



ARIS Risk & Compliance Manager **INSTALLATION**

Version 9.8 - Service Release 5

Juli 2016

Dieses Dokument gilt für ARIS Risk & Compliance Manager ab Version 9.8. Hierin enthaltene Beschreibungen unterliegen Änderungen und Ergänzungen, die in nachfolgenden Release Notes oder Neuausgaben bekanntgegeben werden.

Urheberrechtlich geschützt © 2010 - 2016 [Software AG](#), Darmstadt, Deutschland und/oder Software AG USA Inc., Reston VA, USA und/oder ihre Tochtergesellschaften und/oder ihre Lizenzgeber.

Der Name Software AG und die Namen der Software AG Produkte sind Marken der Software AG und/oder Software AG USA Inc., einer ihrer Tochtergesellschaften oder ihrer Lizenzgeber. Namen anderer Gesellschaften oder Produkte können Marken ihrer jeweiligen Schutzrechtsinhaber sein. Genaue Informationen über die geschützten Marken und Patente der Software AG und ihrer Tochtergesellschaften sind veröffentlicht unter <http://softwareag.com/licenses>.

Die Nutzung dieser Software unterliegt den Lizenzbedingungen der Software AG. Diese Bedingungen sind Bestandteil der Produktdokumentation und befinden sich unter <http://softwareag.com/licenses> und/oder im Wurzelverzeichnis des lizenzierten Produkts.

Diese Software kann Teile von Software-Produkten Dritter enthalten. Urheberrechtshinweise, Lizenzbestimmungen sowie zusätzliche Rechte und Einschränkungen dieser Drittprodukte können dem Abschnitt „License Texts, Copyright Notices and Disclaimers of Third Party Products“ entnommen werden. Diese Dokumente enthalten den von den betreffenden Lizenzgebern oder den Lizenzen wörtlich vorgegebenen Wortlaut und werden daher in der jeweiligen Ursprungssprache wiedergegeben. Für einzelne, spezifische Lizenzbeschränkungen von Drittprodukten siehe PART E der Legal Notices, abrufbar unter dem Abschnitt „License Terms and Conditions for Use of Software AG Products / Copyrights and Trademark Notices of Software AG Products“. Diese Dokumente sind Teil der Produktdokumentation, die unter <http://softwareag.com/licenses> oder im Verzeichnis der lizenzierten Produkte zu finden ist.

Inhalt

1	Textkonventionen	1
2	ARIS Risk & Compliance Manager	2
3	Wichtige Informationen für die Installation des Systems	3
4	Installation von ARIS Risk & Compliance Manager mit Verwendung einer Oracle- oder Microsoft® SQL-Server-Datenbank	4
4.1	Installation der Datenbank	4
4.2	Installation des Datenbankschemas (Oracle)	5
4.3	Installation des Datenbankschemas (Microsoft® SQL-Server)	6
5	Installation und Konfiguration der Anwendung	7
5.1	Installation	8
5.2	Umstieg von der Testinstallation auf ein Produktivsystem	10
5.3	ARIS Risk & Compliance Manager in bestehende ARIS-Installation integrieren	13
5.3.1	Entfernen der nicht mehr benötigten Komponenten	14
5.3.2	Start der nicht mehr benötigten Komponenten verhindern	15
5.4	Konfigurationsparameter	16
5.5	Konfiguration der E-Mail-Funktionalität	19
5.6	Ändern der System-E-Mail-Adressen	20
6	Installation einer kundenspezifischen Version (Customizing)	21
7	Neue Version von ARIS Risk & Compliance Manager installieren	22
7.1	Datensicherung	22
7.2	Ausführung des Update-Setups	23
7.3	Datenmigration	23
7.3.1	Migration der Daten aus ARIS Dokumentablage	24
7.3.2	Migration der Datenbank von ARIS Risk & Compliance Manager	27
7.4	Importieren von modellierten Benutzer ins User Management	28
7.4.1	Modellierte Benutzer aus ARIS Architect exportieren	28
7.4.2	Modellierte Benutzer ins User Management importieren	29
7.4.3	Benutzer in ARIS Risk & Compliance Manager aktualisieren	29
7.5	Anbindung an einen Verzeichnisdienst (LDAP)	30
7.6	Kennwortverschlüsselung in der Laufzeitkonfiguration	30
7.7	Konfiguration von Event-Enabling in ARIS Risk & Compliance Manager	30

8	Installation der ARIS Architect-Komponenten	33
9	Server von MashZone für die Dashboard-Integration vorbereiten	34
10	Anbindung an ARIS Publisher.....	35
11	Häufige Fehler	38
11.1	Datenbankprobleme.....	38
12	Systemvoraussetzungen	39
12.1	Oracle-System und -Einstellungen	39
12.2	Microsoft® SQL-Server-System und -Einstellungen.....	41
12.3	Acrobat Reader	41
12.4	Microsoft Office/Excel.....	41
13	Glossar	42
14	Support von Software AG.....	43
15	Disclaimer	44
16	Index	i

1 Textkonventionen

Im Text werden Menüelemente, Dateinamen usw. folgendermaßen kenntlich gemacht:

- Menüelemente, Tastenkombinationen, Dialoge, Dateinamen, Eingaben usw. werden **fett** dargestellt.
- Eingaben, über deren Inhalt Sie entscheiden, werden **<fett und in spitzen Klammern>** dargestellt.
- Einzeilige Beispieltex te werden am Zeilenende durch das Zeichen ↵ getrennt, z. B. ein langer Verzeichnispfad, der aus Platzgründen mehrere Zeilen umfasst.
- Dateiauszüge werden in folgendem Schriftformat dargestellt:

Dieser Absatz enthält einen Dateiauszug.

2 ARIS Risk & Compliance Manager

ARIS Risk & Compliance Manager ist eine Web-Anwendung. ARIS Risk & Compliance Manager verwendet Java-Servlets und Java-Server-Pages (JSP), die neben einer Java-Umgebung (JDK) einen Web-Container, d. h. Servlet-Container (Apache-TomEE) als Ablaufumgebung benötigen. Die Daten werden in einem relationalen Datenbanksystem gehalten und durch eine JDBC-Schnittstelle mit der Anwendung ausgetauscht. Zu Testzwecken können Sie ARIS Risk & Compliance Manager mit der Datenbank **Apache Derby** verwenden. Für den Produktivbetrieb benötigen Sie das Datenbanksystem **Oracle** oder **Microsoft®-SQL-Server**.

Falls es eine aktualisierte Version dieses Dokuments gibt, finden Sie diese hier:

<http://aris.softwareag.com/ARISDownloadCenter/ADCDocumentationServer>

(<http://aris.softwareag.com/ARISDownloadCenter/ADCDocumentationServer>)

3 Wichtige Informationen für die Installation des Systems

Wenn Sie das System technisch und/oder fachlich ohne Service-Leistung der Software AG installieren möchten, benötigen Sie umfangreiche Kenntnisse hinsichtlich des zu installierenden Systems, der Zielthematik sowie der Zielsysteme und ihren Abhängigkeiten untereinander. Aufgrund der Vielzahl von Plattformen und sich gegenseitig beeinflussender Hardware- und Softwarekonfigurationen können nur spezifische Installationen beschrieben werden. Es ist nicht möglich, sämtliche Einstellungen und Abhängigkeiten zu dokumentieren.

4 Installation von ARIS Risk & Compliance Manager mit Verwendung einer Oracle- oder Microsoft® SQL-Server-Datenbank

Verwenden Sie zum produktiven Betrieb von ARIS Risk & Compliance Manager das Standarddatenbanksystem, eine Oracle- oder Microsoft® SQL-Server-Datenbank. Die Verwendung einer Derby-Datenbank ist lediglich zu Testzwecken erlaubt. Bitte beachten Sie, dass eine Produktivdatenbank neu aufgesetzt werden sollte. Verwenden Sie in Ihrem Produktivsystem bitte keine Testdaten.

BENÖTIGTE KOMPONENTEN

Zum Betrieb der Anwendung müssen folgende Komponenten installiert werden:

- Java-Umgebung
- TomEE-Server
- ARIS Risk & Compliance Manager (inklusive benötigter Applikationen wie User Management oder ARIS Dokumentablage)

Falls Oracle oder Microsoft® SQL-Server als das Standarddatenbanksystem genutzt werden soll:

- Oracle- oder Microsoft® SQL-Server-Datenbank
- Datenbankschema von ARIS Risk & Compliance Manager
- Datenbanktreiber für Oracle oder Microsoft® SQL-Server

Nachfolgend wird die Installation mit automatischem Setup beschrieben. Wenn Sie Oracle oder Microsoft® SQL Server als DBMS verwenden möchten, müssen Sie vorab die Datenbank und das Datenbankschema installieren.

4.1 Installation der Datenbank

Installieren Sie die Oracle-Datenbank mit dem Oracle-Installationsprogramm, bzw. die Microsoft® SQL-Server-Datenbank mit den entsprechenden Installationsprogrammen. Befolgen Sie die Anweisungen des Installationsprogramms sowie die von den Herstellern mitgelieferten Dokumentation. Notieren Sie dabei die SID bzw. den Datenbanknamen der neuen Datenbank-Instanz und das Konto, d. h. den Benutzernamen und das Kennwort des Systembenutzers.

4.2 Installation des Datenbankschemas (Oracle)

Das Auslieferungspaket von ARIS Risk & Compliance Manager enthält Datenbankskripte, die Ihnen helfen, die Datenbank für ARIS Risk & Compliance Manager vorzubereiten. Für die Ausführung benötigen Sie einen installierten Oracle-Client (sqlplus).

Batch-Datei und verfügbare Skripte:

- **rebuild.bat**
Hauptskript zum Starten der Installation.
- **rebuild.sql**
Eingabe der Daten.
- **init_user.sql**
Anlegen des neuen Oracle-Benutzerschemas für ARIS Risk & Compliance Manager.

Vorgehen

1. Editieren Sie die Datei **rebuild.bat** und das Skript **rebuild.sql**.
2. Tragen Sie in der Datei **rebuild.bat** anstelle der Ausdrücke in spitzen Klammern die Werte für das Kennwort und für die SID (Seite 4) ein.
3. Vor **@rebuild.sql** muss ein Leerzeichen stehen: **sqlplus system/<password>@<SID>@rebuild.sql**.
4. Setzen Sie in der Datei **rebuild.sql** die SID ein: **connect &username/&password@<SID>**.
5. Starten Sie die Datei **rebuild.bat**.
6. Geben Sie einen Benutzernamen und ein Kennwort an. Notieren Sie sich diese Angaben, da sie im späteren Verlauf der Installation benötigt werden.

Danach werden die übrigen Skripte in der richtigen Reihenfolge ausgeführt. Die Datenbank enthält noch kein Datenbankschema mit Tabellen. Diese werden beim ersten Serverstart von ARIS Risk & Compliance Manager automatisch angelegt. Achten Sie auf Fehlermeldungen während die Skripte ablaufen. Der Befehl **drop user <username> cascade** kann bei der ersten Ausführung mit einer Fehlermeldung fehlschlagen, da zu diesem Zeitpunkt der Benutzer noch nicht existiert. Bei erneuter Ausführung des Skripts wird der Benutzer zunächst gelöscht und dann neu angelegt. Alle anderen Befehle müssen fehlerfrei durchlaufen.

4.3 Installation des Datenbankschemas (Microsoft® SQL-Server)

Das Auslieferungspaket von ARIS Risk & Compliance Manager enthält Datenbankskripte, die Ihnen helfen, die Datenbank für ARIS Risk & Compliance Manager vorzubereiten. Die Skripte sind auf dem Host-Computer des SQL-Servers auszuführen.

- **install.bat**
Hauptskript zum Initialisieren eines Datenbankbenutzers für ARIS Risk & Compliance Manager und zur Eingabe der Daten **Datenbankname**, **Benutzername** und **Kennwort**.
- **recreate_database.bat**
Ausführen des SQL-Skripts **recreate_database.sql**
- **recreate_database.sql**
Generieren der Datenbankinstanz für ARIS Risk & Compliance Manager.
- **recreate_dbuser.bat**
Ausführen der SQL-Skripte **drop_dbuser.sql** und **create_dbuser.sql**.
- **drop_dbuser.sql**
Löschen des Datenbankbenutzers von ARIS Risk & Compliance Manager.
- **create_dbuser.sql**
Generierung von Benutzern von ARIS Risk & Compliance Manager und Zuweisung von Rechten.

Warnung

Sollte es bereits eine Datenbank mit selben Namen geben, wird diese gelöscht.

Vorgehen

7. Editieren Sie die Datei **install.bat**.
8. Tragen Sie in der Datei **install.bat** anstelle des Ausdrucks in spitzen Klammern das aktuelle Kennwort des SQL-Server-Benutzers **sa** (Systembenutzer) ein.
9. Ersetzen Sie ebenso die Pfadinformation **<pathinfo>**.
10. Starten Sie die Datei **install.bat**.
11. Geben Sie einen Datenbanknamen, einen Benutzernamen und ein Kennwort an. Notieren Sie sich diese Angaben, da sie im späteren Verlauf der Installation benötigt werden.

Das Datenbankschema wird installiert.

5 Installation und Konfiguration der Anwendung

Mit ARIS Risk & Compliance Manager wird neben dem Standarddatenbanksystem die Datenbank **Apache Derby** ausgeliefert. Sie wird, falls gewünscht, bei der Installation von ARIS Risk & Compliance Manager mit installiert. Verwenden Sie zum produktiven Betrieb von ARIS Risk & Compliance Manager das Standarddatenbanksystem, eine Oracle- oder Microsoft® SQL-Datenbank. Beachten Sie, dass eine Produktivdatenbank neu aufgesetzt werden sollte. Verwenden Sie in Ihrem Produktivsystem keine Testdaten.

Wurde die Installationsgröße **Large** gewählt, sollte eine Oracle- oder Microsoft® SQL-Datenbank eingesetzt werden.

Die Verwendung einer Derby-Datenbank ist lediglich zu Testzwecken erlaubt. Wenn Sie ARIS Risk & Compliance Manager mit der Datenbank **Apache Derby** betreiben, wird auf der Oberfläche von ARIS Risk & Compliance Manager der Begriff **Demoversion** angezeigt. Diese Option steht nur dann zur Verfügung, wenn als Installationsgröße **Demo scenario** gewählt wurde.

5.1 Installation

Achten Sie darauf, dass die Portnummer von keiner anderen Software verwendet wird. Das ist vor allem dann wichtig, wenn Sie auf demselben Computer den Oracle-Server installiert haben. Evtl. ist bereits ein Web-Server an Port **80** installiert, welcher gleichzeitig der voreingestellte Port des Apache-Web-Servers ist, welcher als Loadbalancer mitinstalliert wird. Die Installationsquellen können Sie per Download der Datei als ZIP-Datei oder als Installationsmedium beziehen.

Diese Anleitung geht von einer lokalen Installation aus. Das bedeutet, dass ARIS Risk & Compliance Manager auf dem Server installiert wird, auf dem auch das Setup ausgeführt wird. Es besteht neben der lokalen Installation die Möglichkeit ARIS Risk & Compliance Manager per Remote-Installation auf einem anderen Server zu installieren. Lesen Sie dazu bitte das Kapitel **3.4 ARIS remote installations (Windows operating system)** im **Server Installation and Administration Guide**.

Vorgehen

1. Liegen die Installationsquellen als ZIP-Datei vor, entpacken Sie zunächst die ZIP-Datei von ARIS Risk & Compliance Manager in ein neues Verzeichnis. Geben Sie dazu das Kennwort der ZIP-Datei ein, das Ihnen von Software AG mitgeteilt wurde. Stellen Sie sicher, dass beim Entpacken die Pfadangaben berücksichtigt werden. Bei WinZip wird dies z. B. durch die Option **Pfadangaben verwenden** vorgegeben. Alternativ legen Sie das Installationsmedium von ARIS Risk & Compliance Manager in das Laufwerk.
2. Öffnen Sie das Verzeichnis **Setup** und starten Sie die Datei **setup.exe**.
3. Klicken Sie auf **Next**. Die Lizenzvereinbarungen werden angezeigt.
4. Wenn Sie die Lizenzvereinbarungen akzeptieren, klicken Sie auf **Next**. Der Dialog **Installation scenario** wird angezeigt.
5. Wählen Sie das Installationszenario **Perform installation on this active computer** und klicken Sie auf **Next**.
6. Geben Sie das Verzeichnis ein, in das ARIS Risk & Compliance Manager installiert werden soll und klicken Sie auf **Next**.
7. Wenn Sie den vorgeschlagenen Pfad verwenden, brauchen Sie keine Änderung vorzunehmen.
8. Klicken Sie im nächsten Dialog ohne Änderung auf **Next**.
9. Wählen Sie eine bereits vorhandene Lizenzdatei, welche vom Setup automatisch verwendet wird. Alternativ ist das nach der Installation im User Management möglich.
10. Klicken Sie auf **Next**.
11. Aktivieren Sie den gewünschten Modellierungsansatz für ARIS Risk & Compliance Manager und klicken Sie auf **Next**. Nach Installation ist es nicht mehr möglich den Modellierungsansatz zu ändern.
12. Legen Sie die Portnummer für die Verbindung zum Web-Application-Server fest und klicken Sie auf **Next**.

13. Geben Sie den Namen des Mail-Servers und die Standard-E-Mail-Adresse ein, falls diese Angaben bereits bekannt sind. Sollte der Mail-Server eine Authentifizierung verlangen, geben Sie ein E-Mail-Konto mit Kennwort an.
14. Klicken Sie auf **Next**.
15. Aktivieren Sie ggf. das Event-Enabling. Lesen Sie dazu die Detailinformationen (Seite 30) zu den einzelnen Konfigurationsmöglichkeiten.
16. Klicken Sie auf **Next**. Der Dialog **System settings** wird angezeigt.
17. Wählen Sie die Installationsgröße aus, um den zugewiesenen Speicher für ARIS Risk & Compliance Manager zu bestimmen: **Demo scenario** = 1GB, **Medium** = 4GB, **Large** = 8GB.
18. Klicken Sie auf **Next**. Der Dialog **Datenbanksystem wählen** wird angezeigt.
19. Wählen Sie die gewünschte Datenbank. **Standard Datenbank System** für eine PostgreSQL-Datenbank und **Derby (for demonstration purposes only)** für eine Apache Derby-Datenbank. Für Oracle oder Microsoft® SQL-Server ist zusätzlich ein passender Datenbanktreiber bereitzustellen, der durch das Setup mitinstalliert werden soll. Der Treiber kann bei Oracle/Microsoft heruntergeladen werden.
20. Haben Sie Oracle oder Microsoft® SQL gewählt, führen Sie zusätzlich die folgenden Schritte aus.
 - a. Tragen Sie den Namen des Datenbankservers ein.
 - b. Tragen Sie die Portnummer des Datenbankservers ein.
 - c. Tragen Sie den Service-Namen der Datenbank (Seite 5) ein (Oracle-SID) bzw. den Datenbanknamen (Microsoft® SQL-Server) der Datenbankinstanz.
 - d. Tragen Sie Name und Kennwort des Benutzers der Datenbank (Seite 4) ein.
21. Klicken Sie auf **Next**.
22. Klicken Sie auf **Install**, um die Installation zu starten.

ARIS Risk & Compliance Manager wird installiert.

Sie können den Tomcat-Server von ARIS Risk & Compliance Manager mit Hilfe der Einträge **Start ARIS Risk & Compliance Manager** und **Stop ARIS Risk & Compliance Manager** in der installierten Programmgruppe starten und stoppen. Um ARIS Risk & Compliance Manager zu öffnen, geben Sie die Adresse **http://<Servername>/arcm** im Browser ein.

5.2 Umstieg von der Testinstallation auf ein Produktivsystem

Wir empfehlen, das Testsystem vom Produktivsystem auch Server-seitig (Apache TomEE) getrennt zu halten. Je nach Auslastung des Produktiv- und Testsystems, kann auch eine Hardware-seitige Trennung notwendig sein. Ein Umstieg von einer Testinstallation auf ein Produktivsystem ist mit einer Neuinstallation von ARIS Risk & Compliance Manager auf der Produktiv-Hardware verbunden.

Es ist möglich ARIS Risk & Compliance Manager auf die Produktivdatenbank umzulenken, indem die Parameter für die Datenbankverbindung angepasst werden. Dazu müssen die Datenbankparameter in ARIS Cloud Controller geändert werden. Das folgende Vorgehen bezieht sich auf die Installationsgröße **Medium (arcm_m)**. Verwenden Sie **arcm_l** für die Installationsgröße **Large**.

STANDARDDATENBANK

Vorgehen

1. Starten Sie ARIS Cloud Controller und stoppen Sie die Komponente ARIS Risk & Compliance Manager mit **stop arcm_m**.
2. Lassen Sie sich mit **show instance arcm_m** die aktuellen und verfügbaren Datenbankparameter anzeigen.
3. Starten Sie die Komponente ARIS Risk & Compliance Manager mit **start arcm_m**.
4. Möchten Sie von einem anderen Datenbanksystem zum Standarddatenbanksystem wechseln, geben Sie **reconfigure arcm_m dbms.system="infrastructure"** ein. Das Standarddatenbanksystem wird aktiviert. Die weiteren Verbindungsparameter bezieht ARIS Risk & Compliance Manager aus der ARIS-Infrastruktur.
5. Starten Sie die Komponente ARIS Risk & Compliance Manager mit **start arcm_m**.

ORACLE

Vorgehen

1. Starten Sie ARIS Cloud Controller und stoppen Sie die Komponente ARIS Risk & Compliance Manager mit **stop arcm_m**.
2. Lassen Sie sich mit **show instance arcm_m** die aktuellen und verfügbaren Datenbankparameter anzeigen.
3. Um den Datenbanktreiberparameter zu ändern, geben Sie **reconfigure arcm_m dbms.driver="oracle.jdbc.driver.OracleDriver"** ein.
4. Um die Datenbank-URL zu ändern, geben Sie **reconfigure arcm_m dbms.url="jdbc:oracle:thin:@<DBserver>:<port>:<SID>"** ein.
5. Um den Datenbankbenutzer zu ändern, geben Sie **reconfigure arcm_m dbms.user="<DBBenutzername>"** ein
6. Um das Kennwort des Datenbankbenutzers zu ändern, geben Sie **reconfigure arcm_m dbms.pwd="<DBBenutzerkennwort>"** ein.
7. Aus lizenzrechtlichen Gründen dürfen die Oracle-JDBC-Datenbanktreiber nicht mit ausgeliefert werden. Laden Sie sich den passenden Datenbanktreiber aus dem Internet herunter und legen Sie ihn auf den Server, auf dem ARIS Risk & Compliance Manager installiert ist. Geben Sie **enhance arcm_m with commonsClasspath local file <Pfad>\\<zum>\\<Treiber-JAR>** in ARIS Cloud Controller ein, um den Datenbanktreiber einzubinden.
8. Starten Sie die Komponente ARIS Risk & Compliance Manager mit **start arcm_m**.

MICROSOFT® SQL-SERVER

Vorgehen

1. Starten Sie ARIS Cloud Controller und stoppen Sie die Komponente ARIS Risk & Compliance Manager mit **stop arcm_m**.
2. Lassen Sie sich mit **show instance arcm_m** die aktuellen und verfügbaren Datenbankparameter anzeigen.
3. Um den Datenbanktreiberparameter zu ändern, geben Sie **reconfigure arcm_m dbms.driver="com.microsoft.sqlserver.jdbc.SQLServerDriver"** ein.
4. Um die Datenbank-URL zu ändern, geben Sie **reconfigure arcm_m dbms.url="jdbc:sqlserver://[server]:<port>;DatabaseName=[database]"** ein.
5. Um den Datenbankbenutzer zu ändern, geben Sie **reconfigure arcm_m dbms.user="<DBBenutzername>"** ein
6. Um das Kennwort des Datenbankbenutzers zu ändern, geben Sie **reconfigure arcm_m dbms.pwd="<DBBenutzerkennwort>"** ein.
7. Aus lizenzrechtlichen Gründen darf der Microsoft® SQL Server-Datenbanktreiber nicht mit ausgeliefert werden. Laden Sie sich den passenden Datenbanktreiber aus dem Internet herunter und legen Sie ihn auf den Server, auf dem ARIS Risk & Compliance Manager installiert ist. Geben Sie **enhance arcm_m with commonsClasspath local file <Pfad>\\<zum>\\<Treiber-JAR>** in ARIS Cloud Controller ein, um den Datenbanktreiber einzubinden.
8. Starten Sie die Komponente ARIS Risk & Compliance Manager mit **start arcm_m**.

5.3 ARIS Risk & Compliance Manager in bestehende ARIS-Installation integrieren

Integrieren Sie ARIS Risk & Compliance Manager in die Installation von ARIS Design Server. Die Benutzerverwaltung erfolgt ab Version 9.5 zentral im User Management. Daher werden Benutzer nicht mehr in ARIS Risk & Compliance Manager angelegt. Das User Management für alle ARIS-Produkte, nicht zu verwechseln mit der Administration in ARIS Risk & Compliance Manager, dient zur Verwaltung von Benutzern, Benutzergruppen, Funktions- und Lizenzrechten, Lizenzen, Dokumenten und Konfigurationen. Damit ist die einmalige Anmeldung für verschiedene ARIS-Produkte gewährleistet. Das folgende Vorgehen bezieht sich auf die Installationsgröße **Medium** (**arcm_m/postgres_m**). Verwenden Sie **arcm_l/postgres_l** für die Installationsgröße **Large**.

Warnung

Installieren Sie ARIS Risk & Compliance Manager nicht auf einem Server, auf dem bereits ARIS Design Server oder ARIS Connect Server installiert ist. Die Installation von ARIS Risk & Compliance Manager würde die bestehende Infrastruktur der bestehenden Installation von ARIS überschreiben.

Vorgehen

1. Installieren Sie ARIS Design Server per Setup auf einem Server. Informationen zur Installation finden Sie im **ARIS Server Installation and Administration Guide**.
2. Konfigurieren Sie ARIS Design Server.
3. Starten Sie ARIS Design Server.
4. Installieren (Seite 8) Sie ARIS Risk & Compliance Manager auf einem anderen Server per Setup.
5. Starten Sie ARIS Cloud Controller der ARIS Risk & Compliance Manager-Installation über **Start > ARIS > ARIS Cloud Controller**.
6. Geben Sie in der Konsole den Befehl **reconfigure arcm_m zookeeper.connect.string="<ARISDesignServer>:2181"** ein.
7. Tragen Sie für den Platzhalter **<ARISDesignServer>** den Namen des Servers ein, den Sie in Schritt 1 für ARIS Design Server verwendet haben.
8. Hatten Sie den Port nicht verändert, bleibt auch hier die Standardeinstellung.
9. Um das Standarddatenbanksystem zu nutzen, geben Sie in der Konsole den Befehl **reconfigure postgres_m zookeeper.connect.string="<ARISDesignServer>:2181"** ein.
10. Tragen Sie für den Platzhalter **<ARISDesignServer>** den Namen des Servers ein, den Sie in Schritt 1 für ARIS Design Server verwendet haben.
11. Hatten Sie den Port nicht verändert, bleibt auch hier die Standardeinstellung.
12. Prüfen Sie mit dem Befehl **list**, ob alle Komponenten im Status **STOPPED** sind.
13. Starten Sie ARIS Risk & Compliance Manager mit dem Befehl **start arcm_m**. Die Endung **_m** ist entsprechend der Installationsgröße anzupassen (Small, Medium, Large), die Sie für den Speicher gewählt haben.

ARIS Risk & Compliance Manager wird mit ARIS Design Server verbunden und kann sowohl auf das User Management als auch auf ARIS Dokumentablage zugreifen.

Um ARIS Risk & Compliance Manager in einem Browser zu öffnen, geben Sie **ARIS Design Server** ein, gefolgt von **/arcm**.

Da die anderen Komponenten auf dem Server von ARIS Risk & Compliance Manager nicht länger benötigt werden, können diese entweder entfernt (Seite 14) oder so konfiguriert werden, dass sie beim Start des Servers nicht mehr automatisch gestartet werden.

Siehe auch

ARIS Cloud Controller

(http://documentation.softwareag.com/aris/aris95e/ARIS_Server_Installation_and_Administration_Guide.pdf)

5.3.1 Entfernen der nicht mehr benötigten Komponenten

Entfernen Sie nicht mehr benötigte Komponenten.

Warnung

Das Entfernen der Komponenten hat den Nachteil, dass sich diese Installation nicht mehr mit einem Setup aktualisieren lässt. Die Komponente ARIS Risk & Compliance Manager muss dann manuell per Update-Befehl aktualisiert werden.

Vorgehen

1. Stellen Sie sicher, dass die Komponente ARIS Risk & Compliance Manager gestartet ist. Öffnen Sie dazu ARIS Cloud Controller der ARIS Risk & Compliance Manager-Installation über **Start > ARIS > ARIS Cloud Controller**.
2. Prüfen Sie mit dem Befehl **list**, ob sich die Komponente **arcm_s** im Status **STARTED** befindet und alle anderen im Status **STOPPED**.
3. Geben Sie den Befehl **deconfigureall** ein und bestätigen Sie den Befehl mit **Y**. Dieser Befehl entfernt alle Komponenten, die sich im Status **STOPPED** befinden.

Die nicht benötigten Komponenten wurden entfernt.

5.3.2 Start der nicht mehr benötigten Komponenten verhindern

Verhindern Sie den Start der nicht mehr benötigten Komponenten.

Vorgehen

1. Öffnen Sie ARIS Cloud Controller der ARIS Risk & Compliance Manager-Installation (**Start > ARIS > ARIS Cloud Controller**).
2. Geben Sie den Befehl **set autostart.mode=autostart.flag** ein.
3. Setzen Sie für die nicht mehr benötigten Komponenten **autostart property** auf **false**:
 - e. **set zoo_m property autostart="false"**
 - f. **set postgres_m property autostart="false"**
 - g. **set couchdb_m property autostart="false"**
 - h. **set elastic_m property autostart="false"**
 - i. **set adsadmin_m property autostart="false"**
 - j. **set umcadmin_m property autostart="false"**
 - k. **set loadbalancer_m property autostart="false"**

Die nicht mehr benötigten Komponenten werden bei einem Neustart des Servers nicht mehr automatisch gestartet. Der Befehl **startall** in ARIS Cloud Controller startet aber trotzdem alle Komponenten.

5.4 Konfigurationsparameter

Die meisten Parameter, mit denen das Verhalten von ARIS Risk & Compliance Manager beeinflusst werden kann, finden Sie in der Datei **<Installationsordner von ARIS Risk & Compliance**

Manager>\server\bin\work\work_arcm_m\base\webapps\arcm\WEB-INF\runtime config.xml. Diese haben das folgende Format:

```
<parameterList name="applicationlayer">
  <!--entries per page in a list-->
  <parameter name="application.view.entriesPerPage" value="20"/>
  <!-- edit only in consultation of Software AG -->
  <parameter name="application.batchserver.enable.remoteconnection"
value="false"/>
  <!-- edit only in consultation of Software AG -->
  <parameter name="application.batchserver.resend.trails" value="5"/>
</parameterList>
```

Die wichtigsten Parameter werden im Folgenden detailliert beschrieben. Alle nicht genannten Parameter haben internen Charakter und sollten nicht geändert werden. Voreingestellte Werte sind in eckigen Klammern aufgeführt.

APPLICATION.VIEW.ENTRIESPERPAGE

param-value	Erläuterung
20	Legt fest, wie viele Listeneinträge pro Seite ausgegeben werden sollen, in diesem Beispiel 20.

SERVERURL

param-value	Erläuterung
http://<host>:<port>/<Kontext>	Damit in den Benachrichtigungen (intern oder E-Mail) der angegebene Link zur Anwendung korrekt ist, müssen Sie diesen Eintrag an Ihre Gegebenheiten anpassen.

WHISTLEBLOWEMAIL

param-value	Erläuterung
adminpleaseChangeEmail_at_your_server	Legt fest, an welche E-Mail-Adresse Whistle-blow-Mails versendet werden.

SCHEDULER-EINSTELLUNGEN

Nachfolgend werden die Einstellungen der verschiedenen Scheduler erläutert. Scheduler führen zeitgesteuerte Jobs aus. Die beiden wichtigsten Parameter werden nur einmal aufgeführt, da sie für folgende Jobs, von der Art der Konfiguration, identisch sind:

- generatorJobTestcases
- monitorJobTestcases
- generatorJobRiskAssessment
- monitorJobRiskAssessment
- generatorJobSOPProcess
- monitorJobSOPProcess
- generatorJobSurvey
- monitorJobQuestionnaire
- monitorJobSurvey
- monitorJobIssue
- generatorJobAudit
- monitorJobAudit
- generatorJobPolicy
- monitorJobPolicy
- updaterJobPolicy
- cleaningJob
- jobListCleaningJob

STARTSCHEDULER

Schalter für die Zeitsteuerung. Testfälle werden über eine Art Cronjob generiert und überprüft. Der Quartz-Scheduler wird verwendet.

param-value	Erläuterung
false	Deaktiviert die Zeitsteuerung.
true	Aktiviert die Zeitsteuerung.

EXECUTIONTIME

Hier werden die Ausführungszeiten für den Quartz-Scheduler (siehe **Scheduler-Einstellungen**) eingetragen. Diese werden als **Cron Expressions!** angegeben. Weitere Informationen zum Quartz-Scheduler (<http://www.quartz-scheduler.org/documentation/quartz-2.1.x/tutorials/tutorial-lesson-06>) finden Sie auf der Internetseite.

CLIENTEXCLUDINGLIST

Hier können Mandanten eingetragen werden, die vom jeweiligen Job ausgeschlossen werden sollen. Die Mandanten müssen kommasepariert sein.

CLIENTINCLUDINGLIST

Hier können Mandanten eingetragen werden, die vom jeweiligen Job eingeschlossen werden sollen. Die Mandanten müssen kommasepariert sein. Alle anderen Mandanten werden von den Jobs ignoriert.

5.5 Konfiguration der E-Mail-Funktionalität

Sie können ARIS Risk & Compliance Manager so konfigurieren, dass in bestimmten Fällen E-Mails automatisch versendet werden, z. B. an einen Tester, dem ein Testfall zugeordnet wurde. Zum Versenden von E-Mails wird ein externer Mail-Server mit SMTP-Unterstützung genutzt, der in der Regel bereits eingerichtet und verfügbar ist. ARIS Risk & Compliance Manager beinhaltet selbst keinen SMTP-Mailserver.

Vorgehen

1. Starten Sie ARIS Cloud Controller.
2. Um den SMTP-Host-Parameter zu konfigurieren, geben Sie **reconfigure arcm_m smtp.host="< IP-Adresse oder gültiger DNS-Name des Mail-Versand-Servers>"** ein.
3. Ist auf dem Mail-Server die SMTP-Authentifizierung aktiviert ist, geben Sie **reconfigure arcm_m smtp.account="< Benutzername des SMTP-Accounts>"** ein, um den Parameter **smtp.account** zu konfigurieren.
4. Ist auf dem Mail-Server die SMTP-Authentifizierung aktiviert, geben Sie **reconfigure arcm_m smtp.password="<Kennwort des SMTP-Accounts>"** ein, um den Parameter **smtp.password** zu konfigurieren.
5. Für den Fall, dass beim Versenden von automatischen E-Mails keine gültige E-Mail-Adresse definiert ist, geben Sie **reconfigure arcm_m smtp.default.sender.address="<Fallback-Absender>"** ein, um den Parameter **default.sender.address** zu konfigurieren.
6. Um die Änderungen der Mail-Konfiguration zu übernehmen, beenden Sie die Komponente ARIS Risk & Compliance Manager mit **stop arcm_m** und starten Sie sie wieder mit **start arcm_m**.

Die E-Mail-Funktionalität wird konfiguriert.

In ARIS Risk & Compliance Manager werden E-Mails und interne Nachrichten immer in der definierten Sprache des Mandanten versendet, falls das entsprechende Objekt in der Nachricht mandantenspezifisch ist. Für allgemeine Nachrichten, wie die Anforderung eines neuen Kennworts, wird die eingestellte Sprache des Systems verwendet.

5.6 Ändern der System-E-Mail-Adressen

Nach der Installation von ARIS Risk & Compliance Manager sind alle E-Mail-Adressen der vordefinierten Benutzer (z. B. des System-Benutzers) auf die ungültige E-Mail-Adresse **adminpleaseChangeEmail_at_your_server** gesetzt. Für den Produktivbetrieb müssen sie durch gültige Adressen wie nachfolgend beschrieben ersetzt werden.

RUNTIMECONFIG.XML

- **parameter name="WhistleBlowEmail"**
value="adminpleaseChangeEmail@example.com"/>
- **WhistleBlowAnonymousSender (<parameter name="WhistleBlowAnonymousSender"**
value="adminpleaseChangeEmail@example.com"/>
- **<parameter name="default.sender.address"**
value="changeEmail@example.com"/>

In ARIS Risk & Compliance Manager müssen die E-Mail-Adressen von folgenden Benutzern geändert werden:

- Systemadministrator (system)
- Internalsystem (Internal system user)
- Job User (jobUser)

6 Installation einer kundenspezifischen Version (Customizing)

ARIS Risk & Compliance Manager kann umfassend an Kundenwünsche angepasst werden. Diese Anpassungen werden in XML und Java-Dateien vorgenommen und später in einer ZIP-Datei zusammengefasst. Diese ZIP-Datei muss nach einer Installation von ARIS Risk & Compliance Manager mit Hilfe des ARIS Cloud Controller eingespielt werden.

Vorgehen

1. Installieren (Seite 7) Sie ARIS Risk & Compliance Manager.
2. Starten Sie nach der Installation über **Start > ARIS > Administration** den ARIS Cloud Controller.
3. Stoppen Sie ARIS Risk & Compliance Manager über **Start > ARIS > Stop ARIS Risk & Compliance Manager**.
4. Geben Sie in der Konsole den Befehl ein **enhance <ARCM-runnable> with customizing local file "<Pfad zum CustomizingZip>"**. Der Name der Komponente ARIS Risk & Compliance Manager ist von der Installationsart abhängig. Mögliche Namen für **<ARCM-runnable>** sind: **arcm_s**, **arcm_m** oder **arcm_l**. Achten Sie bitte darauf, dass Sie stets doppelte Anführungszeichen („“) verwenden, um den Pfad zur ZIP-Datei anzugeben.
5. Starten Sie ARIS Risk & Compliance Manager über **Start > ARIS > Start > ARIS Risk & Compliance Manager**

ARIS Risk & Compliance Manager wurde durch kundenspezifische Änderungen erweitert.

7 Neue Version von ARIS Risk & Compliance Manager installieren

Ab Version 9.5 von ARIS Risk & Compliance Manager können neuere Versionen per Update-Setup aktualisiert werden. Die Aktualisierung einer Installation von ARIS Risk & Compliance Manager besteht aus folgenden manuell auszuführenden Schritten. Vor dem Ausführen des Setups sollte eine Datensicherung der Datenbank von ARIS Risk & Compliance Manager und von ARIS Dokumentablage durchgeführt werden.

Warnung

Die Migration kann nicht rückgängig gemacht werden.

- Datensicherung (Seite 22)
- Ausführung des Update-Setups (Seite 23)
- Datenmigration (Seite 23)
 - Migration der Daten aus ARIS Dokumentablage (Seite 24)*
 - Migration der Datenbank von ARIS Risk & Compliance Manager (Seite 27)
- Importieren von modellierten Benutzer ins User Management (Seite 28)
- Anbindung an einen Verzeichnisdienst (LDAP) (Seite 30)*
- Kennwortverschlüsselung in der Laufzeitkonfiguration (Seite 30)*
- Konfiguration des Event-Enabling in ARIS Risk & Compliance Manager (Seite 30)*

Die mit * markierten Schritte sind in Abhängigkeit von der zuvor verwendeter Version und dem genutztem Funktionsumfang optional.

7.1 Datensicherung

Führen Sie die empfohlenen Schritte zum Sichern der Daten aus. Haben Sie ARIS Dokumentablage bisher nicht verwendet, entfällt die Sicherung der Daten von ARIS Dokumentablage.

Vorgehen

1. Stoppen Sie die bestehende Installation.
2. Sichern Sie die Daten Ihrer Produktivdatenbank. Wenn Sie Oracle nutzen, verwenden Sie **dataPump**.
3. Sichern Sie die CouchDBs von ARIS Dokumentablage.
 - a. Um die CouchDB von ARIS Risk & Compliance Manager zu sichern, kopieren Sie das Verzeichnis **<ARCM 4.x Installationsverzeichnis>\couchdb\var\lib\couchdb** nach **<Sicherungsverzeichnis ARCM 4.x CouchDB>**.
 - b. Um die CouchDB von Process Governance zu sichern, kopieren Sie das Verzeichnis **<APG Installationsverzeichnis>\ads\adsdata\couchdb** nach **<Sicherungsverzeichnis APG CouchDB>**.

Die Datensicherung ist abgeschlossen.

7.2 Ausführung des Update-Setups

Um die neue Version zu installieren, ist es nicht mehr notwendig zuerst die bestehende Installation zu deinstallieren. Alle Einstellungen die bei der Erstinstallation im Setup konfiguriert wurden, werden automatisch übernommen. Die Einstellungen, die nach der Installation in der **runtimeconfig.xml** geändert wurden, werden nicht übernommen. Der Download-Ordner, der alle erstellten PDF- und Excel-Reporte sowie Mandanten- und Datenbanksicherungen enthält, wird gesichert.

Folgende Parameter können im Setup gesetzt werden und werden automatisch beim Update-Setup übernommen:

- Modellierungsansatz (Risiko- oder Kontrollbasiert)
- Mailserverkonfiguration (ARIS Risk & Compliance Manager und User Management)
- Event-Processing (Event-Server, Port- und EventTypeStore)
- Datenbankkonfiguration

Alle anderen nachträglichen Änderungen, die Sie in der **runtimeconfig.xml** gemacht haben (z. B. Jobeinstellungen), müssen nach dem Update wieder in die aktualisierte **runtimeconfig.xml** übernommen werden. Diese Einstellungen sollten Sie sich notieren, um sie nach dem Update wieder konfigurieren zu können.

7.3 Datenmigration

Sie müssen Ihre bestehenden Daten migrieren, um sie in einer neueren Version von ARIS Risk & Compliance Manager verwenden zu können. Das gilt auch für einen Umstieg innerhalb eines Hauptreleases, z. B. von der Version 9.7 auf 9.8.

Die Migration der Daten besteht aus zwei Teilen:

- Migration von ARIS Dokumentablage (nur relevant beim Update von Version 4).
- Migration der Datenbank von ARIS Risk & Compliance Manager. Datenbanken aus Versionen vor 3.1 SR4 werden nicht mehr unterstützt. Möchten Sie eine ältere Version migrieren, wenden Sie sich bitte an den Support der Software AG (Seite 43).

Zur Migration müssen Befehle in der Windows-Eingabeaufforderung (CMD) und Befehle im ARIS Cloud Controller (ACC) ausgeführt werden. Die Umgebung der Ausführung (CMD oder ACC) steht jeweils vor dem jeweiligen auszuführenden Befehl. ARIS Cloud Controller (ACC) ist nach der Installation im Startmenü von Windows verfügbar (**Start > ARIS > Administration > ARIS Cloud Controller**). Die Windows-Eingabeaufforderung ist Bestandteil des Betriebssystems (**Start > Zubehör > Eingabeaufforderung**).

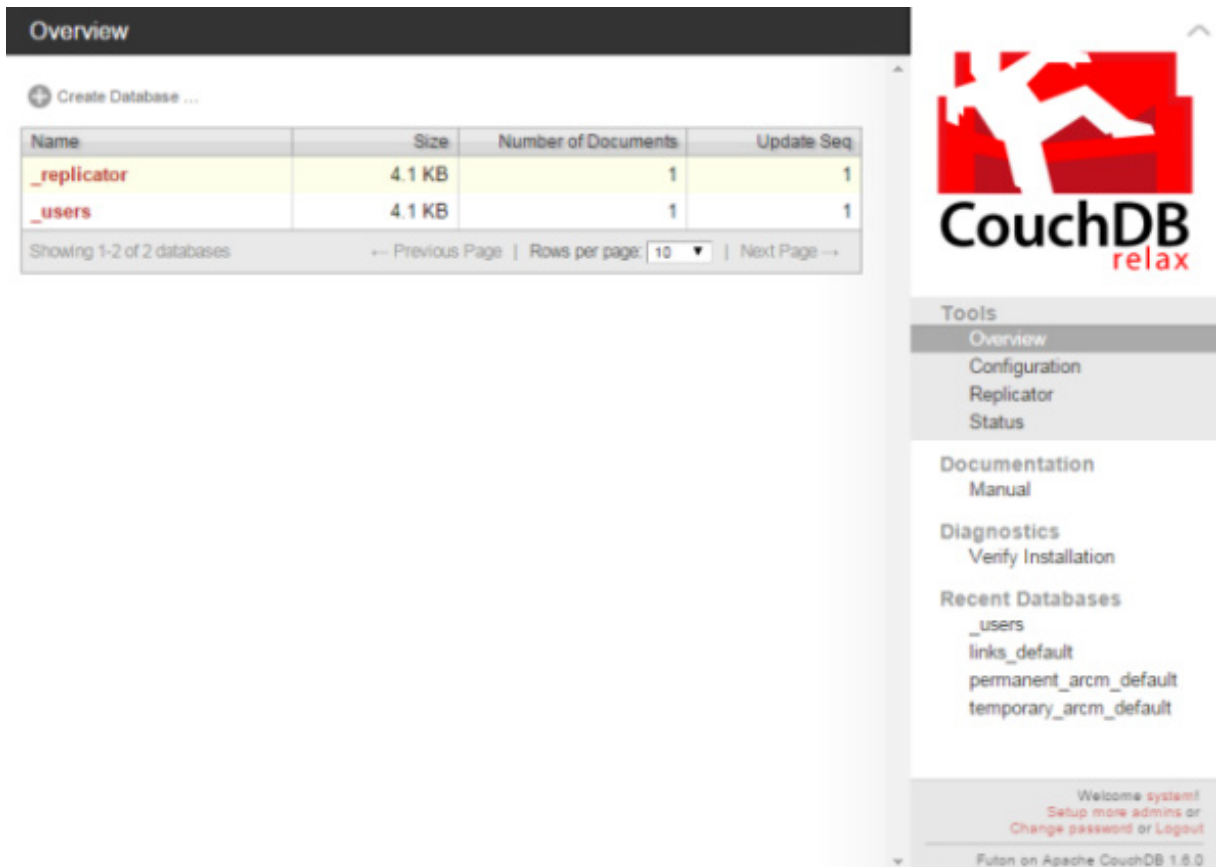
7.3.1 Migration der Daten aus ARIS Dokumentablage

Migrieren Sie die Daten von ARIS Dokumentablage, um sie in einer neueren Version von ARIS Risk & Compliance Manager verwenden zu können. Haben Sie ARIS Dokumentablage bisher nicht verwendet oder aktualisieren Sie von einer Version 9.x ausgehend, brauchen Sie die Migration nicht durchzuführen. Wechseln Sie von Version 4.x zur aktuellen Version, müssen Sie die Daten von ARIS Dokumentablage migrieren. In den Versionen 4.x gab es für ARIS Business Server mit Anbindung an Process Governance und ARIS Risk & Compliance Manager separate Installationen von ARIS Dokumentablage. Seit Version 9 gibt es nur noch eine gemeinsamen ARIS Dokumentablage.

Im Folgenden werden die Schritte zum Zusammenführen und migrieren der beiden Dokumentablagen beschrieben.

Vorgehen

1. Stoppen Sie das Runnable von ARIS Risk & Compliance Manager ACC: **stop <arcm-runnable>**. Alle anderen Runnables müssen laufen.
2. Überprüfen Sie den Inhalt der CouchDB (http://<your host>:19975/_utils/ - Basisauthentifizierung, Anmeldedaten eines Benutzers der das Funktionsrecht **Dokumentenadministrator** hat).
3. Der Inhalt der CouchDB sollte so aussehen:



The screenshot shows the CouchDB Relax administration interface. The main content area displays a table with the following data:

Name	Size	Number of Documents	Update Seq
_replicator	4.1 KB	1	1
_users	4.1 KB	1	1

Below the table, it indicates "Showing 1-2 of 2 databases" and provides navigation options: "-- Previous Page | Rows per page: 10 | Next Page --".

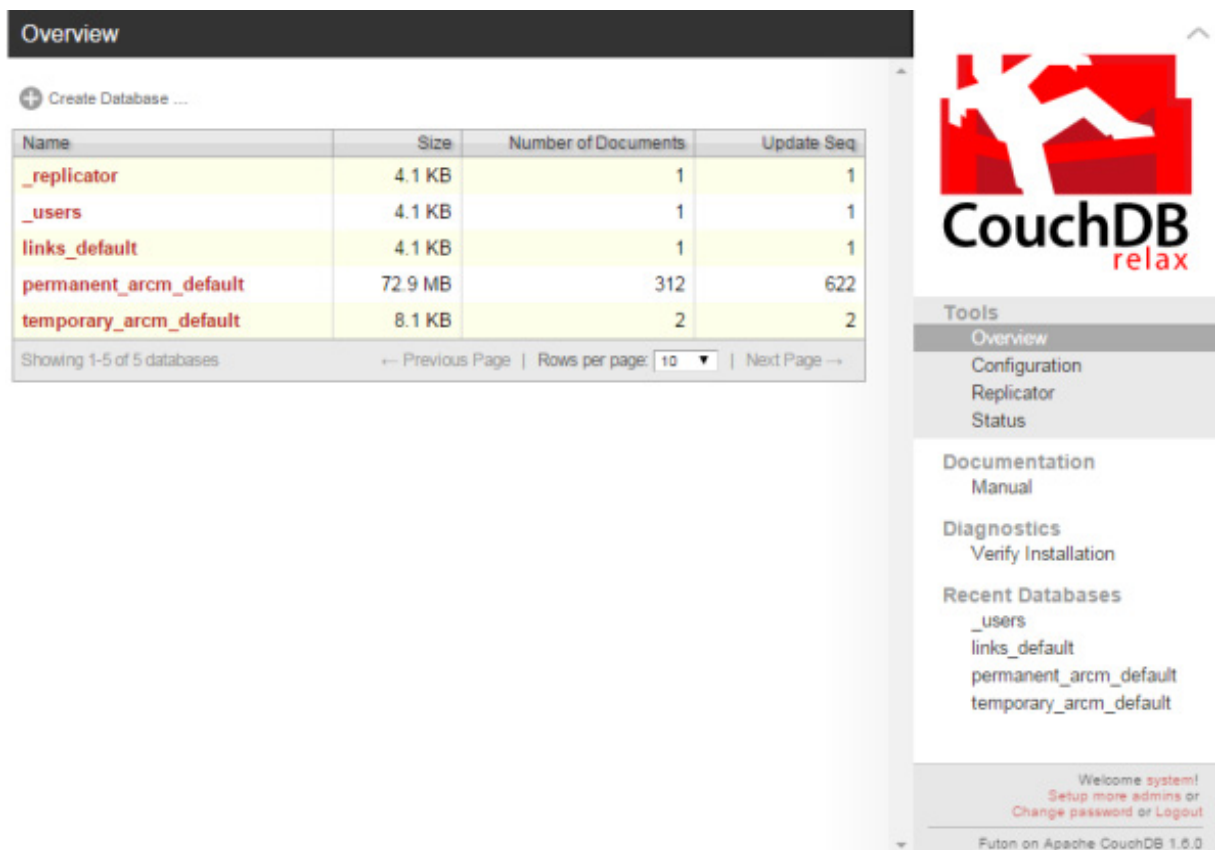
The sidebar on the right contains the following menu items:

- Tools
 - Overview
 - Configuration
 - Replicator
 - Status
- Documentation
 - Manual
- Diagnostics
 - Verify Installation
- Recent Databases
 - _users
 - links_default
 - permanent_arcm_default
 - temporary_arcm_default

At the bottom of the sidebar, there is a welcome message: "Welcome system! Setup more admins or Change password or Logout" and the version information: "Futon on Apache CouchDB 1.8.0".

4. Starten Sie die Windows-Eingabeaufforderung (CMD) und wechseln in das Verzeichnis **<ARCM-Installationsverzeichnis>\server\bin\work\work_adsadmin_m\tools\bin**.
 - a. Starten Sie die Migration der CouchDB von ARIS Risk & Compliance Manager
 CMD: **y-admintool.bat migrate -r arcm -s "<Sicherungsverzeichnis ARCM 4.x CouchDB>" -t "<ARCM-Installationsverzeichnis>\server\bin\work\work_couchdb_m\data**
 - b. Starten Sie die Migration der CouchDB von Process Governance:
 CMD: **y-admintool.bat migrate -s "<Sicherungsverzeichnis Governance CouchDB>" -t "<ARCM-Installationsverzeichnis>\server\bin\work\work_couchdb_m\data"**

In der Übersicht der CouchDB sollten nun neue Datenbanken mit Dokumenten angezeigt werden:



The screenshot shows the CouchDB Overview page. The main content is a table with the following data:

Name	Size	Number of Documents	Update Seq
_replicator	4.1 KB	1	1
_users	4.1 KB	1	1
links_default	4.1 KB	1	1
permanent_arcm_default	72.9 MB	312	622
temporary_arcm_default	8.1 KB	2	2

Below the table, it says "Showing 1-5 of 5 databases" and "Rows per page: 10".

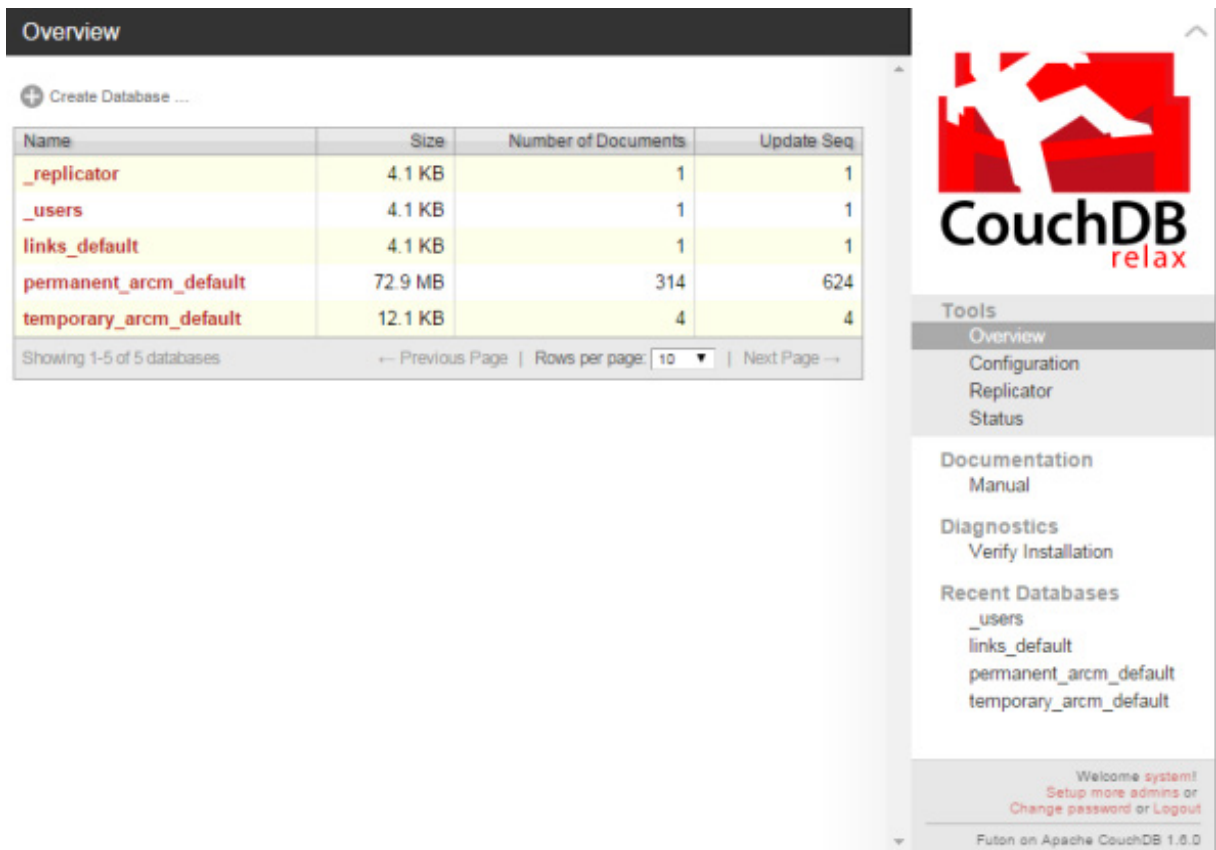
The sidebar on the right contains the following sections:

- Tools**
 - Overview
 - Configuration
 - Replicator
 - Status
- Documentation**
 - Manual
- Diagnostics**
 - Verify Installation
- Recent Databases**
 - _users
 - links_default
 - permanent_arcm_default
 - temporary_arcm_default

At the bottom of the sidebar, there is a "Welcome system!" message with links for "Setup more admins or Change password or Logout" and "Futon on Apache CouchDB 1.6.0".

5. Starten Sie die Reindizierung der CouchDB:
 CMD: **y-admintool.bat -t default reindex -u <USER> -p <PASSWORD>**
 Ersetzen Sie **<USER>** und **<PASSWORD>** durch die Anmeldedaten eines Benutzers der das Funktionsrecht **Dokumentenadministrator** hat.

6. Nach der Reindizierung hat sich die Anzahl der Dokumente erhöht:



The screenshot shows the CouchDB relax overview page. The main content is a table listing databases with their names, sizes, number of documents, and update sequences. The table is as follows:

Name	Size	Number of Documents	Update Seq
_replicator	4.1 KB	1	1
_users	4.1 KB	1	1
links_default	4.1 KB	1	1
permanent_arcm_default	72.9 MB	314	624
temporary_arcm_default	12.1 KB	4	4

Below the table, it says "Showing 1-5 of 5 databases" and "Rows per page: 10".

On the right side, there is a sidebar with the CouchDB relax logo and a "Tools" menu. The "Tools" menu includes:

- Overview
- Configuration
- Replicator
- Status
- Documentation
- Manual
- Diagnostics
- Verify Installation
- Recent Databases
- [_users](#)
- [links_default](#)
- [permanent_arcm_default](#)
- [temporary_arcm_default](#)

At the bottom of the sidebar, there is a welcome message: "Welcome system! Setup more admins or Change password or Logout". At the very bottom, it says "Futon on Apache CouchDB 1.6.0".

Die Migration der Daten von ARIS Dokumentablage ist abgeschlossen.

7.3.2 Migration der Datenbank von ARIS Risk & Compliance Manager

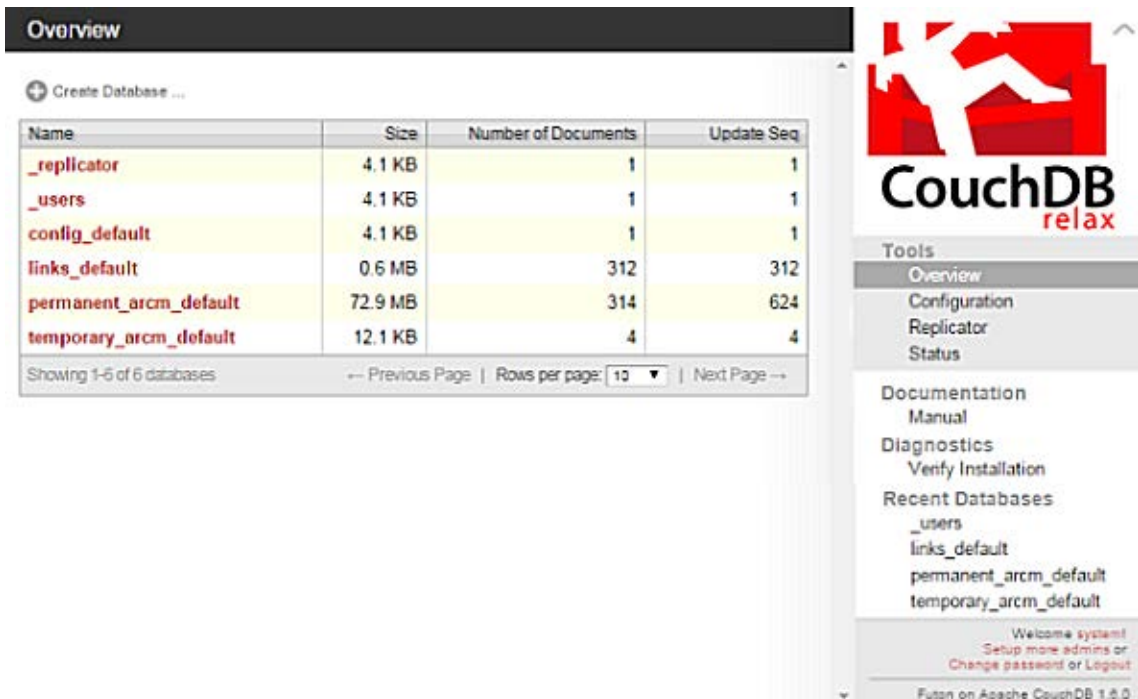
Migrieren Sie Ihre bestehende Datenbank, um sie in einer neueren Version von ARIS Risk & Compliance Manager verwenden zu können.

Voraussetzung

Der Benutzer **system** hat das Funktionsrecht **Dokumentenadministrator**. Ohne dieses Funktionsrecht kann die Migration der Dokumentverlinkung nicht durchgeführt werden. Ordnen Sie es gegebenenfalls vor der Migration zu und entfernen Sie es danach wieder.

Vorgehen

1. Stoppen Sie das Runnable von ARIS Risk & Compliance Manager
ACC: **stop <arcm-runnable>**. Alle anderen Runnables müssen laufen.
2. Aktivieren Sie die Datenmigration durch ARCM-Runnable per ARIS Cloud Controller (ACC):
ACC: **reconfigure <arcm-runnable> dbms.autoStartMigration=true**
3. Starten Sie die Datenmigration indem Sie das Runnable von ARIS Risk & Compliance Manager starten:
ACC: **start <arcm-runnable>**. Das Starten kann je nach Datenmenge einige Zeit in Anspruch nehmen. Der Inhalt der CouchDB sollte nun so aussehen:



The screenshot shows the CouchDB Overview page. The main content is a table with the following data:

Name	Size	Number of Documents	Update Seq
_replicator	4.1 KB	1	1
_users	4.1 KB	1	1
config_default	4.1 KB	1	1
links_default	0.6 MB	312	312
permanent_arcm_default	72.9 MB	314	624
temporary_arcm_default	12.1 KB	4	4

Below the table, it says "Showing 1-6 of 6 databases" and "Rows per page: 10". The sidebar on the right contains the CouchDB logo and a "Tools" menu with the following items: Overview (selected), Configuration, Replicator, Status, Documentation (Manual), Diagnostics (Verify Installation), and Recent Databases (_users, links_default, permanent_arcm_default, temporary_arcm_default). At the bottom of the sidebar, there is a "Welcome system!" message and a footer "Futon on Apache CouchDB 1.6.0".

4. Deaktivieren Sie die automatische Migration per ARIS Cloud Controller (ACC):
ACC: **stop <arcm-runnable>**.
ACC: **reconfigure <arcm-runnable> dbms.autoStartMigration=false**
5. Starten Sie ARIS Risk & Compliance Manager für den produktiven Betrieb.
ACC: **start <arcm-runnable>**.

Die Migration der Daten ist damit abgeschlossen.

7.4 Importieren von modellierten Benutzer ins User Management

Nach dem Import eines Datenbankexports aus ARIS Architect in ARIS Risk & Compliance Manager, sind alle importierten Benutzer zunächst deaktiviert. Sie können aktiviert werden, indem sie im User Management manuell angelegt und dann mit ARIS Risk & Compliance Manager synchronisiert werden (**Administration > Mit User Management synchronisieren**). Der Report **ARCM-Benutzerexport für das User Management** erledigt dies automatisiert, indem alle modellierten Benutzer einer Datenbank (Objektyp **Person**) exportiert werden. Folgende Attribute eines Benutzers werden exportiert:

- Anmeldung
- Vorname
- Nachname
- E-Mail-Adresse

Der Report ermittelt außerdem, welches Lizenzrecht ein Benutzer benötigt. Dabei gelten folgende Regeln:

- Ist ein Benutzer keiner Benutzergruppe zugeordnet, wird ihm das Lizenzrecht **Contribute** zugeordnet. Benutzer ohne Gruppenzuordnung sind berechtigt, Aufgaben im Issue-Management wahrzunehmen.
- Ist ein Benutzer einer Benutzergruppe mit der Rolle Vorfall-Owner oder Policy-Addressee zugeordnet, wird ihm das Lizenzrecht **Contribute** zugeordnet.
- Bei allen anderen Rollenzuordnungen erhält der Benutzer das Lizenzrecht **Operate**.

7.4.1 Modellierte Benutzer aus ARIS Architect exportieren

Exportieren Sie die modellierten Benutzer aus ARIS Architect.

Vorgehen

1. Öffnen Sie ARIS Architect.
2. Öffnen Sie die Datenbank, deren modellierte Benutzer Sie für den Import in das User Management exportieren möchten.
3. Klicken Sie mit der rechten Maustaste auf die Hauptgruppe.
4. Klicken Sie auf **Auswerten > Report starten**.
5. Wählen Sie die Kategorie von ARIS Risk & Compliance Manager.
6. Wählen Sie den Report **ARCM-Benutzerexport für das User Management**.
7. Wählen Sie die Ausgabeeinstellungen.
8. Klicken Sie auf **Fertigstellen**.

Eine Textdatei mit den Attributen Anmeldung, Vor- und Nachname sowie E-Mail-Adresse wird exportiert.

7.4.2 Modellierte Benutzer ins User Management importieren

Importieren Sie die modellierten Benutzer ins User Management.


Vorgehen

1. Legen Sie das Installationsmedium von ARIS Risk & Compliance Manager in das Laufwerk.
2. Kopieren Sie die Datei **create_user.bat** aus dem Ordner **Content** in den Ordner **<ARCM-Installationsordner>\server\bin\work\work_umcadmin_s\tools\bin**.
3. Kopieren Sie die Textdatei, die Sie zuvor mit dem Report **ARCM-Benutzerexport für das User Management** erstellt haben in den gleichen Ordner.
4. Ersetzen Sie in der Datei **create_user.bat** den Eintrag **set INPUTFILE** mit dem entsprechenden Namen der Exportdatei.
5. Speichern Sie die Änderung.
6. Führen Sie die Datei **create_user.bat** aus. Sie können dabei ein Kennwort für alle importierten Benutzer vergeben. Möchten Sie kein Kennwort vergeben, drücken Sie die Eingabetaste ohne ein Kennwort einzugeben.

Die Benutzer werden ins User Management importiert.

7.4.3 Benutzer in ARIS Risk & Compliance Manager aktualisieren

Aktualisieren Sie die Benutzer in ARIS Risk & Compliance Manager mit den Daten aus dem User Management.

1. Melden Sie sich als Systemadministrator in ARIS Risk & Compliance Manager an.
2. Klicken Sie auf  **Administration**.
3. Klicken Sie unter **Aktionen** auf **Mit User Management synchronisieren**. Die Benutzerdaten in ARIS Risk & Compliance Manager werden durch die Daten aus dem User Management ersetzt. Dadurch werden Funktions- und Lizenzrechte, Namen, Kennwörter, E-Mail-Adressen usw. aktualisiert sowie Benutzer deaktiviert.

Der Dialog wird geschlossen. **Monitoring > Jobs und Importe/Exporte** wird angezeigt. Der Job wird unter **Wartende Jobs und Importe/Exporte** ausgegeben. Ist er abgeschlossen, wird er unter **Beendete Jobs und Importe/Exporte** aufgelistet. Die importierten Benutzer werden in ARIS Risk & Compliance Manager aktiviert.

7.5 Anbindung an einen Verzeichnisdienst (LDAP)

Anders als in den Vorgängerversionen wird LDAP nun nicht mehr direkt mit ARIS Risk & Compliance Manager verbunden. Stattdessen muss die LDAP-Anbindung im User Management konfiguriert werden. Informationen hierzu finden Sie im **ARIS Server Installation and Administration Guide**, im Kapitel **Set up ARIS for LDAP server operation**.

7.6 Kennwortverschlüsselung in der Laufzeitkonfiguration

Benutzerkennungen, Kennwörter und sonstige sicherheitsrelevante Inhalte waren in der Laufzeitkonfiguration von ARIS Risk & Compliance Manager (**runtimeconfig.xml**) bisher immer im Klartext enthalten. Nun wurde die Möglichkeit geschaffen, sie beim Serverstart verschlüsseln zu lassen. Dazu muss in der gewünschten Parameterzeile das XML-Attribut **encrypted="false"** eingefügt werden. Der Inhalt des Attributs **value** wird dann vom Server beim Hochfahren verschlüsselt, und das Flag **encrypted** wird auf **true** gesetzt. Bedingung dafür ist, dass die XML-Attribute **encrypted** und **value** in derselben Zeile stehen.

Beispiel

Vorher: `<parameter name="dbms.pwd" encrypted="false" value="sox"/>`

Nachher: `<parameter name="dbms.pwd" encrypted="true" value="72a5e995b3996dc0ca5882bf42dafd1e"/>`

Aus Sicherheitsgründen sollte die Konfigurationsdatei nach dem Verschlüsseln mit Schreibschutz versehen werden.

7.7 Konfiguration von Event-Enabling in ARIS Risk & Compliance Manager

Mit ARIS Risk & Compliance Manager besteht die Möglichkeit, Events von einem Messaging-Provider (Standard ist Universal-Messaging) zu abonnieren und daraus in ARIS Risk & Compliance Manager definierte Objekte zu generieren, z. B. Testfälle. Die Konfiguration der Steuerung über Events erfolgt während des Setups oder nachträglich über ARIS Cloud Controller.

Beispiele - Befehle für ARIS Cloud Controller

```
reconfigure arcm_m eventenabling.active="true"
reconfigure arcm_m eventenabling.providerUrl="nsp://localhost:9000"
reconfigure arcm_m eventenabling.eventTypeStoreLocation="
C:/SoftwareAG/common/EventTypeStore"
reconfigure arcm_m eventenabling.configurationLocation="
C:/SoftwareAG/profiles/SPM/configuration"
reconfigure arcm_m
eventenabling.securityFilePath="C:/SoftwareAG/common/conf/event/routing/event-ro
uting-security.xml"
reconfigure arcm_m
eventenabling.classpathJarPath="C:/SoftwareAG/common/lib/event-routing-classpath
.jar"
```

BEDEUTUNG DER PARAMETER

- **eventenabling.active**

Zentrale Angabe zur Aktivierung des Event-Enabling. Ist der Wert false angegeben, wird der Service nicht gestartet. Bei true müssen die weiteren Parameter gültige Werte enthalten.
- **eventenabling.providerUrl**

Der Parameter erwartet die gültige URL einer Universal-Messaging-Server-Instanz, z. B. nsp://localhost:9000.
- **eventenabling.eventTypeStoreLocation**

Der absolute Pfad zu einem lokal verfügbaren Event-Type-Store ist zu hinterlegen. Liegt die Instanz des Universal-Messaging-Servers auf demselben Host, kann der Store dieser Installation verwendet werden. Beispiel: C:\SoftwareAG\common\EventTypeStore
- **eventenabling.configurationLocation**

Der absolute Pfad des Basisverzeichnisses einer spezifischen Event-Routing-Konfiguration wird benötigt. Liegt die Instanz des Universal-Messaging-Servers auf demselben Host, kann das Basiskonfigurationsverzeichnis dieser Installation verwendet werden. Beispiel: C:\SoftwareAG\profiles\SPM\configuration
- **eventenabling.securityFilePath**

In diesem Parameter wird der absolute Pfad der Sicherheitskonfigurationsdatei erwartet. Bei identischem Host kann die Datei der Universal-Messaging-Server-Installation referenziert werden. Beispiel: C:\SoftwareAG\common\conf\event\routing\event-routing-security.xml
- **eventenabling.classpathJarPath**

Dieser Parameter muss den absoluten Pfad auf das Java-Klassenpfadarchiv der benötigten Event-Routing-Framework-Bibliotheken beinhalten. Bei identischem Host kann die Universal-Messaging-Server-Installation referenziert werden. Beispiel: C:\SoftwareAG\common\lib\event-routing-classpath.jar
- **eventenabling.useDurableSubscriptions**

Standardmäßig arbeitet das Event-Enabling mit dauerhaften Abonnements von Messages. Diese Funktionalität kann deaktiviert werden, indem dieser optionale Parameter auf den Wert false gesetzt wird.

UNTERSTÜTZE EVENT TYPEN

Um aus den Events in ARIS Risk & Compliance Manager definierte Objekte zu generieren, werden bestimmte vordefinierte Event-Typen mitgeliefert. Diese müssen in den lokalen Event Type Store und in den Event Type Store des Event-generierenden Systems kopiert werden. Die zugehörigen Dateien für den Event Type Store befinden sich im Hauptverzeichnis des Installationsmediums von ARIS Risk & Compliance Manager im Ordner Event Type Store. Der Inhalt dieses Ordners wird dann in das Hauptverzeichnis des jeweiligen Event Type Store kopiert.

Das Verschicken von Events mithilfe der in ARIS Risk & Compliance Manager mitgelieferten Event-Typen ist Bestandteil von Complex Event Processing. Weitere Informationen hierzu entnehmen Sie bitte der Dokumentation von Complex Event Processing.

BETRIEB EINER AUTARKEN INSTALLATION VON ARIS RISK & COMPLIANCE MANAGER

Liegen ARIS Risk & Compliance Manager und Universal-Messaging-Server nicht auf dem gleichen Host, können die benötigten Konfigurationen und Ressourcen nicht direkt referenziert und verwendet werden. In diesem Fall müssen die folgenden Ressourcen aus der Universal-Messaging-Server-Installation auf das Host-System der Installation von ARIS Risk & Compliance Manager kopiert werden. Zu kopierende Verzeichnisstrukturen (minimales Bundle*):

1. <SAG install directory>\common\conf\event\...
2. <SAG install directory>\common\EventTypeStore\...
3. <SAG install directory>\common\lib\...
4. <SAG install directory>\common\runtime\bundles\...
5. <SAG install directory>\profiles\SPM\configuration\event\routing\...

Anschließend können die kopierten Ressourcen wie zuvor beschrieben in der Event-Enabling-Konfiguration von ARIS Risk & Compliance Manager verwendet werden.

* Weiterführende Information zum Betrieb von Universal-Messaging, insbesondere die Konfiguration durch den Software AG Platform-Manager, entnehmen Sie bitte den produktspezifischen Dokumentationen.

Warnung

Um den fehlerfreien Betrieb und die Kompatibilität zu gewährleisten, achten Sie bitte darauf, die Version der kopierten Ressourcen der Installation von ARIS Risk & Compliance Manager immer mit der Version des verwendeten Universal-Messaging-Servers synchron zu halten.

8 Installation der ARIS Architect-Komponenten

Die Makros und Reporte für ARIS Risk & Compliance Manager sind Bestandteil der ARIS Design Server/ARIS Connect Installation. Die Installation weiterer Komponenten entfällt dadurch.

9 Server von MashZone für die Dashboard-Integration vorbereiten

Sie können die Nutzung von MashZone in ARIS Risk & Compliance Manager aktivieren, um Daten in Dashboards zusammenzuführen, zu kombinieren und anschaulich zu visualisieren. Dafür sind Änderungen an den Servereinstellungen von MashZone erforderlich.

Zwei unterschiedliche Instanzen des User Management können nicht parallel auf einem Computer laufen. Daher benötigen MashZone und ARIS Risk & Compliance Manager jeweils eine eigene Instanz. Die Dashboards von MashZone werden daher von einem anderen Server bereitgestellt, als die Oberfläche von ARIS Risk & Compliance Manager, in die sie eingebettet sind.

Die Umleitung von Inhalten aus MashZone zu anderen Systemen, wie ARIS Risk & Compliance Manager, ist zur Sicherheit standardmäßig in MashZone beschränkt auf die Option **SAMEORIGIN**, d. h. der MashZone-Server antwortet nur auf eigene Anfragen. Deshalb muss die Beschränkung **SAMEORIGIN** in der Datei **mashzone.properties** durch die Option **ALLOW FROM <URI >** ersetzt werden. Nicht alle Browser unterstützen die Option **ALLOW FROM <URI >**. Detaillierte Informationen zu X-Frame-Optionen finden Sie hier <https://developer.mozilla.org/en-US/docs/Web/HTTP/X-Frame-Options>.

Vorgehen

1. Öffnen Sie die Datei **mashzone.properties**
(`<MashZoneInstallDir>\ppmmashzone\server\bin\work\work_mashzone_m\base\webapps\mashzone\WEB-INF\`)
2. Fügen Sie die folgenden Zeilen hinzu:

```
mashzone.httpheader.xframe.options.enabled=true  
mashzone.httpheader.xframe.options=ALLOW FROM <Host-Name von ARIS Risk &  
Compliance Manager>
```

Der Host-Name von ARIS Risk & Compliance Manager muss der Name des Computers sein, auf dem ARIS Risk & Compliance Manager installiert ist und auf dem der Load-Balancer des Servers von ARIS Risk & Compliance Manager läuft, zum Beispiel **arcmserver.subdomain.domain**.
3. Speichern Sie ihre Änderungen.
4. Starten Sie den Server von MashZone erneut.

Der Server von MashZone ist für die Dashboard-Integration vorbereitet.

10 Anbindung an ARIS Publisher

Gemäß dem empfohlenen Vorgehen sollten die Stammdaten (Benutzer, Risiken, Kontrollen, usw.) in ARIS Architect modelliert werden. Nach der Modellierung können diese Daten mit dem Export-Report von ARIS Risk & Compliance Manager exportiert und in ARIS Risk & Compliance Manager importiert werden. Zusätzlich ist es möglich die Datenbank von ARIS Architect mit ARIS Publisher zu veröffentlichen. Nach dem Import der Stammdaten in ARIS Risk & Compliance Manager, kann über die Mandanten die Anbindung an ARIS Publisher konfiguriert werden. Dadurch kann z. B. in ARIS Risk & Compliance Manager von einem Risikoformular auf das Objekt im veröffentlichten Modell verlinkt werden, um den Prozess in ARIS Publisher anzuzeigen.

Voraussetzung

ARIS Risk & Compliance Manager und ARIS Publisher verwenden das gleiche User Management zur Verwaltung von Benutzern. Das User Management für alle ARIS-Produkte, nicht zu verwechseln mit der Administration in ARIS Risk & Compliance Manager, dient zur Verwaltung von Benutzern, Benutzergruppen, Funktions- und Lizenzrechten, Lizenzen, Dokumenten und Konfigurationen. Damit ist die einmalige Anmeldung für verschiedene ARIS-Produkte gewährleistet.

Vorgehen

USER MANAGEMENT

1. Öffnen Sie das User Management.
2. Legen Sie im User Management eine Benutzergruppe und einen Benutzer an.
3. Ordnen Sie dem Benutzer diese Benutzergruppe zu.
4. Ordnen Sie der Benutzergruppe das Funktionsrecht **Publisher-Administrator** zu.

ARIS ARCHITECT

1. Starten Sie **ARIS Architect**.
2. Klicken Sie auf **ARIS > Administration**. Die **Administration** wird angezeigt.
3. Melden Sie sich an der Datenbank an, die Sie exportieren möchten.
4. Klicken Sie in der Navigation auf **Benutzer**. Die Benutzer und Benutzergruppen werden angezeigt.
5. Klicken Sie mit der rechten Maustaste auf die zuvor erstellte Benutzergruppe.
6. Klicken Sie auf **Eigenschaften**.
7. Klicken Sie auf **Funktionsrechte**.
8. Aktivieren Sie das Kontrollkästchen für das Recht **Datenbankexport**. (Die produktspezifischen Berechtigungen werden nicht zentral im User Management zugewiesen, sondern im jeweiligen ARIS-Produkt.)
9. Klicken Sie auf **Zugriffsrechte**.
10. Ordnen Sie der Benutzergruppe mindestens das Zugriffsrecht **Lesen** für die Hauptgruppe zu.
11. Klicken Sie auf **Rechte vererben**, um die Rechte auf alle Untergruppen zu übertragen.
12. Klicken Sie auf **OK**.
13. Veröffentlichen Sie die gewünschte Datenbank.
14. Ändern Sie nach dem Export den Status auf **Aktiviert**.


ARIS PUBLISHER

1. Öffnen Sie ARIS Publisher.
2. Melden Sie sich mit dem Benutzer **root** und dem Kennwort **root** an.
3. Öffnen Sie das Modul **Gruppen**. Die von Ihnen angelegte Benutzergruppe wird angezeigt.
4. Klicken Sie in der Zeile der Gruppe auf **Zuordnen**. Der Dialog wird geöffnet.
5. Ordnen Sie die zuvor im User Management angelegte Gruppe ARIS Publisher zu.
6. Klicken Sie auf **Speichern**.

ARIS RISK & COMPLIANCE MANAGER

1. Öffnen Sie ARIS Risk & Compliance Manager.
2. Öffnen Sie den Mandanten, in den Sie die Stammdaten importiert haben.
3. Tragen Sie in der Zeile **Objektverknüpfung** den ARIS Publisher-Link in folgender Form ein:
4. `http://<BusinessPublisherServer>:19990/businesspublisher/link.do?login=<Benutzername>&password=<Kennwort>&localeid=1033&ph=<exportID>&objectguid={GUID}`
5. Ersetzen Sie die Platzhalter folgendermaßen:
 - a. **<BusinessPublisherServer>** = Name oder IP Adresse des ARIS Publisher-Servers.
 - b. **<Benutzername>** = Name des Benutzers, der zuvor angelegt wurde.
 - c. **<Kennwort>** = Kennwort des Benutzers, der zuvor angelegt wurde.
 - d. **<exportID>**
 1. Öffnen Sie ein Modell in ARIS Publisher.
 2. Klicken Sie mit der rechten Maustaste auf ein Objekt.
 3. Klicken Sie auf **Link kopieren**.
 4. Kopieren Sie im angezeigten Link den Parameter **ph** mit seinem Wert und ersetzen Sie damit **<exportID>**.

Der Platzhalter **{GUID}** muss nicht ersetzt werden. Dieser wird von ARIS Risk & Compliance Manager dynamisch ersetzt.

6. Tragen in das Feld **Modellverknüpfung** den Link ein, den sie in zuvor angelegt haben.
7. Ersetzen Sie den Parameter **objectguid** durch **modelguid**:
`http://<BusinessPublisherServer>:19990/businesspublisher/link.do?login=<Benutzername>&password=<Kennwort>&localeid=1033&ph=<exportID>&modelguid={GUID}`
8. Klicken Sie auf  **Speichern**.
9. Führen Sie einen Test durch.
10. Melden Sie sich bei ARIS Risk & Compliance Manager mit der Rolle **Test-Manager** an.
11. Öffnen Sie ein Risiko, welches durch den Stammdatenimport generiert wurde.
12. Klicken Sie im Feld **Funktion** auf **Objektverknüpfung** und **Modellverknüpfung**.

ARIS Publisher wird in einem neuen Fenster geöffnet. Das entsprechende Objekt oder Modell wird geöffnet, wenn die Anbindung korrekt konfiguriert wurde.

11 Häufige Fehler

Viele Probleme lassen sich nur erkennen und beheben, wenn die entsprechenden Fehlermeldungen analysiert werden. Dazu können Sie die Log-Dateien des Verzeichnisses **<Installationsordner von ARIS Risk & Compliance Manager>\server\bin\work\work_arcm_m\base\logs** heranziehen.

11.1 Datenbankprobleme

SYMPTOM 1

Beim Starten von Tomcat wird in der DOS-Box die Fehlermeldung **java.lang.ClassNotFoundException: oracle.jdbc.driver.OracleDriver** ausgegeben.

URSACHE

Es steht kein JDBC-Treiber zur Verfügung.

ABHILFE

Kopieren Sie den JDBC-Treiber in das Verzeichnis **%CATALINA_HOME%\webapps\arcm\WEB-INF\lib**.

SYMPTOM 2

Beim Starten von Tomcat wird in der DOS-Box die Fehlermeldung **java.sql.SQLException: E/A-Exception: The Network Adapter could not establish the connection** ausgegeben.

URSACHE

Die Datenbank wurde nicht gestartet oder die Verbindungsparameter Adresse, Port und/oder SID wurden nicht korrekt gesetzt.

ABHILFE

Bitte starten Sie die Datenbank oder korrigieren Sie die Verbindungsparameter.

SYMPTOM 3

Beim Starten von Tomcat wird in der DOS-Box die Fehlermeldung **java.sql.SQLException: ORA-01017: invalid username/password; logon denied** ausgegeben.

URSACHE

Das Benutzerkonto für die Datenbankverbindung wurde nicht richtig konfiguriert.

ABHILFE

Korrigieren Sie die Benutzerdaten.

12 Systemvoraussetzungen

12.1 Oracle-System und -Einstellungen

Die folgende Konfiguration zeigt die Minimalkonfiguration. Sie ist auf die Anforderungen Ihres Systems von ARIS Risk & Compliance Manager anzupassen. Dabei richtet sich die Konfiguration des Oracle-Systems nach der Anzahl der parallel auf dem ARCM-Server angemeldeten Benutzer. Bei der Installation des ARCM-Servers muss die Konfiguration des Oracle-Systems und des Connectionpools von ARIS Risk & Compliance Manager aufeinander abgestimmt werden. Außerdem darf zwischen ARCM-Server und Oracle-DBMS keine Firewall installiert sein. Sollte dies unvermeidbar sein, aktivieren Sie die **dead connection detection** des Oracle-DBMS-Systems.

SYSTEM

- Oracle 12c Enterprise Edition (12.1.0.1.0)

ALLGEMEIN

- ARCM-Instanz als Shared-Server-Instanz anlegen
- `shared_servers` = `Processes/10` (minimum 20)
- `open_cursors`: 500
- `session_cached_cursors`: 100
- `sessions`: $(1.1 * \text{Processes}) + 5$
- `processes`: Anzahl der parallel angemeldeten Benutzer (Minimum 1000)
- `checkpoint_interval`: 40000
- `checkpoint_timeout`: 0

SGA

- SGA MAX SIZE: Generell 2/3 des verfügbaren physischen Speichers

TABLESPACE-EINSTELLUNGEN

- SYSTEM: 500 MB (autoextend eingeschaltet)
- TEMP: 300 MB (autoextend eingeschaltet)
- USERS: 3 GB (autoextend eingeschaltet)
- ARCMDATA: 3 GB (autoextend eingeschaltet)
- ARCMINDEX: 8 GB (autoextend eingeschaltet)
- Next-Extent: 100 MB

REDO LOG FILES

Mindestens 20 MB für jede Redo-log-Datei. Eine Redo-log-Datei sollte die Änderungsdaten von einer halben Stunde aufnehmen können.

JDBC-TREIBER

Im Konfigurationsfile **runtimeconfig.xml** von ARIS Risk & Compliance Manager kann ein JDBC-interner Cursorcache aktiviert werden. Der Parameter hierfür ist **dbms.statement.cache.size**. Wir empfehlen diesen Parameter auf 0 zu setzen und diesen Cache zu deaktivieren. Nutzen Sie stattdessen die Datenbanksystemeinstellung **session_cached_cursors** der Oracle-Instanz.

APPLIKATIONSSERVER (EMPFOHLENE KONFIGURATION)

- Prozessor: CPU mit 8 Kernen
- Server:
 - Microsoft® Windows Server 2008 R2 Enterprise
 - Microsoft® Windows 2012
 - Red Hat Linux ES 6.4 (64 bit)
- Hauptspeicher: 8 GB RAM oder mehr
- Controller: SAS (RAID0)
- Festplatten: im RAID-Verbund (Beispiel: RAID0, 2x146 GB (SAS 15000 UPM))
- Software:
 - JDK 1.7.0 (64bit)

DATENBANKSERVER

- Prozessor: Intel Xeon X56xx, 2,4 GHz
- Hauptspeicher: 24 GB RAM oder mehr
- Controller: Zweikanal-Ultra320-SCSI (RAID5)
- Festplatten: im RAID-Verbund (Beispiel: RAID5, 4x146 GB (SAS 15000 UPM))

CLIENT-COMPUTER

- Bildschirmauflösung: Mindestens 1024 x 768 Pixel. Empfohlen werden 1600 x 800 Pixel.
- Software: Microsoft® Internet Explorer Version 9.0, 10.0 und 11.0, Mozilla Firefox Version 23.x oder höher, Google Chrome.

Neuere Versionen sind von Software AG nicht freigegeben, können aber vermutlich verwendet werden.

12.2 Microsoft® SQL-Server-System und -Einstellungen

SYSTEM

- Microsoft® SQL-Server 2012
- Microsoft® SQL-Server 2014

DATENBANKSERVER

- Prozessor: Intel Xeon X56xx, 2,4 GHz
- Hauptspeicher: 24 GB RAM oder mehr
- Controller: Zweikanal-Ultra320-SCSI (RAID5)
- Festplatten: im RAID-Verbund (Beispiel: RAID5, 4x146 GB (SAS 15000 UPM))

12.3 Acrobat Reader

Für das Anzeigen von PDF-Reporten muss Adobe Reader installiert sein.

12.4 Microsoft Office/Excel

Für das Anzeigen von Excel-Berichten muss Microsoft® Excel ab Version 2003 installiert sein.

13 Glossar

Global Unique Identifier (GUID)

Eindeutiger, datenbankübergreifender Identifizierer für Elemente von ARIS.

Java Database Connectivity (JDBC)

Schnittstelle, die die Kommunikation zwischen einer Java-Anwendung und einer Datenbank ermöglicht.

Multi-Purpose Internet Mail Extensions-Mapping (MIME-Mapping)

Verbindet eine Dateinamenextension mit dem Typ der Datendatei, z. B. Text, Audio, Bild.

Service-ID von Oracle (SID)

Eindeutige Kennung, die Oracle benötigt, um die Datenbankinstanz zu identifizieren.

Simple Mail Transfer Protocol (SMTP)

Übertragungsprotokoll speziell für den Austausch von Mails. Es legt beispielsweise fest, wie zwei Mailsysteme interagieren und wie die Steuermeldungen zu diesem Zweck aussehen müssen.

14 Support von Software AG

IM WEB

Mit einem gültigen Support-Vertrag haben Sie Zugriff auf die Lösungsdatenbank.

Klicken Sie auf **<https://empower.softwareag.com/>**
(**<https://empower.softwareag.com/>**).

Bei Fragen zu speziellen Installationen, die Sie nicht selbst ausführen können, wenden Sie sich an Ihre lokale Software AG-Vertriebsorganisation.

TELEFONISCH

Mit einem gültigen Support-Vertrag erreichen Sie den Global Support ARIS unter:

+800 ARISHELP

Dabei steht das "+" für das jeweilige Präfix, um in diesem Land eine internationale Verbindung anzuwählen.

Beispiel für die Anwahl innerhalb Deutschlands mit direkter Amtsleitung: 00 800 2747 4357

15 Disclaimer

ARIS-Produkte sind für die Verwendung durch Personen gedacht und entwickelt. Automatische Prozesse wie das Generieren von Inhalt und der Import von Objekten/Artefakten per Schnittstellen können zu einer immensen Datenmenge führen, deren Verarbeitung wiederum Verarbeitungskapazitäten und physische Grenzen überschreiten können. Physikalische Grenzen können dann überschritten werden, wenn der verfügbare Speicherplatz für die Ausführung der Operationen oder die Speicherung der Daten nicht ausreicht.

Der ordnungsgemäße Betrieb von ARIS Risk & Compliance Manager setzt voraus, dass eine zuverlässige und schnelle Netzwerkverbindung vorhanden ist. Ein Netzwerk mit unzureichender Antwortzeit reduziert die Systemperformanz und kann zu Timeouts führen.

Wenn ARIS-Produkte in einer virtuellen Umgebung genutzt werden, müssen ausreichende Ressourcen verfügbar sein, um das Risiko einer Überbuchung zu vermeiden.

Das System wurde im Szenario **Internal control system** mit 400 gleichzeitig angemeldeten Benutzern getestet. Es enthält 2.000.000 Objekte. Um eine ausreichende Performance zu gewährleisten, empfehlen wir mit nicht mehr als 500 parallel angemeldeten Benutzern zu arbeiten. Kundenspezifische Anpassungen, vor allem in Listen und Filtern, wirken sich negativ auf die Performance aus.

16 Index

A

- ARIS Dokumentablage 24
- ARIS Publisher 35

B

- Benutzer
 - Benutzer in ARIS Risk & Compliance Manager aktualisieren 29
 - Importieren von modellierten Benutzer ins User Management 28
 - Modellierte Benutzer aus ARIS Architect exportieren 28
 - Modellierte Benutzer ins User Management importieren 29

C

- Customizing 21

D

- Datenbankmigration 27
- Datenbankprobleme 38

E

- Einführung 2
- Event-Enabling 30

G

- Global Unique Identifier (GUID) 42

H

- Häufige Fehler 38
 - Datenbankprobleme 38

I

- Installation und Konfiguration
 - Ändern der System-E-Mail-Adressen 20
 - ARIS Architect-Komponenten 33
 - Datenbankinstallation 4
 - Datenbankschema Oracle 5
 - Datenbankschemainstallation Microsoft® SQL-Server 6
 - E-Mail-Funktionalität 19
 - In ARIS integrieren 13
 - Konfigurationsparameter 16
 - Nicht mehr benötigte Komponenten entfernen 14
 - Oracle- oder Microsoft® SQL-Server-Datenbank 4
 - Start der nicht mehr benötigten Komponenten verhindern 15
 - Verzeichnisdienst anbinden 30
 - Wichtige Informationen 3

J

- Java Database Connectivity (JDBC) 42

K

- Kennwortverschlüsselung 30

L

- LDAP 30

M

- Makros und Reporte 33
- Migration 27
- Multi-Purpose Internet Mail Extensions-Mapping 42

N

- Neue Version installieren 22
 - Daten aus ARIS Dokumentablage migrieren 24
 - Daten migrieren 23
 - Daten sichern 22
 - Datenbank von ARIS Risk & Compliance Manager migrieren 27
 - Event-Enabling 30
 - Importieren von modellierten Benutzer ins User Management 28
 - Kennwortverschlüsselung 30
 - Update-Setup ausführen 23
 - Verzeichnisdienst anbinden 30

O

- Oracle
 - Service-ID von Oracle 42

S

- Simple Mail Transfer Protocol (SMTP) 42
- Support 43
- Systemvoraussetzungen
 - Acrobat Reader 41
 - Microsoft® Office/Excel 41
 - Microsoft® SQL-Server 41
 - Oracle-System 39

T

- Test 7
 - Installation 8
 - Produktivsystem 10