



Installationshandbuch

ARIS Risk & Compliance Manager
Version 9.8 - Service Release 1

Juni 2015

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 - 2015 [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	7
5.2	Umstieg von der Testinstallation auf ein Produktivsystem	9
5.3	ARIS Risk & Compliance Manager in bestehende ARIS-Installation integrieren	10
5.3.1	Entfernen der nicht mehr benötigten Runnables.....	11
5.3.2	Start der nicht mehr benötigten Runnables verhindern	12
5.4	Konfigurationsparameter	13
5.5	Konfiguration der E-Mail-Funktionalität	15
5.6	Ändern der System-E-Mail-Adressen	16
6	Installation einer kundenspezifischen Version (Customizing)	17
7	Neue Version von ARIS Risk & Compliance Manager installieren.....	18
7.1	Migration der Datenbank von ARIS Risk & Compliance Manager	19
7.2	Migration der Daten aus ARIS Dokumentablage	21
7.3	Importieren von modellierten Benutzer ins User Management	22
7.3.1	Modellierte Benutzer aus ARIS Architect exportieren.....	23
7.3.2	Modellierte Benutzer ins User Management importieren	23
7.3.3	Benutzer in ARIS Risk & Compliance Manager aktualisieren	24



- 7.4 Anbindung an einen Verzeichnisdienst (LDAP)..... 24
- 7.5 Kennwortverschlüsselung in der Laufzeitkonfiguration..... 24
- 7.6 Konfiguration von Event-Enabling in ARIS Risk & Compliance Manager 25
- 8 Installation der ARIS Architect-Komponenten 27
- 9 Anbindung an ARIS Publisher..... 28
- 10 Häufige Fehler 31
 - 10.1 Datenbankprobleme..... 31
- 11 Systemvoraussetzungen 32
 - 11.1 Oracle-System und -Einstellungen 32
 - 11.2 Microsoft® SQL-Server-System und -Einstellungen 34
 - 11.3 Acrobat Reader 34
 - 11.4 Microsoft Office/Excel..... 34
- 12 Glossar..... 35
- 13 Support von Software AG..... 36
- 14 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 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:

- Oracle- oder Microsoft® SQL-Server-Datenbank
- Datenbankschema von ARIS Risk & Compliance Manager
- Datenbanktreiber für Oracle oder Microsoft® SQL-Server
- Java-Umgebung
- TomEE-Server
- ARIS Risk & Compliance Manager (inklusive benötigter Applikationen wie User Management oder ARIS Dokumentablage)

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

1. Editieren Sie die Datei **install.bat**.
2. Tragen Sie in der Datei **install.bat** anstelle des Ausdrucks in spitzen Klammern das aktuelle Kennwort des SQL-Server-Benutzers **sa** (Systembenutzer) ein.
3. Ersetzen Sie ebenso die Pfadinformation **<pathinfo>**.
4. Starten Sie die Datei **install.bat**.
5. 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 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 eine Oracle- oder MS SQL-Datenbank. Beachten Sie, dass eine Produktivdatenbank neu aufgesetzt werden sollte. Verwenden Sie in Ihrem Produktivsystem keine Testdaten.

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.

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 (Seite 25). Geben Sie dann den Event-Server und den Port an.
16. Klicken Sie auf **Next**. Der Dialog **Datenbanksystem wählen** wird angezeigt.
17. Wählen Sie die gewünschte Datenbank. Die Option **Standard Datenbank System** installiert eine Apache Derby-Datenbank. Wenn Sie Oracle oder MS SQL-Server wählen, ist anschließend ein passender Datenbank-Treiber gewählt werden, welcher dann vom Setup mitinstalliert wird.
18. Tragen Sie den Namen des Datenbankservers ein.
19. Tragen Sie die Portnummer des Datenbankservers ein.
20. Tragen Sie den Service-Namen der Datenbank (Seite 5) ein (Oracle-SID) bzw. den Datenbanknamen (MS SQL-Server) der Datenbankinstanz ein.
21. Tragen Sie den Namen und das Kennwort des Benutzers der Datenbank (Seite 4) ein.
22. Klicken Sie auf **Next**. Der Dialog **System settings** wird angezeigt.
23. Wählen Sie die Installationsgröße aus, um den zugewiesenen Speicher für ARIS Risk & Compliance Manager zu bestimmen: **Demo scenario** = 1GB, **Medium** = 4GB, **Large** = 8G.
24. Klicken Sie auf **Next**.
25. 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 auch möglich ARIS Risk & Compliance Manager auf die Produktivdatenbank umzulenken, indem die Parameter für die Datenbankverbindung angepasst werden. Dazu muss die Parameterliste **dbms** der Datei **runtimeconfig.xml** angepasst werden. Die Datei liegt im Pfad **<ARIS Risk & Compliance Manager-Installationspfad>\server\bin\work\work_arcm_m\base\tomcat\webapps\arcm\WEB-INF**.

Die folgenden Beispiele zeigen die Konfiguration für eine Oracle- und Microsoft® SQL-Server-Anbindung. Bitte setzen Sie für die Anbindung die spezifischen Parameter Ihres DBMS-Systems ein:

Oracle

```
<parameter name="dbms.system" value="oracle"/>
<parameter name="dbms.driver" value="oracle.jdbc.driver.OracleDriver"/>
<parameter name="dbms.url" value="jdbc:oracle:thin:@dbserver:1521:ARCM"/>
<parameter name="dbms.user" value="arcm_db"/>
<parameter name="dbms.pwd" value="arcm_db"/>
```

Microsoft® SQL-Server

```
<parameter name="dbms.system" value="MSSQL"/>
<parameter name="dbms.driver" value="net.sourceforge.jtds.jdbc.Driver"/>
<parameter name="dbms.url"
value="jdbc:jtds:sqlserver://t1labarcm:1433;DatabaseName=arcm"/>
<parameter name="dbms.user" value="arcm_db"/>
<parameter name="dbms.pwd" value="arcm_db_passwort"/>
```

Wenn Sie diese Anpassungen durchgeführt haben, wird der Begriff **Demoversion** nicht mehr auf der Oberfläche von ARIS Risk & Compliance Manager angezeigt.

Nachdem Sie die Datenbank angelegt haben, kann ARIS Risk & Compliance Manager installiert werden. Wenn Sie das Installationsprogramm verwenden, werden alle benötigten Softwarekomponenten auf dem Zielsystem installiert. Aus lizenzrechtlichen Gründen dürfen die Oracle-JDBC-Datenbanktreiber und der Microsoft® SQL Server-Datenbanktreiber nicht mit ausgeliefert werden.



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

Integrieren Sie ARIS Risk & Compliance Manager in die Installation von ARIS Design Server, da ab Version 9.5 Benutzer nicht mehr in ARIS Risk & Compliance Manager angelegt werden. Die Benutzerverwaltung erfolgt nun zentral im User Management. 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.

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. Starten und konfigurieren Sie ARIS Design Server.
3. Installieren (Seite 7) Sie ARIS Risk & Compliance Manager auf einem anderen Server per Setup.
4. Starten Sie den ARIS Cloud Controller der ARIS Risk & Compliance Manager-Installation über **Start > ARIS > ARIS Cloud Controller**.
5. Geben Sie in der Konsole den Befehl **reconfigure arcm_m +zookeeper.connect.string=<ARISDesignServer>\\:2181** ein. Verwenden Sie unbedingt das +-Zeichen vor dem Parameter **zookeeper.connect.string**. Dadurch wird nur dieser Parameter durch den neuen Wert ersetzt.
6. Tragen Sie für den Platzhalter **<ARISDesignServer>** den Namen des Servers ein, den Sie in Schritt 1 für ARIS Design Server verwendet haben.
7. Hatten Sie den Port nicht verändert, bleibt auch hier die Standardeinstellung.
8. Prüfen Sie mit dem Befehl **list**, ob alle Runnables im Status **STOPPED** sind.
9. Starten Sie ARIS Risk & Compliance Manager mit dem Befehl **start arcm_m**. Die Endung **_m** ändert sich, je nachdem welche Installationsgröße (Small, Medium, Large) Sie für den Speicher gewählt haben.

ARIS Risk & Compliance Manager wird mit der Umgebung von 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 den Namen des ARIS Design Server ein, gefolgt von **/arcm**.



Da die anderen Runnables auf dem Server von ARIS Risk & Compliance Manager nicht länger benötigt werden, können diese entweder entfernt (Seite 11) oder so konfiguriert werden, dass sie zukünftig 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 Runnables

Entfernen Sie nicht mehr benötigte Runnables.

Warnung

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

Vorgehen

1. Stellen Sie sicher, dass das Runnable von 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 das Runnables **arcm_s** im Status **STARTED** befindet und alle anderen den Status **STOPPED** besitzen.
3. Geben Sie den Befehl **deconfigureall** ein und bestätigen Sie den Befehl mit **Y**. Dieser Befehl entfernt alle Runnables, die sich im Status STOPPED befinden.

Die nicht benötigten Runnables wurden entfernt.



5.3.2 Start der nicht mehr benötigten Runnables verhindern

Verhindern Sie den Start der nicht mehr benötigten Runnables.

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 Runnables **autostart property** auf **false**:
 - a. **set zoo_m property autostart="false"**
 - b. **set postgres_m property autostart="false"**
 - c. **set couchdb_m property autostart="false"**
 - d. **set elastic_m property autostart="false"**
 - e. **set postgres_m property autostart="false"**
 - f. **set adsadmin_m property autostart="false"**
 - g. **set umcadmin_m property autostart="false"**
 - h. **set loadbalancer_m property autostart="false"**
 - i. **set postgres_m property autostart="false"**

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



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
- generatorJobSOProcess
- monitorJobSOProcess
- 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

Damit ARIS Risk & Compliance Manager automatisch E-Mails versenden kann (z. B. E-Mail an einen Tester, dem ein Testfall zugeordnet wurde), muss die Mail-Funktionalität konfiguriert werden. Zum Versenden von 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. Öffnen Sie die Datei **runtimeconfig.xml**. Sie finden diese Datei unter **<Installationsordner von ARIS Risk & Compliance Manager>\server\bin\work\work_arcm_m\base\webapps\arcm\WEB-INF**.
2. In der Sektion **mailing** müssen die Parameter **smtp.host** (IP-Adresse oder gültiger DNS-Name des Mail-Versand-Servers), **smtp.account** (Benutzername des SMTP-Accounts, wenn auf dem Mail-Server die SMTP-Authentifizierung aktiviert ist), **smtp.password** (Kennwort des SMTP-Accounts, wenn auf dem Mail-Server die SMTP-Authentifizierung aktiviert ist) und **default.sender.address** (Fallback-Absender, falls beim Absenden einer automatischen E-Mail keine gültige E-Mail-Adresse definiert ist) angepasst werden.
3. Starten Sie Apache TomEE-Server neu, um die Änderungen der Mail-Konfiguration zu übernehmen.

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. Sollte es sich um allgemeine Nachrichten, z. B. die Anforderung eines neuen Kennworts handeln, 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 den ARIS Risk & Compliance Manager über **Start > ARIS > Stop ARIS Risk & Compliance Manager**.
4. Geben Sie in der Konsole den Befehl ein **enhance arcm_s with customizing local file <Pfad\\Zum\\Customizing\\Zip>**. Der Name des ARIS Risk & Compliance Manager Runnables ist von der Installationsart abhängig. Möglich sind die Namen **arcm_s**, **arcm_m** oder **arcm_l**. Achten Sie bitte darauf, dass Sie stets zwei 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. Es ist dann nicht mehr notwendig zuerst die bestehende Installation zu deinstallieren, um die neue Version zu installieren. Dennoch sollten Sie einige Einstellungen der bestehenden Installation notieren, um diese nach dem Update wieder zu konfigurieren.

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. Auch der Download-Ordner wird gesichert, der alle erstellten PDF- und Excel-Reporte sowie Mandanten- und Datenbanksicherungen enthält.

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 eventuell in der runtimeconfig.xml gemacht haben (z. B. Jobeinstellungen), müssen nach dem Update wieder in die aktualisierte runtimeconfig.xml übernommen werden.



7.1 Migration der Datenbank von ARIS Risk & Compliance Manager

Sie müssen Ihre bestehende Datenbank 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 4.0.0.2 auf 4.0.0.6. Führen Sie vor der Migration eine Sicherung der Datenbank durch. Um Ihr Produktivsystem nicht zu beeinträchtigen, empfehlen wir Ihnen die Migration in einem Testsystem von ARIS Risk & Compliance Manager auszuführen. Dazu sollte außerdem ein unabhängiger Server von ARIS Risk & Compliance Manager verwendet werden.

Die Datenbankmigration kann nur Datenbanken ab der Version 3.1 SR4 von ARIS Risk & Compliance Manager in das neue Datenbankschema migrieren. Es ist nicht möglich einen Datenbestand der Version 3.1 von ARIS Risk & Compliance Manager zu exportieren, um ihn ohne Migration anschließend in die aktuelle Version zu importieren. Der Import würde fehlschlagen. Möchten Sie eine ältere Version als 3.1 SR4 migrieren, wenden Sie sich bitte an den Global Support <_aris> (Seite 36).

Warnung

Die Migration kann nicht rückgängig gemacht werden.

Vorgehen

1. Sichern Sie die Daten Ihrer Produktivdatenbank. Wenn Sie Oracle nutzen, verwenden Sie **dataPump**.
2. Legen Sie einen neuen Datenbankbenutzer an und importieren Sie die Datensicherung für diesen Benutzer.
3. Konfigurieren Sie ARIS Risk & Compliance Manager für die Migration.
 - a. Setzen Sie den Parameter **autoStartMigration** in der Datei **runtimeconfig.xml** auf **true**.
 - b. Setzen Sie den Parameter **application.scheduler.startup** in der Datei **runtimeconfig.xml** auf **false**.
 - c. Setzen Sie den Log-Level in der Datei **log4j.properties** für die Parameter **log4j.logger.com.idsscheer.webapps.arcm** und **log4j.logger.com.idsscheer.webapps.arcm.dl.framework** auf **DEBUG**.
4. Speichern Sie die Datei **runtimeconfig.xml** und starten Sie den ARCM-Server. Die Migration startet automatisch.
5. Melden Sie sich nach der Migration als Systembenutzer bei ARIS Risk & Compliance Manager an.
6. Führen Sie in der **Administration** einen Datenbankexport durch und beenden Sie den ARCM-Server.
7. Legen Sie einen neuen Datenbankbenutzer (Seite 4) an, konfigurieren Sie die Datenbankverbindung in der Datei **runtimeconfig.xml** und starten Sie den ARCM-Server.



8. Importieren Sie die Datenbank, die Sie vorher exportiert haben.
9. Beenden Sie den ARCM-Server, sichern Sie die Datenbank und starten Sie den ARCM-Server erneut.
10. Vergleichen Sie die Datenbank der Version 3.1 SR4 stichprobenhaft mit der migrierten Datenbank.
 - a. Melden Sie sich mit verschiedenen Rollen an und prüfen Sie verschiedene Listen und Objekte.
 - b. Melden Sie sich als Tester an und prüfen Sie verschiedene Listen und Objekte.
 - c. Melden Sie sich als Systembenutzer an. Legen Sie eine Test-Manager-Gruppe an. Ordnen Sie einen Benutzer zu, melden Sie sich mit diesem Benutzer an und prüfen Sie die Liste der Testfälle.
 - d. Prüfen Sie die Anwendungsfälle Ihres Unternehmens.
11. Nachdem die Tests erfolgreich durchgeführt wurden, importieren Sie die Datenbanksicherung noch einmal in die getestete Datenbank, um die Testdaten zu entfernen.
12. Konfigurieren Sie den Produktivserver.
 - a. Setzen Sie den Parameter **autoStartMigration** in der Datei **runtimeconfig.xml** auf **false**.
 - b. Setzen Sie den Parameter **application.scheduler.startup** in der Datei **runtimeconfig.xml** auf **true**.
 - c. Setzen Sie den Log-Level in der Datei **log4j.properties** für die Parameter **log4j.logger.com.idsscheer.webapps.arcm** und **log4j.logger.com.idsscheer.webapps.arcm.dl.framework** auf **ERROR**.
13. Starten Sie den Produktivserver.

Die Datenbank wurde migriert.



7.2 Migration der Daten aus ARIS Dokumentablage

Migrieren Sie auch die Daten von ARIS Dokumentablage, wenn Sie von Version 4.x/4.1.x zur aktuellen Version wechseln. In den Versionen 4.x gab es für ARIS Business Server mit Anbindung an ARIS Governance Engine und ARIS Risk & Compliance Manager separate Installationen von ARIS Dokumentablage. In Version 9.x gibt es nur noch eine gemeinsamen ARIS Dokumentablage, welche die Daten intern getrennt verwaltet. Um die Daten zu migrieren, kopieren Sie die couchDB-Daten von ARIS Business Server 7.2 und von ARIS Risk & Compliance Manager 4.x in ein Verzeichnis des Servers, auf dem Version 9.x von ARIS Risk & Compliance Manager installiert ist.

Vorgehen

1. Starten Sie ARIS Cloud Controller (**Start > ARIS > Administration > ARIS Cloud Controller**).
2. Stoppen Sie alle Komponenten mit dem Befehl **stopall**.
3. Starten Sie die Komponenten Zookeeper, ElasticSearch und User Management mit den folgenden Befehlen:
 - a. **start zoo_s**
 - b. **start elastic_s**
 - c. **start umcadmin_s**
4. Kopieren Sie den Ordner **couchdb** unter **<Process Governance Installationsverzeichnis>\ads\adsdata** in ein beliebiges Verzeichnis.
5. Kopieren Sie den Ordner **couchDB** unter **<ARCM-Installationsverzeichnis>\couchdb\var\lib\couchdb** in ein beliebiges Verzeichnis. Es darf nicht dasselbe Verzeichnis wie in Schritt 1 sein.
6. Öffnen Sie eine Kommandozeile und navigieren Sie in das Verzeichnis **<ARIS Risk & Compliance Manager Installationsordner>\server\bin\work\work_adsadm_m\tools\bin** und führen Sie für die Migration der CouchDB-Daten von Process Governance folgenden Befehl aus:


```
y-admintool.bat migrate -s <couchDB Pfad aus Schritt 1> -t
<ARCM-Installationsverzeichnis>\server\bin\work\work_couchdb_m\data
```
7. Führen Sie für die Migration der CouchDB-Daten von ARIS Risk & Compliance Manager folgenden Befehl aus:


```
y-admintool.bat migrate -r arcm -s <couchDB Pfad aus Schritt 2> -t
<ARCM-Installationsverzeichnis>\server\bin\work\work_couchdb_m\data
```
8. Starten Sie alle Komponenten mit dem Befehl **startall** im ARIS Cloud Controller.
9. Führen Sie mit dem Befehl **y-admintool.bat -t default reindex -u <USER> -p <PASSWORD>** im Verzeichnis **<ARCM-Installationsverzeichnis>\server\bin\work\work_couchdb_m\tools\bin** eine Reindexierung durch, auch wenn Sie die Volltextsuche nicht nutzen.



10. Ersetzen Sie **<USER>** und **<PASSWORD>** durch die Anmeldedaten eines Benutzers der das Funktionsrecht **Dokumentenadministrator** hat.

Die Migration der Daten von ARIS Dokumentablage ist abgeschlossen. Starten Sie alle Komponenten von ARIS Risk & Compliance Manager. Überprüfen Sie die Migration indem Sie in ARIS Risk & Compliance Manager ein verknüpftes Dokument öffnen.

Die Dokumente aus der CouchDB von ARIS Governance Engine stehen zur Verfügung. Die Dokumente aus der CouchDB von ARIS Risk & Compliance Manager müssen in ARIS Risk & Compliance Manager überprüft werden.

7.3 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 synchronisiert werden. Der Report **ARCM-Benutzerexport für das User Management** erledigt dies automatisiert, indem alle modellierten Benutzer einer Datenbank (Objekttyp **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**.



7.3.1 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.

7.3.2 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 importierte Benutzer vergeben. Möchten Sie kein Kennwort vergeben, drücken Sie die Eingabetaste ohne ein Kennwort einzugeben.

Die Benutzer werden ins User Management importiert.



7.3.3 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.

7.4 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**.

7.5 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.



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

Mit ARIS Risk & Compliance Manager besteht die Möglichkeit, Events von einem JMS 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 über zwei Dateien im Installationsverzeichnis von ARIS Risk & Compliance Manager:

- `<ARCM-Installationsverzeichnis>\WEB-INF\com.softwareag.eda.nerv.properties`
- `<ARCM-Installationsverzeichnis>\WEB-INF\runtimeconfig.xml`

`com.softwareag.eda.nerv.properties`

Innerhalb dieser Datei wird die Verbindung zum zugehörigen JMS Provider eingetragen. Dazu muss der Servername und des Brokers und dessen Port bekannt sein.

Beispiel

```
com.softwareag.eda.nerv.default.jms.provider=nsp://localhost:9000
```

Die Verbindung zum lokal verfügbaren Event Type Store wird unter dem Eigenschaftsschlüssel `com.softwareag.eda.nerv.eventtypestore.location` in Form eines Pfades ([event type store path]) eingetragen.

Beispiel

```
com.softwareag.eda.nerv.eventtypestore.location=C:/SoftwareAG/common/EventTypeStore
```

`runtimeconfig.xml`

Der zur Verfügung stehende JMS Provider kann über eine Parameterliste in der `runtimeconfig.xml` in ARIS Risk & Compliance Manager eingebunden werden.

Beispiel

Für die Event-Anbindung sieht eine typische Parameterliste wie folgt aus:

```
<section id="eventenabling">
  <parameterList name="provider_1">
    <parameter name="active" value="true"/>
    <parameter name="edaConfigUri"
      value="com.softwareag.eda.nerv.properties"/>
  </parameterList>
</section>
```



Bedeutung der Parameter:

- **active**

Angabe ob der Eventservice zur Verfügung steht. Sollte **false** angegeben sein, wird der Service nicht gestartet.

- **edaConfigUri**

Pfad zur **com.softwareag.eda.nerv.properties** der Konfiguration des JMS Provider. Sollte nur der Dateiname angegeben werden, wird diese Datei im gleichen Verzeichnis wie die **runtimeconfig.xml** gesucht. Dies ist auch die vordefinierte Standardeinstellung.

Unterstützte 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.



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 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**:
8. `http://<BusinessPublisherServer>:19990/businesspublisher/link.do?login=<Benutzername>&password=<Kennwort>&localeid=1033&ph=<exportID>&modelguid={GUID}`
9. Klicken Sie auf  **Speichern**.
10. Führen Sie einen Test durch.
11. Melden Sie sich bei ARIS Risk & Compliance Manager mit der Rolle **Test-Manager** an.
12. Öffnen Sie ein Risiko, welches durch den Stammdatenimport generiert wurde.
13. 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.



10 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.

10.1 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.



11 Systemvoraussetzungen

11.1 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)
- ARCMATA: 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
- Server:
 - Microsoft® Windows Server 2008 R2 Enterprise
 - Microsoft® Windows Server 2008 R2 Enterprise (64bit)
 - Microsoft® Windows Server 2012 (64Bit)
- 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.



11.2 Microsoft® SQL-Server-System und -Einstellungen

System

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

Datenbankserver

- Prozessor: Intel Xeon X56xx, 2,4 GHz
- Server:
 - Microsoft® Windows Server 2008 R2 Enterprise
 - Microsoft® Windows 2003 Server Enterprise Edition mit PAE-Option (5.2.3790)
- Hauptspeicher: 24 GB RAM oder mehr
- Controller: Zweikanal-Ultra320-SCSI (RAID5)
- Festplatten: im RAID-Verbund (Beispiel: RAID5, 4x146 GB (SAS 15000 UPM))

11.3 Acrobat Reader

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

11.4 Microsoft Office/Excel

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



12 Glossar

Klicken Sie auf einen Buchstaben, um die zugehörigen Einträge anzuzeigen.

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.



13 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



14 Index

A

ARIS Dokumentablage 21
ARIS Publisher 28

B

Benutzer
 Benutzer in ARIS Risk & Compliance
 Manager aktualisieren 24
 Importieren von modellierten Benutzer
 ins User Management 22
 Modellierte Benutzer aus ARIS Architect
 exportieren 23
 Modellierte Benutzer ins User
 Management importieren 23

D

Datenbankmigration 19
Datenbankprobleme 31

E

Einführung 2

H

Häufige Fehler 31
 Datenbankprobleme 31

I

Installation und Konfiguration
 Ändern der System-E-Mail-Adressen 16
 ARIS Architect-Komponenten 27
 Datenbankinstallation 4
 Datenbankschema Oracle 5
 Datenbankschemainstallation Microsoft®
 SQL-Server 6
 E-Mail-Funktionalität 15
 In ARIS integrieren 10
 Konfigurationsparameter 13
 Nicht mehr benötigte Runnables
 entfernen 11
 Oracle- oder Microsoft®
 SQL-Server-Datenbank 4
 Start der nicht mehr benötigten
 Runnables verhindern 12
 Verzeichnisdienst anbinden 24
 Wichtige Informationen 3

K

Kennwortverschlüsselung 24

L

LDAP 24

M

Makros und Reporte 27
Migration 19

N

Neue Version installieren 18

S

Support 36
Systemvoraussetzungen
 Acrobat Reader 34
 Microsoft® Office/Excel 34
 Microsoft® SQL-Server 34
 Oracle-System 32

T

Test 7
 Installation 7
 Produktivsystem 9