ARIS RISK AND COMPLIANCE

ADMINISTRATIONS-HANDBUCH

VERSION 10.0 - SERVICE RELEASE 18

MAI 2022

This document applies to ARIS Risk and Compliance Version 10.0 and to all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Inhalt

1 Einleitung

ARIS Risk and Compliance ist eine Web-Anwendung. ARIS Risk and Compliance 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 oder für kleine Umgebungen (bis zu 50 gleichzeitige Benutzer) können Sie ARIS Risk and Compliance mit der Datenbank **PostgreSQL** verwenden. Für den Produktivbetrieb benötigen Sie das Datenbanksystem **Oracle** oder **Microsoft®-SQL-Server**.

2 Administration

2.1 Externe Ereignisse integrieren

Die Steuerung von Prozessen in ARIS Risk and Compliance kann durch externe Events erfolgen. Die eingehenden Events lösen die Generierung von bestimmten Objekten in ARIS Risk and Compliance mit vorgegebenen Status aus. Für das Event-Enabling wird eine Verbindung zu einem Messaging-Provider hergestellt. Kontrollausführungen, Vorfälle, Issues, Risikobewertungen und Kontrolltests können automatisch generiert werden.

Der Subscription-Manager kann unter **Administration > Integration > Subscription-Management > Subscriptions** ein Objekt mit bestimmten Attributen und Standardwerten anlegen (Seite 6), das dann durch ein eingehendes Event z. B. die Generierung eines Issues auslöst. Enthält das eingehende Event bereits alle benötigten Attributdefinitionen, werden die in ARIS Risk and Compliance festgelegten Werte ignoriert.

Detaillierte technische Informationen zum Event-Enabling finden Sie in den Handbüchern ARCM - Administration Guide (../../../../../abs/help/de/documents/4 Administration/41 Basic (Single node)/ARCM - Administration Guide.pdf) (Kapitel **Configuration of event enabling in ARIS Risk and Compliance**) und ARCM - Customizing Guide (../../../../../abs/help/en/documents/5 Customizing/ARCM - Customizing Guide.pdf) (Kapitel **Adapt and extend event enabling**).

ARIS Videotutorial

Event-Enabling (ca. 7 Minuten)

Online-Version (http://www.ariscommunity.com/videos/lernen-sie-wie-sie-prozesse-arcm-durch-externe-ereignisse-steuern) in ARIS Community.

Wenn Ihr Computer nicht mit dem Internet verbunden ist, verwenden Sie bitte die Offline-Version (../videos/arcm_event_enabling_de.mp4).

2.1.1 Was ist Event-Enabling?

Die Steuerung von Prozessen in ARIS Risk and Compliance kann durch externe Events erfolgen. Die eingehenden Events lösen die Generierung von bestimmten Objekten in ARIS Risk and Compliance mit vorgegebenen Status aus. Für das Event-Enabling wird eine Verbindung zu einem Messaging-Provider hergestellt. Kontrollausführungen, Vorfälle, Issues, Risikobewertungen und Kontrolltests können automatisch generiert werden.

Der Subscription-Manager kann unter **Administration > Integration > Subscription-Management > Subscriptions** ein Objekt mit bestimmten Attributen und Standardwerten anlegen (Seite 6), das dann durch ein eingehendes Event z. B. die

Generierung eines Issues auslöst. Enthält das eingehende Event bereits alle benötigten Attributdefinitionen, werden die in ARIS Risk and Compliance festgelegten Werte ignoriert.

Detaillierte technische Informationen zum Thema **Event-Enabling anpassen und erweitern** finden Sie im **ARCM - Customizing-Handbuch**.

ARIS Videotutorial

Event-Enabling (ca. 7 Minuten)

Online-Version (http://www.ariscommunity.com/videos/lernen-sie-wie-sie-prozesse-arcm-durch-externe-ereignisse-steuern) in ARIS Community .

2.1.2 Konfiguration des Event-Enabling in ARIS Risk and Compliance

ARIS Risk and Compliance bietet die Möglichkeit, Events von einem Messaging-Provider (Standard: Universal-Messaging digitaler Ereignisservices) zu abonnieren und daraus in ARIS Risk and Compliance definierte Objekte zu generieren, z. B. Kontrolltests. Die Steuerung durch Events wird während des Setups oder nachträglich über ARIS Cloud Controller konfiguriert. Sie können sich auch das Videotutorial **Event-Enabling** in der Online-Hilfe ansehen.

Beispiele - Befehle für ARIS Cloud Controller

```
reconfigure arcm_m arcm.config.eventProviderActive="true"
reconfigure arcm_m arcm.config.eventProviderUrl="nsp://localhost:9000"
reconfigure arcm_m
arcm.config.eventSagInstallationLocation="C:/SoftwareAG"
reconfigure arcm_m
arcm.config.eventRoutingConfigurationLocation="C:/EventsRoutingConfigurat
ion
reconfigure arcm_m
arcm.config.eventProviderServiceAlias="UniversalMessaging"
reconfigure arcm_m arcm.config.useDurableEventSubscriptions="true"
```

BEDEUTUNG DER PARAMETER

- **arcm.config.eventProviderActive**

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

- **arcm.config.eventProviderUrl**

  Der Parameter muss die gültige URL einer Universal-Messaging-Server-Instanz enthalten, z. B. **nsp://eventserver:9000**.

- **arcm.config.eventProviderServiceAlias**

  Die Kennung des Services bzw. der zu verwendenden Nachrichteneinstellungen. Standard ist **UniversalMessaging**.

- **arcm.config.eventSagInstallationLocation**

  Gibt den absoluten Pfad zum Wurzelverzeichnis einer lokalen SAG-Installation oder zum Wurzelverzeichnis des extrahierten Nicht-OSGi-Client-Archivs an. Beispiel: **C:\SoftwareAG**
- **arcm.config.eventRoutingConfigurationLocation**

  Gibt den absoluten Pfad zu einem beliebigen Verzeichnis an, an dem die Routing-Konfiguration gespeichert ist. Beim ersten Starten der Anwendung wird automatisch das Unterverzeichnis **DigitalEventServices** angelegt, um die Out-of-the-box-Konfiguration zu speichern. Beispiel: **C:\EventsRoutingConfiguration**
- **arcm.config.useDurableEventSubscriptions**

  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.

DIGITALE EREIGNISTYPEN UNTERSTÜTZEN

Um aus den in ARIS Risk and Compliance empfangenen Ereignissen definierte Objekte zu generieren, werden vordefinierte digitale Ereignistypen mitgeliefert. Beim ersten Starten der Anwendung werden die unter dem Namensraum **des.aris.arcm** gebündelten, spezifischen digitalen Ereignistypen automatisch im Standardspeicherort der **Event-Typen** der SAG-Installation angelegt. Beispiel: **C:/SoftwareAG/common/DigitalEventServices/TypeRepository/eventtypes/des/aris/arcm**

Diese müssen in das TypeRepository des Event-generierenden Systems kopiert werden. Das Verschicken von Events mithilfe der in ARIS Risk and Compliance mitgelieferten digitalen Ereignistypen 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 AND COMPLIANCE

Liegen ARIS Risk and Compliance und Universal-Messaging-Server nicht auf dem gleichen Host, können die benötigten Konfigurationen und Ressourcen nicht direkt referenziert und verwendet werden. In diesem Fall können die Ressourcen mit dem Tool **NonOsgiClientArchiveCreator**, das im Ordner **Add-ons/UniversalMessaging/ARCM** der ARIS-Installation zur Verfügung steht, aus der SAG-Installation extrahiert werden. **NonOsgiClientArchiveCreator.zip** muss in das Host-System der SAG-Installation entpackt werden, anschließend kann **createClientArchive** (Batch-Skript oder Shell-Skript) ausgeführt werden. Beide Skripte benötigen eine vorhandene Java-Laufzeitinstallation auf dem Host-System. Bei einem Linux-System müssen möglicherweise die Berechtigungen für den Wurzelordner des entpackten Tools geändert werden, z. B. sudo chmod –R 777 ./ . Das Skript **creatClientArchive** fragt den Pfad der lokalen SAG-Installation ab und extrahiert dann alle erforderlichen Ressourcen, einschließlich der Lizenzinformationen, in das Archiv

./build/UniversalMessagingNonOsgiClient.zip. Das Archiv **UniversalMessagingNonOsgiClient.zip** muss anschließend in das Host-System der ARIS Risk and Compliance-Installation entpackt und referenziert werden, wie bereits für den Konfigurationsparameter **arcm.config.eventSagInstallationLocation** beschrieben.

*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 and Compliance immer mit der Version des verwendeten Universal-Messaging-Servers synchron zu halten.

2.1.3 Voraussetzungen für das Generieren von Event-Typen

Je nach Event-Typ gelten für das Event-Enabling bestimmte Bedingungen zum Generieren der Objekte.

KONTROLLAUSFÜHRUNGEN

Kontrollausführungen können nur in folgenden Status durch ein Event generiert werden:

- Status der Kontrollausführungsdokumentation **Neu**, **In Bearbeitung**, **Abgeschlossen** und **Nicht durchführbar**.

Das Attribut **Ereignisgesteuerter Task erlaubt** muss aktiviert sein. Abhängig vom Status der Kontrollausführungsdokumentation muss das Event die entsprechenden Pflichtangaben liefern.

VORFÄLLE

Vorfälle können nur in folgenden Status durch ein Event generiert werden:

- Owner-Status **Neu**, **In Bearbeitung** und **Geschlossen**
- Reviewer-Status **Nicht gewählt**

Ist als verantwortliche Owner- und Reviewer-Gruppe eine Gruppe mit der Rolle **Verlust-Owner** zugeordnet, kann ein Vorfall mit Owner-Status **Geschlossen** und Reviewer-Status **Akzeptiert** generiert werden. Die Systemabfrage, ob der Vorfall auch gleichzeitig freigegeben werden soll, wird intern beim Generieren immer automatisch mit **Ja** beantwortet. Dies ist ein Sonderfall, in dem ein Vorfall direkt abschließend durch einen Reviewer bearbeitet werden kann.

Enthält das auslösende Event die Werte für **Erwarteter Verlustwert** und **Währung**, werden die in ARIS Risk and Compliance festgelegten Werte ignoriert. Abhängig vom Owner-Status muss das Event die entsprechenden Pflichtangaben liefern.

ISSUES

Issues können nur in folgenden Status durch ein Event generiert werden:

- Creator-Status **Freigegeben**
- Owner-Status **Neu**
- Reviewer-Status **Nicht gewählt**

Abhängig vom Creator- und Owner-Status muss das Event die entsprechenden Pflichtangaben liefern.

RISIKOBEWERTUNGEN

Risikobewertungen können nur in folgenden Status durch ein Event generiert werden:

- Owner-Status **Neu**
- Reviewer-Status **Nicht gewählt**

Für das zugeordnete Risiko muss das Attribut **Ereignisgesteuerter Task erlaubt** aktiviert sein.

KONTROLLTESTS

Kontrolltests können nur in folgenden Status durch ein Event generiert werden:

- Teststatus **Neu**, **In Bearbeitung**, **Kontrolle effektiv** und **Kontrolle nicht effektiv**
- Reviewer-Status **Nicht gewählt**

Für die zugeordnete Kontrolltestdefinition muss das Attribut **Ereignisgesteuerter Task erlaubt** aktiviert und die Testfrequenz **Ereignisgesteuert** gewählt sein.

Ist in ARIS Risk and Compliance kein Wert für **Kontrollfrequenz (Ist)** vorgegeben und das Event enthält hierzu auch keine Information, wird der Wert aus dem in ARIS Risk and Compliance festgelegten Wert für **Kontrollfrequenz (Soll)** übernommen.

Abhängig vom Owner-Status muss das Event die entsprechenden Pflichtangaben liefern.

2.1.4 Subscription anlegen

Sie können mit Event-Enabling (Seite 2) ARIS Risk and Compliance mit einem Messaging-Provider verbinden. Dadurch können in ARIS Risk and Compliance Events empfangen werden, um automatisiert Objekte mit bestimmten Attributen und Standardwerten anzulegen, z. B. ein Issue. Enthält das eingehende Event bereits alle benötigten Attributdefinitionen, werden die in ARIS Risk and Compliance festgelegten Werte ignoriert. Kontrollausführungen, Vorfälle, Issues, Risikobewertungen und Kontrolltests können automatisch generiert werden.

Voraussetzung

- Sie haben die Rolle **Subscription-Manager**.

- Sie haben die Rechte für den gewünschten Objekttyp. Beispiel: Wenn Sie ein TestcaseEvent erstellen möchten, müssen Sie die Rolle **Test-Manager** haben. Dies gilt nicht für Issues.
- Event-Enabling ist in ARIS Risk and Compliance konfiguriert (Seite 3).
- Die Voraussetzungen (Seite 5) zum Generieren des jeweiligen Event-Typs sind erfüllt.

Vorgehen

1. Klicken Sie auf **Administration > Integration**.
2. Klicken Sie unter **Subscription-Management** auf **Subscriptions**. Die Liste wird angezeigt.
3. Klicken Sie auf ✚ **Anlegen**. Das Formular **Subscriptions**wird angezeigt.
4. Sind Sie mehreren Umgebungen zugeordnet, wählen Sie die Umgebung, für die Sie die Subscription anlegen möchten.
5. Geben Sie einen Namen für die Subscription und, falls gewünscht, eine Beschreibung ein.
6. Wählen Sie den **Event-Typ**. Je nachdem, welchen Event-Typ Sie wählen, werden die für den entsprechenden Objekttyp relevanten Attribute unter **Filter** und **Standardwerte** angezeigt.
7. Legen Sie unter Beachtung der Bedingungen (Seite 5) für die komplexe Ereignisverarbeitung die gewünschten Filter und Standardwerte fest.
8. Haben Sie mehr als einen Filter oder Standardwert festgelegt, können Sie die Reihenfolge der Zeilen per Drag & Drop neu anordnen.
9. Klicken Sie auf 🖫 **Speichern**.

Die Subscription wird angelegt. Empfängt ARIS Risk and Compliance ein externes Ereignis, wird der in der Subscription festgelegte Event-Typ generiert. Beim Generieren von Kontrolltestsn und Risikobewertungen wird immer die aktuelle Version des zugeordneten Objekts verwendet. D. h., wurde nach dem Anlegen der Subscription das zugeordnete Objekt verändert, wird die aktuelle Version dieses Objekts berücksichtigt. Das generierte Objekt wird dann dem zugeordneten Bearbeiter in seiner Liste der zu bearbeitenden Objekte angezeigt. Die verantwortlichen Benutzer werden automatisch per E-Mail benachrichtigt.

Detaillierte technische Informationen zum Thema **Event-Enabling anpassen und erweitern** finden Sie im **ARCM - Customizing-Handbuch**.

ARIS Videotutorial

Event-Enabling (ca. 7 Minuten)

Online-Version (http://www.ariscommunity.com/videos/lernen-sie-wie-sie-prozesse-arcm-durch-externe-ereignisse-steuern) in ARIS Community.

2.2 Modellierte Benutzer übertragen

Die Verwaltung der Benutzer erfolgt für alle ARIS-Produkte zentral in ARIS Administration/User Management. In Situationen ohne produktive ARIS Administration / produktives User Management, beispielsweise bei Schulungen oder Demos, können Sie

- die modellierten Benutzer aus ARIS Architect exportieren.
- sie in die Benutzerverwaltung von ARIS Administration/User Management importieren, und anschließend
- die Benutzer in ARIS Risk and Compliance mit Benutzern in ARIS Administration/User Management synchronisieren (Seite 10), um die Benutzerkonten in ARIS Risk and Compliance zu übertragen.

Detaillierte Informationen zur Verwaltung von Benutzern in ARIS Administration/User Management finden Sie in der **ARIS Administration**-Hilfe in ARIS oder in der User Management-Hilfe.

2.2.1 Modellierte Benutzer exportieren

Die Verwaltung der Benutzer erfolgt für alle ARIS-Produkte zentral in ARIS Administration/User Management. In Situationen ohne produktive ARIS Administration / produktives User Management, beispielsweise bei Schulungen oder Demos, können Sie

- die modellierten Benutzer aus ARIS Architect exportieren.
- sie in die Benutzerverwaltung von ARIS Administration/User Management importieren, und anschließend
- die Benutzer in ARIS Risk and Compliance mit Benutzern in ARIS Administration/User Management synchronisieren (Seite 10), um die Benutzerkonten in ARIS Risk and Compliance zu übertragen.

Detaillierte Informationen zur Verwaltung von Benutzern in ARIS Administration/User Management finden Sie in der **ARIS Administration**-Hilfe in ARIS oder in der User Management-Hilfe.

Folgende Attribute eines Benutzers werden exportiert: Anmeldung, Vorname, Nachname und 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 **ARIS Risk and Compliance (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 **ARIS Risk and Compliance (Contribute)** zugeordnet.
- Bei allen anderen Rollenzuordnungen erhält der Benutzer das Lizenzrecht **ARIS Risk and Compliance (Operate)**.

Voraussetzung

- Sie benötigen das Zugriffsrecht **Lesen** für die Gruppen, in denen die Datenbankelemente gespeichert werden.
- Die Elemente wurden gespeichert.
- Sie können auf dieses Skript zugreifen. Der Zugriff auf Skripte kann auf bestimmte Benutzergruppen beschränkt sein.

Vorgehen

1. Starten Sie ARIS Architect.
2. Klicken Sie auf **ARIS >** **Explorer**. Die Registerkarte **Explorer** wird geöffnet.
3. Klicken Sie in der Leistenanzeige auf **Navigation**, wenn die Leiste **Navigation** noch nicht aktiviert ist.
4. Öffnen Sie die Datenbank, deren modellierte Benutzer Sie exportieren möchten.
5. Klicken Sie mit der rechten Maustaste auf die Hauptgruppe.
6. Klicken Sie auf **Auswerten > Report starten**.
7. Wählen Sie die Kategorie von **ARIS Risk and Compliance**.
8. Wählen Sie den Report **ARCM-Benutzerexport für die Benutzerverwaltung**.
9. Klicken Sie auf **Weiter** und dann auf **Fertigstellen**.

Eine Textdatei mit den Attributen Anmeldung, Vorname, Nachname sowie E-Mail-Adresse wird exportiert. Es werden die Benutzer angezeigt, die wegen fehlender Attribute vom Export ausgeschlossen wurden. Sie haben so die Möglichkeit, die benötigten Attribute einzutragen und durch erneutes Starten des Reports alle Benutzer zu exportieren.

Importieren (Seite 9) Sie nun die Benutzer mit der Datei **create_user.bat** in ARIS Administration/User Management.

2.2.2 Importieren von modellierten Benutzer in ARIS Administration/User Management

Importieren Sie die modellierten Benutzer ins User Management.

Vorgehen

1. Legen Sie das Installationsmedium von ARIS Risk and Compliance 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 die Benutzerverwaltung** 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 in die Benutzerverwaltung von ARIS Administration/User Management importiert.

Anschließend synchronisieren (Seite 10) Sie die Benutzer in ARIS Risk and Compliance mit Benutzern in ARIS Administration/User Management.

2.2.3 Benutzer mit ARIS Administration/User Management synchronisieren

Um aktuelle Benutzerdaten von der Benutzerverwaltung in ARIS Administration/User Management nach ARIS Risk and Compliance zu übertragen, synchronisieren Sie die Benutzer in ARIS Risk and Compliance mit ARIS Administration/User Management.

Die Verwaltung der Benutzer erfolgt für alle ARIS-Produkte zentral in ARIS Administration/User Management. Ihnen werden Lizenzrechte (Beispiel: **ARIS Risk and Compliance (Operate)** oder **ARIS Connect Viewer**), Funktionsrechte (Beispiel: **ARCM-Administrator** oder **ARIS Connect-Administrator**), Datenbankrechte (Beispiel: **ARIS Connect Governance-Modelle**) und Benutzergruppen (Beispiel: **IT-Abteilung**) zugeordnet. Die Benutzergruppen in ARIS Administration/User Management entsprechen nicht denen in ARIS Risk and Compliance und sind daher für Benutzer, die in ARIS Risk and Compliance arbeiten, von geringer Bedeutung. In ARIS Risk and Compliance werden Benutzer speziellen Benutzergruppen zugeordnet, die ihre GRC-Rollen repräsentieren. Detaillierte Informationen hierzu finden Sie unter Wie Sie Benutzer und deren Rechte verwalten. Detaillierte Informationen hierzu finden Sie unter Wie Sie Benutzer und deren Rechte verwalten.

Voraussetzung

Sie haben die Rolle **Benutzer-/Benutzergruppenadministrator** mit dem Rollenlevel **Umgebungsübergreifend**, Systemadministrator- oder Benutzeradministrator-Rechte in ARIS Risk and Compliance.

Vorgehen

1. Klicken Sie auf  **Administration > User Management**.

2. Klicken Sie unter **Benutzerverwaltung > Mit Benutzerverwaltung synchronisieren** auf **Synchronisieren**. Die Benutzerdaten in ARIS Risk and Compliance werden durch die Daten aus ARIS Administration/User Management aktualisiert.

Der Dialog wird geschlossen. **Administration > Monitoring > Funktional > Server-Aufträge** wird angezeigt. Der Server-Task wird unter **Server-Tasks in Bearbeitung** angezeigt. Wenn er abgeschlossen ist, wird er unter **Abgeschlossene Server-Tasks (letzte 10)** aufgelistet.

Benutzername, Name (Vor- und Nachname in ARIS Administration/User Management), Beschreibung, E-Mail-Adresse und Telefonnummer werden nach ARIS Risk and Compliance übertragen und die Benutzer werden aktiviert. Benutzer, die keine ARIS Risk and Compliance-Lizenzrechte in ARIS Administration/User Management besitzen, werden in ARIS Risk and Compliance als deaktiviert markiert.

2.3 Anbindung an einen Verzeichnisdienst (LDAP)

Anders als in den Vorgängerversionen wird LDAP nun nicht mehr direkt mit ARIS Risk and Compliance verbunden. Stattdessen muss die LDAP-Anbindung in ARIS Administration/im User Management konfiguriert werden. Detaillierte Informationen hierzu finden Sie im Handbuch **ARIS SSO, LDAP, KERBEROS, SAML, SCIM** im Kapitel **Use LDAP**.

2.4 Runnable über ARIS Cloud Controller sichern und rücksichern

ARIS Risk and Compliance ermöglicht das Generieren und Rücksichern von Datenbankschnappschüssen direkt aus der Web-Anwendung. Die ARIS Cloud Controller (ACC)-Funktionalität zum Sichern und Rücksichern von Mandanten ist zusätzlich zum Generieren von Runnable-Sicherungsdateien verwendbar, die einen Datenbankschnappschuss sowie alle angewandten individuellen Anpassungen enthalten. Nähere Informationen finden Sie im Handbuch für das **ARIS Cloud Controller (ACC)-Kommandozeilenprogramm** in den Kapiteln **Back up a tenant** und **Restore a tenant**.

2.5 Runnable über ARIS Tenant Management sichern und rücksichern

ARIS Tenant Management erlaubt die Sicherung und Rücksicherung mandantenspezifischer Daten von ARIS Risk and Compliance. Die erzeugten Runnable-Sicherungsdateien enthalten einen Datenbankschnappschuss sowie alle angewandten individuellen Anpassungen. Nähere Informationen finden Sie im **ARIS Tenant Management Handbuch**.

Hinweis: Bei der Rücksicherung mandantenspezifischer Daten über ARIS Tenant Management müssen die Sicherungsdateien dieselben individuellen Anpassungen enthalten wie die angewandten Exemplare von ARIS Risk and Compliance. Ist dies nicht der Fall, sind die individuellen Anpassungen für die entsprechenden Exemplare manuell anzuwenden.

2.6 ARCM mit anderen Mandanten als dem 'Standard'-Mandanten verwenden

Wenn ARIS Risk and Compliance für einen anderen Mandanten als den **Standard**-Mandanten konfiguriert ist, muss der Mandantenname in der URL für den Zugriff auf ARIS Risk and Compliance enthalten sein. Nach der Anmeldung wird der Mandantenname nicht mehr in der URL angezeigt.

Beispiel

URL für Zugriff auf ARIS Risk and Compliance mit Mandant **umg**:

https://<servername>:<port>/arcm/login.jsp?tenant=umg

2.7 Sprachen in ARIS Administration wählen

Wenn ARIS Risk and Compliance in derselben Infrastruktur ausgeführt wird wie ARIS, können die verfügbaren Sprachen in ARIS Administration konfiguriert werden. Standardmäßig stehen die folgenden Sprachen zur Verfügung: Deutsch, Englisch, Französisch, Chinesisch, Japanisch, Spanisch, Portugiesisch, Italienisch, Magyarisch, Arabisch. Sie können Sprachen deaktivieren, sodass sie nicht mehr in ARIS Risk and Compliance und ARIS verfügbar sind. Wenn nur Sprachen konfiguriert sind, die ARIS Risk and Compliance nicht unterstützt, wird auf Englisch zurückgegriffen.

Vorgehen

1. Starten Sie ARIS.
2. Melden Sie sich als **Systembenutzer** an.
3. Klicken Sie auf **Anwendungsstarter** > **Administration**. **ARIS Administration** wird geöffnet.
4. Klicken Sie auf **Konfigurations-Sets verwalten**. Alle verfügbaren Konfigurations- und Änderungs-Sets werden angezeigt. Das aktuelle Konfigurations- oder Änderungs-Set ist als **(aktiv)** gekennzeichnet.
5. Bearbeiten Sie ein vorhandenes Änderungs-Set oder erstellen Sie ein neues. Sie können nur benutzerdefinierte Änderungs-Sets bearbeiten. Detaillierte Informationen, wie etwa zum Erstellen eines Änderungssets, finden Sie in der Online-Hilfe von ARIS.
6. Halten Sie den Mauszeiger über das entsprechende Änderungs-Set und klicken Sie auf **Bearbeiten**. Die Seite **Änderungs-Set definieren** wird geöffnet und Sie können das Änderungs-Set bearbeiten.
7. Klicken Sie auf **Sprachen wählen**.
8. Wählen Sie in der Liste **Aktuelle Sprache** die Sprachen aus, die Sie nicht benötigen, und klicken Sie dann auf **Deaktivieren**. Die ausgewählten Sprachen werden in die Liste **Weitere Sprachen** aufgenommen.
9. Wählen Sie in der Liste **Weitere Sprachen** die Sprachen aus, die Sie benötigen, und klicken Sie dann auf **Aktivieren**. Die Sprachen werden in die Liste **Aktuelle Sprache** aufgenommen.
10. Klicken Sie auf **Anwenden**.
11. Klicken Sie auf **Zurück**.
12. Aktivieren Sie das Änderungs-Set, sofern es nicht bereits aktiviert ist, etwa im Fall, dass Sie ein neues Änderungs-Set erstellt haben.

Die in der Liste **Aktuelle Sprache** aufgeführten Sprachen können von den ARIS Risk and Compliance- und ARIS-Benutzern ausgewählt werden.

2.8 Schrift und Farben anpassen

Sie können die Einstellungen an das Corporate Design Ihres Unternehmens anpassen. Detaillierte Informationen hierzu finden Sie in der Online-Hilfe von ARIS.

2.9 Server-Task-Zeitpläne anpassen

ARIS Risk and Compliance stellt Server-Tasks bereit, die automatisch entsprechend den Zeitplänen ausgeführt werden, beispielsweise um Aufgaben zu generieren und die Fälligkeitsdaten für Tasks zu überwachen. Die Server-Tasks werden in der Systemkonfiguration von ARIS Risk and Compliance (**Administration > Systemkonfiguration > Server-Task-Zeitpläne**) festgelegt. In der Regel werden sie nachts ausgeführt. Ein automatisierter Server-Task sollte höchstens dreimal täglich ausgeführt werden. Wenn Sie eine Server-Task häufiger ausführen müssen, wenden Sie sich bitte an den Support der Software AG. Wenn Sie über die entsprechende Managerrolle verfügen, können Sie nur für Schulungen und Präsentationen in ARIS Risk and Compliance (**Administration > Server-Tasks**) einen Server-Task auch manuell anstoßen.

Server-Task-Konfigurationsparameter beginnen stets mit **arcm.config.schedule.job**, gefolgt vom Server-Task-Typ (Generator, Monitor, Updater) und dann vom Objekttyp, für den der Server-Task verantwortlich ist, z. B. **arcm.config.schedule.job.generator.testcase**. Der Cleaning-Server-Task verfügt nicht über diesen Objekttyp-Anhang: **arcm.config.schedule.job.cleaning**. Der Wert eines Server-Task-Parameters besteht aus einer Abfolge von Schlüsselwertpaaren, die durch eckige Klammern **[]** zu Gruppen zusammengefasst sind. Schlüssel und Wert sind durch einen senkrechten Strich (**|**) voneinander getrennt. Um die Einstellungen der geplanten Server-Tasks in ARIS Risk and Compliance zu ändern, gehen Sie wie folgt vor. Weitere Informationen finden Sie in der CronTrigger-Dokumentation auf der Quartz-Homepage (http://www.quartz-scheduler.org).

Beispiele

- Der Generator-Server-Task für Kontrolltests soll jeden Tag um 00:52 gestartet werden. Der Server-Task soll für alle Umgebungen ausgeführt werden, außer der Umgebung **env1**.

  Eigenschaftsschlüssel:

  ```
  arcm.config.schedule.job.generator.testcase
  ```

  Wert:

  ```
  [ jobitem | generatorJob ] [ startScheduler | true ] [ executionTime | 0 52 00 ? * SUN-SAT ] [ excludedEnvironments | env1] [ includedEnvironments | ] [ objecttypes | TESTCASE ]
  ```

- Der Überwachungs-Server-Task für Risikobewertungen soll von Montag bis Freitag um 08:00 und um 18:00 gestartet werden. Der Server-Task soll nur für die Umgebung **env1** ausgeführt werden.

  Eigenschaftsschlüssel:

  ```
  arcm.config.schedule.job.monitor.riskassessment
  ```

  Wert:

  ```
  [ jobitem | monitorJob ] [ startScheduler | true ] [ executionTime | 0 0 8,18 ? * MON-FRI  ] [ excludedEnvironments | ] [ includedEnvironments | env2] [ objecttypes | RISKASSESSMENT ]
  ```

BEDEUTUNG DER EINZELNEN PARAMETER

JOBITEM

Der Server-Task, der ausgeführt werden soll. Der Parameterwert muss einer EnumItem-ID aus der Aufzählung **jobs** in der Datei **enumerations.xml** entsprechen.

STARTSCHEDULER

Der Wert muss **true** sein, damit die Zeitsteuerung für diesen Server-Task aktiv ist.

EXECUTIONTIME

Dieser Ausdruck legt fest, wann der Server-Task gestartet werden soll. Er hat das Format **CronTrigger**, welches die Angabe von Zeitintervallen erlaubt. Von links nach rechts bedeuten die einzelnen Werte:

- **Seconds** (0-59)
- **Minutes** (0-59)
- **Hours** (0-23)
- **Day of month** (1-31 oder Fragezeichen (**?**) für einen beliebigen Kalendertag des Monats)
- **Month** (1-12, JAN-DEZ, oder Sternchen (*****) für einen beliebigen Monat)
- **Day of week** (1-7 oder SUN-SAT)
- **Year** (kann leer sein, 1984, 1970-2099, ...)

EXCLUDEDENVIRONMENTS

Hier werden die Umgebungen innerhalb der Datenbank von ARIS Risk and Compliance angegeben, für die der Server-Task nicht ausgeführt werden soll. Die Werte können durch Kommas getrennt angegeben werden. Dies gilt nur für umgebungsspezifische Server-Tasks.

INCLUDEDENVIRONMENTS

Hier werden die Umgebungen innerhalb der Datenbank von ARIS Risk and Compliance angegeben, für die der Server-Task ausgeführt werden soll. Ist kein Wert festgelegt, wird für jede einzelne Umgebung ein separater Server-Task gestartet. Die Werte können durch Kommas getrennt angegeben werden. Dies gilt nur für umgebungsspezifische Server-Tasks.

OBJECTTYPES

Die Objekttypen, für die der Server-Task ausgeführt werden soll. Im obigen Beispiel soll diese Instanz des Überwachungs-Server-Task ausschließlich die Kontrolltests überprüfen. Die Werte können durch Kommas getrennt angegeben werden.

GEPLANTE SERVER-TASKS KONFIGURIEREN

Voraussetzung

Sie verfügen über Systemadministratorrechte in ARIS Risk and Compliance.

Vorgehen

1. Klicken Sie auf **Administration**. Das Menüelement **Allgemein** wird anfänglich angezeigt.
2. Klicken Sie unter **Systemmanagement** auf **Systemkonfiguration**. Die Konfigurationsparameter werden angezeigt.
3. Um die zeitgesteuerten Server-Tasks anzuzeigen, filtern Sie die Systemkonfiguration nach **Administration > Server-Task-Zeitpläne**. Das Suchergebnis zeigt alle zeitgesteuerten Server-Tasks mit ihren aktuellen Werten an.
4. Klicken Sie in der Zeile des Parameters, den Sie ändern möchten, auf **Bearbeiten**. Der Dialog **Parameterwert setzen** wird geöffnet.
5. Kopieren Sie **Current value** in die Zwischenablage. Zum Beispiel:

   ```
   [ jobitem | generatorJob ] [ startScheduler | true ] [ executionTime | 0 52 00 ? * SUN-SAT ] [ excludedEnvironments | ] [ includedEnvironments | ] [ objecttypes | TESTCASE ]
   ```
6. Fügen Sie den Wert in einen Texteditor ein und nehmen Sie eine relevante Änderung vor, ändern Sie z. B. die Ausführungszeit. Zum Beispiel:

   ```
   [ jobitem | generatorJob ] [ startScheduler | true ] [ executionTime | 0 0 8-18 ? * MON-FRI ] [ excludedEnvironments | ] [ includedEnvironments | ] [ objecttypes | TESTCASE ]
   ```
7. Kopieren Sie den geänderten Parameter in die Zwischenablage und fügen Sie ihn in das Textfeld **New value** ein.

   Stellen Sie sicher, dass Sie immer den vollständigen String kopieren und einfügen. Sie können nicht nur einen Teil des Strings verwenden, den Sie anpassen wollen, z. B. executionTime | 0 0 8-18 ? * MON-FRI].
8. Klicken Sie auf **OK**.

Die Änderungen werden sofort übernommen und in der Datenbank gespeichert. Klicken Sie in der Zeile des entsprechenden Parameters auf **Zurücksetzen**, um ihn auf den Standardwert zurückzusetzen.

3 Glossar

Im Glossar sind grundlegende Fachbegriffe erklärt.

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 Dateinamenerweiterung 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.

SINGLE SIGN-ON (SSO)

Durch die Einmalanmeldung (Single Sign-On, SSO) braucht sich ein Benutzer nur einmal mit Benutzername und Kennwort zu authentifizieren, um ohne erneute Anmeldung auf alle Dienste, Programme und Rechner zuzugreifen. Wenn Dienste, Programme und Rechner eine erneute Authentifizierung verlangen, wird diese durch den zugrunde liegenden SSO-Mechanismus vorgenommen.

4 Rechtliche Hinweise

4.1 Dokumentationsumfang

Die zur Verfügung gestellten Informationen beschreiben die Einstellungen und Funktionalitäten, die zum Zeitpunkt der Veröffentlichung gültig waren. Da Software und Dokumentation verschiedenen Fertigungszyklen unterliegen, kann die Beschreibung von Einstellungen und Funktionalitäten von den tatsächlichen Gegebenheiten abweichen. Informationen über solche Abweichungen finden Sie in den mitgelieferten Release Notes. Bitte lesen und berücksichtigen Sie diese Datei bei Installation, Einrichtung und Verwendung des Produkts.

Wenn Sie technische und/oder geschäftliche Systemfunktionen ohne Nutzung der Service-Leistungen der Software AG installieren möchten, benötigen Sie umfangreiche Kenntnisse hinsichtlich des zu installierenden Systems, seines Zwecks sowie der Zielsysteme und ihrer Abhängigkeiten untereinander. Aufgrund der Anzahl an Plattformen und voneinander abhängigen Hardware- und Software-Konfigurationen können wir nur spezifische Installationen beschreiben. Es ist nicht möglich, sämtliche Einstellungen und Abhängigkeiten zu dokumentieren.

Beachten Sie bitte gerade bei der Kombination verschiedener Technologien die Hinweise der jeweiligen Hersteller, insbesondere auch aktuelle Verlautbarungen auf deren Internet-Seiten bezüglich Freigaben. Für die Installation und einwandfreie Funktion freigegebener Fremdsysteme können wir keine Gewähr übernehmen und leisten daher keinen Support. Richten Sie sich grundsätzlich nach den Angaben der Installationsanleitungen und Handbücher der jeweiligen Hersteller. Bei Problemen wenden Sie sich bitte an die jeweilige Herstellerfirma.

Falls Sie bei der Installation von Fremdsystemen Hilfe benötigen, wenden Sie sich an Ihre lokale Software AG-Vertriebsorganisation. Beachten Sie bitte, dass solche Hersteller- oder kundenspezifischen Anpassungen nicht dem Standard-Softwarepflege- und Wartungsvertrag der Software AG unterliegen und nur nach gesonderter Anfrage und Abstimmung erfolgen.

Bezieht sich eine Beschreibung auf ein spezifisches ARIS-Produkt, wird dieses genannt. Andernfalls werden die Bezeichnungen für die ARIS-Produkte folgendermaßen verwendet:

Name	Umfasst
ARIS-Produkte	Bezeichnet sämtliche Produkte, für die die Lizenzbedingungen der Software AG-Standard-Software gelten.
ARIS-Clients	Bezeichnet alle Programme, die über ARIS Server auf gemeinsam verwendete Datenbanken zugreifen, z. B. ARIS Architect oder ARIS Designer.
ARIS-Download-Clients	Bezeichnet ARIS-Clients, die aus dem Browser gestartet werden können.

5 Index