie mit **Statistik zurücksetzen** die Anzahl erfolgreich verarbeiteter Jobs zurücksetzen.

### 1.5.36. Was sind priorisierte Profile und wie verwende ich sie?

Sie können Profilen eine Priorität zuordnen, damit sie schneller verarbeitet werden.

Ein priorisiertes Profil kann Ihnen helfen, wenn Sie z.B. viele Profile zur Massenarchivierung und wenige zeitkritische Profile zur Verarbeitung von Eingangsrechnungen haben. Aufgrund der hohen Last werden zunächst die Profile zur Massenarchivierung verarbeitet. Daher kann es vorkommen, dass zeitkritische E-Mails zu spät ins System importiert werden.

Mit priorisierten Profilen können Sie sicherstellen, dass die entsprechenden Profile parallel zur regulären Profilverarbeitung verarbeitet werden und somit zeitkritische E-Mails rechtzeitig im System sind.

Standardmäßig sind Profile nicht priorisiert. Priorisieren Sie nur so viele Profile wie nötig. Wenn alle Profile zeitkritisch sind, empfehlen wir, kein Profil zu priorisieren.

## 1.6. 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.keelelearning.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>.