software AG

ARIS

BASIC TROUBLESHOOTING GUIDE

Version 10.0 - Service Release 5

July 2018

Contents

1 General notices

This manual describes the settings and features as they were at the time of print.

- You can install ARIS Connect/ARIS Design Server and ARIS Risk & Compliance Manager on one machine. ARIS Publisher Server must be installed on a dedicated machine, if required. For advanced installations Software AG strongly recommends that you request an installation service by Global Consulting Services. You can order that service from your Software AG sales representative (page 20). This is of particular importance when you intend to install ARIS across several computers/VMs (distributed installation). Such a specific scenario requires profound knowledge of the technical ARIS infrastructure and environment. This cannot be provided in the product documentation. The required know-how can be acquired only by attending the training course **ARIS Server Installation**, available via Global Education Services (http://softwareag.com/training).

- In general, it is advisable to use up-to-date hardware taking into account the number of users who will be accessing the ARIS.

- When you combine various technologies, please observe the manufacturers' instructions, particularly announcements concerning releases on their Internet pages. We cannot guarantee proper functioning and installation of approved third-party systems and do not support them. Always follow the instructions provided in the installation manuals of the relevant manufacturers. If you experience difficulties, please contact the relevant manufacturer.

- If you need help installing third-party systems, please contact your local Software AG sales organization (page 20). Please note that this type of manufacturer-specific or customer-specific change is not subject to the standard Software AG software maintenance agreement and that these changes can only be performed if you requested and agreed on them.

- Please consider the legal notices (http://softwareag.com/licenses).

2 Text conventions

Menu items, file names, etc. are indicated in texts as follows:

- Menu items, key combinations, dialogs, file names, entries, etc. are displayed in **bold**.

- User-defined entries are shown **\<in bold and in angle brackets\>**.

- Single-line example texts (for example, a long directory path that covers several lines due to a lack of space) are separated by ↵ at the end of the line.

- File extracts are shown in this font format:

  `This paragraph contains a file extract.`

- Warnings have a colored background:

  Warning

  This paragraph contains a warning.

3 Basic troubleshooting

This document is intended to solve problems with ARIS Server installations that were carried out with the setup program. If you face problems starting ARIS, please refer to the Monitoring health chapter and read the following pages.

3.1 ARIS Download Client cannot be started

PROBLEMS

Starting ARIS Download Client does not work.

Either there is no Java Runtime Environment (JRE) installed on the user's computer, or the file extension **.JAR** is NOT assigned to the JRE.

SOLUTIONS

1. If no JRE is installed on the user's computer, download and install it from http://java.com (http://java.com).

2. Start the Windows Explorer and navigate to the **%UserProfile%\downloads** download folder, or to that folder where the ARIS downloader **JAR** file has been saved by the browser.

3. Right click the ARIS downloader **JAR** file.

4. Select **Open with**.

5. Assign it with a locally installed Java ™ Platform SE binary Oracle Corporation **JAR** file.

    If a file extension assignment for **.JAR** files is not feasible, the ARIS downloader can be started using the JRE on a command line.

3.2 HTTPS connection fails (SSL) - wrong keystore password

PROBLEM

If the keystore password is wrong, an error message will be logged for the runnable:

```
SEVERE: Failed to initialize end point associated with ProtocolHandler
["http-bio-23456"]
java.io.IOException: Keystore was tampered with, or password was incorrect
        at sun.security.provider.JavaKeyStore.engineLoad(JavaKeyStore.java:772)
        at sun.security.provider.JavaKeyStore$JKS.engineLoad(JavaKeyStore.java:55)
        at java.security.KeyStore.load(KeyStore.java:1445)
        at
org.apache.tomcat.util.net.jsse.JSSESocketFactory.getStore(JSSESocketFactory.jav
a:429)
        at
org.apache.tomcat.util.net.jsse.JSSESocketFactory.getKeystore(JSSESocketFactory.
java:328)
        at
org.apache.tomcat.util.net.jsse.JSSESocketFactory.getKeyManagers(JSSESocketFacto
ry.java:586)
        at
org.apache.tomcat.util.net.jsse.JSSESocketFactory.getKeyManagers(JSSESocketFacto
ry.java:526)
        at
org.apache.tomcat.util.net.jsse.JSSESocketFactory.init(JSSESocketFactory.java:47
1)
        at
org.apache.tomcat.util.net.jsse.JSSESocketFactory.createSocket(JSSESocketFactory
.java:218)
        at org.apache.tomcat.util.net.JIoEndpoint.bind(JIoEndpoint.java:400)
        at
org.apache.tomcat.util.net.AbstractEndpoint.init(AbstractEndpoint.java:649)
        at org.apache.coyote.AbstractProtocol.init(AbstractProtocol.java:434)
        at
org.apache.coyote.http11.AbstractHttp11JsseProtocol.init(AbstractHttp11JsseProto
col.java:119)
        at
org.apache.catalina.connector.Connector.initInternal(Connector.java:978)
        at org.apache.catalina.util.LifecycleBase.init(LifecycleBase.java:102)
        at
org.apache.catalina.core.StandardService.initInternal(StandardService.java:559)
        at org.apache.catalina.util.LifecycleBase.init(LifecycleBase.java:102)
        at
org.apache.catalina.core.StandardServer.initInternal(StandardServer.java:821)
        at org.apache.catalina.util.LifecycleBase.init(LifecycleBase.java:102)
        at org.apache.catalina.startup.Catalina.load(Catalina.java:638)
        at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
        at
sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62)
        at
sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.jav
a:43)
        at java.lang.reflect.Method.invoke(Method.java:497)
        at org.apache.catalina.startup.Bootstrap.load(Bootstrap.java:280)
        at org.apache.catalina.startup.Bootstrap.main(Bootstrap.java:454)
Caused by: java.security.UnrecoverableKeyException: Password verification failed
        at sun.security.provider.JavaKeyStore.engineLoad(JavaKeyStore.java:770)
        ... 25 more
```

SOLUTION

Provide the proper keystore password using the **connector.https.keystorePass** configure parameter:

By default, Apache Tomcat™ uses **changeit** as both the keystore and the key password. If you follow the general recommendation, your keystore should have different passwords. If you only set the key password, Apache Tomcat™ will also use it as keystore password. Only if key and keystore passwords differ, you must set both parameters.

Follow this procedure to change the key and keystore passwords.

Procedure

1. Start ARIS Cloud Controller on your ARIS Publisher Server.

2. Enter: **stop businesspublisher_<s,m or l>**

   The runnable will be stopped.

3. Enter: **reconfigure businesspublisher_<s,m or l> connector.https.keyPass=<key password> connector.https.keystorePass=<keystore password>**

   for example **reconfigure businesspublisher_m connector.https.keyPass="g3h31m" connector.https.keystorePass="g3h31m3r"**

   In this example quotes are not strictly necessary. Quotes are necessary for strong passwords containing special characters.

4. Enter: **start businesspublisher_<s,m or l>**

The key and keystore passwords are set.

3.3   HTTPS connection fails (SSL) - wrong key password

PROBLEM

If the key password is wrong, an error message will be logged for the runnable:

```
SEVERE: Failed to initialize end point associated with ProtocolHandler
["http-bio-23456"]
java.io.IOException: Cannot recover key
     at
org.apache.tomcat.util.net.jsse.JSSESocketFactory.init(JSSESocketFactory.java:49
6)
     at
org.apache.tomcat.util.net.jsse.JSSESocketFactory.createSocket(JSSESocketFactory
.java:218)
     at org.apache.tomcat.util.net.JIoEndpoint.bind(JIoEndpoint.java:400)
     at
org.apache.tomcat.util.net.AbstractEndpoint.init(AbstractEndpoint.java:649)
     at org.apache.coyote.AbstractProtocol.init(AbstractProtocol.java:434)
     at
org.apache.coyote.http11.AbstractHttp11JsseProtocol.init(AbstractHttp11JsseProto
col.java:119)
     at
org.apache.catalina.connector.Connector.initInternal(Connector.java:978)
     at org.apache.catalina.util.LifecycleBase.init(LifecycleBase.java:102)
     at
org.apache.catalina.core.StandardService.initInternal(StandardService.java:559)
     at org.apache.catalina.util.LifecycleBase.init(LifecycleBase.java:102)
     at
org.apache.catalina.core.StandardServer.initInternal(StandardServer.java:821)
     at org.apache.catalina.util.LifecycleBase.init(LifecycleBase.java:102)
     at org.apache.catalina.startup.Catalina.load(Catalina.java:638)
     at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
     at
sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62)
     at
sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.jav
a:43)
     at java.lang.reflect.Method.invoke(Method.java:497)
     at org.apache.catalina.startup.Bootstrap.load(Bootstrap.java:280)
     at org.apache.catalina.startup.Bootstrap.main(Bootstrap.java:454)
Caused by: java.security.UnrecoverableKeyException: Cannot recover key
     at sun.security.provider.KeyProtector.recover(KeyProtector.java:328)
     at sun.security.provider.JavaKeyStore.engineGetKey(JavaKeyStore.java:138)
     at
sun.security.provider.JavaKeyStore$JKS.engineGetKey(JavaKeyStore.java:55)
     at java.security.KeyStore.getKey(KeyStore.java:1023)
     at
sun.security.ssl.SunX509KeyManagerImpl.<init>(SunX509KeyManagerImpl.java:133)
     at
sun.security.ssl.KeyManagerFactoryImpl$SunX509.engineInit(KeyManagerFactoryImpl.
java:70)
     at javax.net.ssl.KeyManagerFactory.init(KeyManagerFactory.java:256)
     at
org.apache.tomcat.util.net.jsse.JSSESocketFactory.getKeyManagers(JSSESocketFacto
ry.java:597)
     at
org.apache.tomcat.util.net.jsse.JSSESocketFactory.getKeyManagers(JSSESocketFacto
ry.java:526)
```

```
      at
org.apache.tomcat.util.net.jsse.JSSESocketFactory.init(JSSESocketFactory.java:47
1)
      ... 18 more
```

SOLUTION

Provide the proper keystore password using the **connector.https.keyPass** configure parameter:

By default, the **loadbalancer** runnable is set to allow both unencrypted HTTP (port 80) and encrypted HTTPS/SSL (port 443) access. In order to use SSL the SSL certificate must fit to the load balancer's host name. Otherwise client connections in particular web browser connections will fail due to an invalid certificate.

Using SSL with ARIS Publisher must be configured in a different way.

OBTAINING A VALID CERTIFICATE

If you want to use SSL, you need a valid certificate for the server on which the load balancer is running. This certificate must be signed by a certificate authority (CA). Please make sure that the certificate is compatible with the Java version of all ARIS clients.

- You can buy a certificate from an official CA. Most clients in particular browsers will trust certificates signed by such a CA.
- If your company uses own CA, use a certificate from this CA and add this CA to the trust store of all clients.

ADDING A VALID CERTIFICATE TO THE LOAD BALANCER

Your certificate must contain two parts:

- The private key used to encrypt information sent back to the client (file extension **.key**).
- The server certificate (file extension **.crt**).

1. Put these two files into a ZIP file.
2. Copy this ZIP file to a local directory that can be accessed by ARIS Cloud Controller (ACC).
3. Start the ACC.
4. Stop the **loadbalancer** runnable. Enter, for example:

   stop loadbalancer_m

5. Enter the ACC command **enhance loadbalancer_<s, m, or l> with sslCertificate local file "<path to the ZIP file>"**

   Example:

   enhance loadbalancer_m with sslCertificate local file "c:\\temp\\lbcert.zip".

   If you have blanks or special characters in the path, you must put it in quotes and use a double backslash instead of a single slash. Alternatively, use single forward slashes, for example: **"c:/temp/lbcert.zip"**.

6. Start the **loadbalancer** runnable again. Enter, for example:

   start loadbalancer_m

The SSL certificate is available.

If ARIS clients cannot perform connections to servers using SSL certification, you need to provide an additional certificate (page 11) (see: **Basic Troubleshooting Guide**).

3.4   HTTPS connection fails (SSL) - wrong certificate in use (Alfabet)

PROBLEM

The ARIS Server cannot communicate with an external system such as Alfabet.

SOLUTION

Import the certificate used by Alfabet to the Java VM used by the ARIS Server:

Procedure

1. Open a Windows command prompt for **<ARIS installation path>server\jre\bin**.

2. Run the command:

    keytool.exe -importcert -file <pathToCertFile> -alias <certificateAlias> -keystore <ARIS installation path>server\jre\lib\security\cacerts -storepass <keystorePassword>

    The default password for the **cacerts** keystore is **changeit**.

3. To check if the import actually worked open a Windows command prompt for **<ARIS installation path>server\jre\lib\security** and enter:

    keytool -list -keystore cacerts -alias <certificateAlias>

4. Restart the **abs** runnable.

The ARIS Server uses the same certificate as the external system.

3.5   HTTPS connection fails (SSL) - wrong certificate in use (ARIS Publisher Server)

PROBLEM

If you access Publisher exports via HTTPS connections, Process Governance cannot be reached.

SOLUTION

Adapt the system manually:

Procedure

1.   Open the **webappserver.cfg** navigate to the <governance> section

2.   Change the <port value="**80**"/> to <port value="**443**"/>.

3.   Change the <protocol value="**http**"/> to <protocol value="**https**"/>

4.   Import the certificates from the ARIS Server into the JRE certificate store of the ARIS Publisher Server:
Open a Windows command prompt for **<ARIS installation path>server\jre\bin**.

5.   Run the command:

keytool.exe -importcert -file <pathToCertFile> -alias <certificateAlias> -keystore <ARIS installation path>server\jre\lib\security\cacerts -storepass <keystorePassword>

SSL is configured.

3.6 ARIS clients cannot connect to servers using SSL

PROBLEM

A SSL certificate is available but ARIS clients cannot be started using SSL certification.

This may happen due to ARIS clients using Java trust store having trouble verifying the certificate chain.

SOLUTION

An additional certificate must be made available for the load balancer.

1. Download the zip file of the certificate from a certificate authority (CA), for example, GlobalSign.

2. Start ARIS Cloud Controller (ACC).

3. Stop the **loadbalancer** runnable.

4. Enhance the certificate using this command:

5. **enhance <runnable of the load balancer component> with sslCertificate local file "<path to the downloaded zip file>"**, for example:

   enhance loadbalancer_m with sslCertificate local file "c:\\temp\\lbcert.zip".

   Notice the double backslashes. Alternatively, use single forward slashes, for example, **"c:/temp/lbcert.zip"**.

6. Start the **loadbalancer** runnable again.

The SSL certificate is available.

3.7   ARIS clients using SSL throw Java exceptions

PROBLEM

The **loadbalancer** runnables are configured for the use of SSL and a SSL certificate is available. Nevertheless, ARIS Client or ARIS Download Client throws the following Java exceptions:

```
SEVERE: cannot login
com.aris.modeling.common.serverremoteapi.cscommon.umc.UMCLoginException: cannot
connect to server myARIS.customer.com. Reason:
sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid
certification path to requested target
at
com.aris.modeling.common.serverremoteapi.cscommon.umc.UMCLogin.authenticateOnSer
ver(UMCLogin.java:218)
at
com.aris.modeling.common.serverremoteapi.cscommon.umc.UMCLogin.authenticate(UMCL
ogin.java:113)
at
com.aris.modeling.client.container.serveraccess.AServerContext.getUserToken(ASer
verContext.java:842)
at
com.aris.modeling.client.container.serveraccess.AServerContext.connectBLManager(
AServerContext.java:773)
cannot be started using SSL certification.
```

REASON

Even with valid certificates (that contain the correct ARIS Server and domain name) purchased from a reliable CA, it may occur that the corresponding root certificate is not available in the JRE currently being used. As a consequence, the JRE is unable to validate the certificate and thus considers it as unknown in the same way it does with certificates that were created internally.

SOLUTION

Add the certificate to the certificate store of the JRE in use. This depends on whether users use a locally installed ARIS Client or ARIS Download Client.

INSTALLED ARIS CLIENT

If an ARIS Clientis installed locally, the certificate must be placed into the JRE of the installed ARIS Client. The installed ARIS Client uses its own JRE (see <ARIS installation path>client\jre\). You must distribute the certificate to every single machine from which ARIS Client will be started.

ARIS DOWNLOAD CLIENT

If ARIS Download Client is started using an **ARIS downloader JAR** file but not the Java applet, you can easily roll out an enhanced **cacerts** file. Just place it into the JRE installation path on the machine were the ARIS Server is installed.

1. To roll out the certificate for ARIS Download Client, open your file browser and navigate to the JRE installation path, for example, c:\Program Files (x86)\java\jre**bin**. This directory contains the **keytool.exe** file.

2. To update the required **certs** file located in the <JRE installation path>\lib**security** directory, open a Windows command prompt in this directory and run the command:

    keytool.exe -importcert -file <pathToCertFile> -alias <certificateAlias> -keystore <ARIS installation path>client\jre\lib\security\cacerts -storepass <keystorePassword>

    Replace all <placeholders> with the proper value. Aside from those mentioned above:

    ▪   **<certificateAlias>**
        This placeholder represents a name you give to your certificate. Name it in a way that you can easily identify your certificate from the selection in the cacerts keystore.

    ▪   **<keystorePassword>**
        This placeholder represents the password to the cacerts keystore. Do not use a different password as the default value **changeit**.

3. Copy the **cacerts** file, that was changed (<JRE installation path>\lib**security**), into the on this location:

    "**<ARIS installation path>\server\bin\work\work_abs_<s|m|l>\base\webapps\abs\downloadClient\config**

    If users start ARIS Download Client using an **ARIS downloader JAR** file, this **cacerts** file is downloaded and used.

Users must restart theirARIS_download_client>. Sometimes users are required to restart their browsers. This forces Java to re-read the cacerts keystore.

If an error message is thrown like the following, the certificate is signed for the wrong ARIS Server name. In this case, you must provide the correct certificate.

```
Jul 01, 2018 7:15:08 AM com.idsscheer.utils.logging.ALogger logException
SEVERE: cannot login
com.aris.modeling.common.serverremoteapi.cscommon.umc.UMCLoginException:
 cannot connect to server myARIS.customer.com. Reason: Certificate
for <myARIS.customer.com> doesn't contain CN or DNS
subjectAlt
at
com.aris.modeling.common.serverremoteapi.cscommon.umc.UMCLogin.authenticateOnSer
ver(UMCLogin.java:218)
at
com.aris.modeling.common.serverremoteapi.cscommon.umc.UMCLogin.authenticate(UMCL
ogin.java:113)
at
com.aris.modeling.client.container.serveraccess.AServerContext.getUserToken(ASer
verContext.java:842)

...
```

3.8 Using SSL or using other port than port 80

PROBLEM

The local script service **Determine link (design)** is currently not able to handle a changed port (default port is port **80**) or work properly in a system using Process Governance which is set up with SSL.

SOLUTION

Change the port and SSL-mode manually in the local script. To do so proceed as follows.

Procedure

1. Start ARIS Architect

2. Log into a database.

3. Navigate to **Governance Resources > Determine link (design)**.

4. Double-click the service **Determine link (design)**. The service opens on a separate tab. You can edit the code.

5. In the **//link="http://** section of the code, add your port and your SSL-mode.

6. Save the changes.

The problem should no longer occur.

3.9 Server started but no access to ARIS

PROBLEM

After you have started the server you still cannot access ARIS.

SOLUTION

Open the ARIS Cloud Controller (ACC) using the link in the start menu. Once the prompt appears, type **list**. Check if all runnables are in state **STARTED**.

If the output of the list command shows one or more runnables in state **STARTING** please wait a while and type **list** again.

Please ensure that the DNS name resolution works correctly.

3.10 Runnables do not start

PROBLEM

- Runnables are still in **STARTING** state.
- Runnables are in the **DEACTIVATED** state.

SOLUTION

Kill the runnable using the **kill** command. For example **kill abs_m**. Try starting it again with the **start** command, for example, **start abs_m**.

If the output of the **list** command shows one or more runnables in state **FAILED** or **STOPPED**. Type **startall**. Once the command finishes give the runnables some time to complete startup and type **list** to see their current state.

If a runnable is **DEACTIVATED**, activate the runnable again.

3.11 Resolving port conflicts

PROBLEM

You have killed and restarted (page 15) a FAILED/STARTING runnable several times but it still doesn't start up properly.

SOLUTION

Port collisions are a common reason for runnables not starting up at all or not working properly. Beware of port conflicts, for example, web servers or programs like **World Wide Web Publishing Service** or **Routing and Remote Access** might use the ports **80** and **443** by default.

1. Check the log files for messages indicating port conflicts.

2. Find out the ports used by an ARIS runnable using the ACC command **show instance <instanceId>**:

    Example:

    ```
    ACC+ localhost>show instance abs_m
    ID: abs_m state:STARTED
    type:com.aris.modeling.runnables.y-server-run-prod-9.0.
    0-RC108-Trunk-SNAPSHOT)
    Configuration parameters:
            JAVA_OPTS=-server
    -Xrunjdwp:transport=dt_socket,address=9704,server=y,suspend=n
            JAVA-Dcom.sun.management.jmxremote.port=9604
            JAVA-Dcom.sun.management.jmxremote.ssl=false
            CATALINA_PORT=10080
            JAVA-Dcom.sun.management.jmxremote.authenticate=false
            JAVA-XX\:MaxPermSize=256m
            JAVA-Dcom.sun.management.jmxremote=/enabled
            JAVA-Xmx=8g
            zookeeper.connect.retry.time.ms=30000
            zookeeper.bundle.type=abs
            zookeeper.session.timeout.ms=60000
            CATALINA_AJP_PORT=11080

    START command was issued at Jun 5, 2013 8:47:11 AM
    Average startup time: 192915msec
    Autostart: OFF
    Desired state: STARTED
    ACC+ localhost>
    ```

3. Use the Windows **netstat** command to find ports used by other programs:

    netstat –ao |more

4. Look for lines containing the port number(s) of the runnable that is not starting up properly and which have the state **listening**.

Sometimes, two programs might startup and use the same port. Only the first program will be reachable via this port.

```
Proto   Local Address    Foreign Address   State        PID
TCP     0.0.0.0:9701     MCY137201:0       LISTENING    5524
TCP     0.0.0.0:9702     MCY137201:0       LISTENING    4652
TCP     0.0.0.0:9703     MCY137201:0       LISTENING    5968
TCP     0.0.0.0:9704     MCY137201:0       LISTENING    3632
TCP     0.0.0.0:9705     MCY137201:0       LISTENING    9740
TCP     0.0.0.0:9706     MCY137201:0       LISTENING    6464
TCP     0.0.0.0:9707     MCY137201:0       LISTENING    6836
TCP     0.0.0.0:9708     MCY137201:0       LISTENING    6400
TCP     0.0.0.0:9709     MCY137201:0       LISTENING    7156
TCP     0.0.0.0:10080    MCY137201:0       LISTENING    2992
TCP     0.0.0.0:10080    MCY137201:0       LISTENING    6836
TCP     0.0.0.0:10081    MCY137201:0       LISTENING    3632
TCP     0.0.0.0:10082    MCY137201:0       LISTENING    7922
TCP     0.0.0.0:10083    MCY137201:0       LISTENING    4094
...
```

5. Use Windows Task Manager to identify the program using its PID that is using that port.

After you have stopped the program causing the conflict or redirected ports (see **ARIS Cloud Controller (ACC) Command-Line Tool**), all ARIS runnables will start up properly.

3.12 Log files are not available

PROBLEM

After transferring projects/branches or performing SAP synchronization all actions are logged. The files can be opened alter each action and will be saved automatically. If log files are not saved in project or solution configurations in ARIS Architect, make sure that, in ARIS document storage configuration, the **txt** file extension is configured as valid extension.

SOLUTION

You have the **Technical configuration administrator** function privilege.

Procedure

1. Start ARIS Connect.

2. Click the ▦ **Configuration** tab.

3. Select **Quota and restrictions** > General.

4. Click ✎ **Edit**.

5. Make sure that **txt** is listed in the **Valid file extensions** field, and that the **txt** file type extension is **not** restricted.

6. Click 💾 **Save**.

Log files with the **txt** extensions can be transferred. Log files will be available.

4   Known restrictions

In general, it is advisable to use up-to-date hardware taking into account the number of users who will be accessing the ARIS. For information about hardware and software requirements, please refer to the **ARIS System Requirements** document on the installation media. You can also download it from Empower (https://empower.softwareag.com/) (login required) or from the ARIS Download Center (aris.softwareag.com).

Please consider the legal notices (http://softwareag.com/licenses).

Despite the approval of our software for operation with the listed operating system versions and other software and hardware requirements, we cannot exclude the possibility of problems arising from unpredictable incompatibility issues with certain hardware/software combinations.

4.1   Update Setup

- Use the **reconfigure** ACC command (see ARIS Cloud Controller (ACC) Command-Line Tool.pdf (../../documents/3 Installation/31 Initial installation/312 Server/3121 Basic (Single node)/ARIS Cloud Controller (ACC) Command-Line Tool.pdf) document) to change settings.

  If you have customized your ARIS Publisher Server manually by modifying **XML** and **CFG** files these modifications will be lost.

  Save modified configuration files locally and document your modifications. After an update installation you can easily compare your saved file and copy the modified line into the updated configuration file.

- Deconfigure all manually added runnables.

  If runnables were added manually, you will not be able to update this installation with an update setup. As the setup will recognize that the installation has been tampered with.

  You can either update the installation manually (see **ARIS Update Cookbook**) or you can remove the added runnables with the ACC **deconfigure** command (see ACC help), then run the update setup and add and configure the runnables again.

- Make sure that no file in the installation directory is locked. Therefore, close all Command Prompts pointing into the ARIS installation folder.

- Make sure to exit ACC before running the update setup.

- If the ARIS help link does not work anymore (404 error) after the update of a custom configuration, the help URL is broken. You can easily fix it by modifying the **useraction_default.xml** file (<ARIS installation directory>\server\bin\work\work_copernicus_<s, m or l>\base\webapps\ROOT\WEB-INF\config\<customization>\instances\UserAction\).

  In the broken URL the **/connect/** entry is missing, for example:

  `/static/help/{locale}/handling/ca/index.htm#52910.htm`

  Add **/connect/**. The URL must look like in this example:

  `/static/help/{locale}/handling/`**`connect/`**`ca/index.htm#52910.htm.`

4.2 Process Governance

You can use Process Governance with up to 1000 process instances running in parallel. But the number may differ depending on the complexity of the running process (for example, self-created reports).

4.3 Right-to-left (RTL)

Languages written in right-to-left (RTL) or top-to-bottom scripts are not fully supported yet. Arabic or Hebrew can be used with ARIS, but not all functionas support RTL.

Localized RTL content and text used for user interface elements are displayed correctly. Furthermore, ARIS Connect also supports mirroring of the user interface. Mirroring is automatically activated when an RTL language is selected. Models are not affected.

Mirroring is not yet available for the following products, functions and ARIS Connect plugins:

- ARIS Architect/ARIS Designer
- ARIS Aware
- ARIS Risk & Compliance Manager
- ARIS Process-Driven Management for SAP® Solutions
- ARIS UML Designer
- Administrative components as Tenant Management and Process Governance administration

4.4 Tenant names

For tenant names please only use up to 25 lowercase ASCII characters and numbers. The name must begin with a character. Special characters and characters, for example, in Chinese, Cyrillic or Arabic cannot be used.

# 5	Contacting support

ON THE WEB

A valid support contract allows you to access the solution database on Empower (https://empower.softwareag.com/).

If you have any questions on specific installations that you cannot perform yourself, contact your local Software AG sales organization (https://empower.softwareag.com/public_directory.asp).

BY PHONE

If you have a valid support contract, you can contact Global Support ARIS at:

+800 ARISHELP

The plus sign stands for the prefix required in a given country to dial an international connection.

Example for dialing within Germany with a direct extension line: 00 800 2747 4357

If this number is not supported by your telephone provider, please refer to Empower (https://empower.softwareag.com/).

6 Glossary

Here you can find the definitions of the technical terms used in the technical ARIS manuals.

A

Administration (Documentation structure)

This area contains manuals that describe, how to adapt an installed system regarding the available system environment, for example, increasing the size of the main memory or how to change a port number.

ARIS Agent

Required service on every machine (node) on which an ARIS server component (runnable) runs. It allows the remote installation, configuration, operation of ARIS runnables.

ARIS Cloud Controller (ACC)

ACC is a command-line tool for administrating and configuring an ARIS installation. It communicates with ARIS Agents on all nodes.

'arisservice' user

The user **arisservice** is created automatically. By default, this user is assigned the **Database administrator** and **Process Governance administrator** function privileges. This user only uses up a license if a license privilege is activated for this user. The default password is **arisservice**. You should change the default password to prevent unauthorized access. You can change all user data except for the user name.

C

Collaboration database

The **postgresECP_<s,m or l>** runnable handles the internal database storing Collaboration content available in ARIS Connect.

Customizing (Documentation structure)

This area contains manuals that describe, how to adapt an installed system to meet company-specific needs that changes a standard system to an individual system. The result of these changes is that the standard update process no longer works. An update to the next minor version has to be done manually, because executing setup programs would overwrite the individual adjustments: they would have been lost.

D

Distributed installation

Byword for multi node installation. Using installation programs and performing manual tasks to establish an executable system on several servers.

Multi node installation, that is, an installation spanning across several computers/VMs. Such a specific scenario requires profound knowledge of the technical ARIS infrastructure and environment. This cannot be provided in the product documentation. The required know-how can be acquired only by attending the training course **ARIS Server Installation**, available via Global Education Services (http://softwareag.com/training). For this type of installation Software AG strongly recommends that you request an installation service by Global Consulting Services. You can order that service from your Software AG sales representative.

Download client

Client that is started via browser link.

If ARIS Server is installed, all authorized users can start ARIS Download Client within their browsers. All necessary files are downloaded from the ARIS Server to a local directory. Users do not need a local ARIS Client installation.

Depending on the browser used, the ARIS Download Client is started or a program icon is saved on your computer that you can use to start the ARIS Client.

G

'guest' user

The user **guest** is created automatically. By default, no function or license privileges are assigned to this user. This user serves technical purposes only. It is not for use by end users. Logging in to ARIS Connect or other Software AG products with this user is not allowed. Further information is available in the Software AG license terms (http://softwareag.com/licenses).

GUID

Globally **U**nique **Id**entifier (GUID).

The GUID is a character set that uniquely identifies elements worldwide.

I

Installation

Using installation programs and performing manual tasks to establish an executable system on one (single node) or several (multi node) servers.

J

JAAS

Java **A**uthentication and **A**uthorization **S**ervice (**JAAS**).

This is a Java interface, which provides services for the authentication and for the access in Java programs. JAAS supports a user based authentication.

L

Load balancer

In ARIS the **loadbalancer** runnable distributes the workload across the installed components.

In computing, load balancing distributes workloads across multiple computing resources, such as computers, a computer cluster, network links, central processing units or disk drives. Load balancing aims to optimize resource use, maximize throughput, minimize response time, and avoid overload of any single resource. Using multiple components with load balancing instead of a single component may increase reliability and availability through redundancy. Load balancing usually involves dedicated software or hardware, such as a multilayer switch or a Domain Name System server process.

M

Migration

Installing a new major version and including the previous content.

Example: Upgrade from version **9.8 Service Release 7** to version **10.0**.

Modeling database

The **postgres_<s,m or l>** runnable manages the internal standard database system storing all ARIS databases (modeling data) and the system databases (ARIS method, filters, templates, languages, fonts, font formats and script data).

This database can be replaced by an external Oracle® or Microsoft® SQL database.

Multi node installation

Using installation programs and performing manual tasks to establish an executable system on several servers.

Distributed ARIS installation extending across several computers, delivered by manual provisioning.

Such a specific scenario requires profound knowledge of the technical ARIS infrastructure and environment. This cannot be provided in the product documentation. The required know-how can be acquired only by attending the training course **ARIS Server Installation**, available via Global Education Services (http://softwareag.com/training).

N

Node

Virtual or physical machine on which ARIS Agent is installed to host ARIS runnables.

O

OTP

One-**T**ime **P**ad (**OTP**).

This one-time pad is a symmetric encryption method for transferring secret messages. This encryption method is characterized by the fact that it uses a key of the same length as the message itself.

The OTP is information-theoretically secure and has proven to be impossible to crack – provided that it is used properly.

P

Provisioning

Setting up an installed system via ARIS Cloud Controller (ACC) commands.

R

Runnable

ARIS server component providing functionality to the ARIS clients. Runnables are physically installed on a node.

Depending on the ARIS server type different runnables are used in order to provide full functionality. Runnables can be managed using ARIS Cloud Controller (ACC). The InstanceID of the ARIS Server program component is used as the name for the runnable.

S

SAML

Security **A**ssertion **M**arkup **L**anguage (**SAML**).

Standard for exchanging authentication data between security domains. SAML is an XML-based protocol that uses security tokens containing assertions to pass information about a user between an identity provider and a service provider and enables web-based authentication scenarios including single sign-on across all ARIS runnables.

Service registry

The **zoo_<s,m or l>** runnable is a server component managing the communication, configuration and status information of all available runnables and external services.

Single node installation

An ARIS server installation delivered by an ARIS server setup.

<s, m or l>

Free variable parameter used in ACC expressions.

Indicator for the three memory sizings **small (s)**, **medium (m)** and **large (l)**. This indicator is part of standard runnable names (runnables). It indicates the maximum size of the Java heap. The **S** sizing which at the time of this writing has a maximum heap size of 1152MB should be used for demonstration reasons (laptop) only. The **M** sizing sets the maximum heap size to 8GB, the **L** sizing to 16GB. You can always change this memory setting later with a **reconfigure** command.

SSL

Secure **S**ocket **L**ayer (**SSL**).

Security software to encrypt data that are exchanged between programs.

SSO

Single **S**ign-**o**n.

Using SSO has the advantage that a user only has to log in once to the network. The user need only one login name and password to access all computers, services and programs whose usage is allowed.

'superuser' user

The user **superuser** is created automatically. By default, this user is assigned the **User management**, **License management**, and **Configuration administrator** function privileges. This user can also enable this function privilege for other users. Users of the **superuser** type do not use up a license. They manage the system administration, but cannot use ARIS products due to license restrictions. The default password is **superuser**. You should change the default password to prevent unauthorized access. The password of the superuser is very important, as it is the only user who cannot be deleted. You can change all user data except for the user name.

System database

This database manages the content of the **configuration** and **evaluations** nodes displayed on ARIS Architect's **ARIS Administration** tab, for example, filters, templates and font formats as well as ARIS method content and scripts.

The database is created during the first ARIS Client login of a user. This content is available in all ARIS databases within this tenant. The system database can be backed up and restored.

System language and locale IDs

The locale ID (LCID (http://msdn.microsoft.com/en-us/goglobal/bb964662.aspx)) designates a language within a language group.

Language groups and code page are also represented by a number, for example, code page=1252. The language group is preceded by a minus sign (-), for example, -1252.

Examples are listed in the table below. For more information please refer to:

http://msdn.microsoft.com/en-us/library/0h88fahh(VS.85).aspx (http://msdn.microsoft.com/en-us/library/0h88fahh(VS.85).aspx).

System language	LCID
Afrikaans - South Africa	1078
Albanian - Albania	1052
Arabic - Algeria	5121
Arabic - Bahrain	15361
Arabic - Egypt	3073
Arabic - Iraq	2049
Arabic - Jordan	11265
Arabic - Kuwait	13313
Arabic - Lebanon	12289
Arabic - Libya	4097
Arabic - Morocco	6145
Arabic - Oman	8193
Arabic - Qatar	16385
Arabic - Saudi Arabia	1025
Arabic - Syria	10241
Arabic - Tunisia	7169
Arabic - U.A.E.	14337
Arabic - Yemen	9217
Basque - Spain	1069
Belarusian - Belarus	1059
Bulgarian - Bulgaria	1026
Catalan - Spain	1027
Chinese - Hong Kong	3076
Chinese - PRC	2052

System language	LCID
Chinese - Singapore	4100
Chinese - Taiwan	1028
Croatian - Croatia	1050
Czech - Czech Republic	1029
Danish - Denmark	1030
Dutch - Belgium	2067
Dutch - Netherlands	1043
English - Australia	3081
English - Belize	10249
English - Canada	4105
English - Caribbean	9225
English - Ireland	6153
English - Jamaica	8201
English - New Zealand	5129
English - South Africa	7177
English - Trinidad	11273
English - United Kingdom	2057
English - United States	1033
Estonian - Estonia	1061
Faeroese - Faeroe Islands	1080
Farsi - Iran	1065
Finnish - Finland	1035
French - Belgium	2060
French - Canada	3084
French - France	1036
French - Luxembourg	5132
French - Switzerland	4108
German - Austria	3079
German - Germany	1031
German - Liechtenstein	5127
System language	**LCID**

System language	LCID
German - Luxembourg	4103
German - Switzerland	2055
Greek - Greece	1032
Hebrew - Israel	1037
Hungarian - Hungary	1038
Icelandic - Iceland	1039
Indonesian - Indonesia	1057
Italian - Italy	1040
Italian - Switzerland	2064
Japanese - Japan	1041
Korean - Korea	1042
Latvian - Latvia	1062
Lithuanian - Lithuania	1063
Norwegian - Norway (Bokmal)	1044
Norwegian - Norway (Nynorsk)	2068
Polish - Poland	1045
Portuguese - Brazil	1046
Portuguese - Portugal	2070
Romanian - Romania	1048
Russian - Russia	1049
Serbian - Serbia (Cyrillic)	3098
Serbian - Serbia (Latin)	2074
Slovak - Slovakia	1051
Slovene - Slovenia	1060
Spanish - Argentina	11274
Spanish - Bolivia	16394
Spanish - Chile	13322
Spanish - Colombia	9226
Spanish - Costa Rica	5130
Spanish - Dominican Republic	7178

System language	LCID

System language	LCID
Spanish - Ecuador	12298
Spanish - El Salvador	17418
Spanish - Guatemala	4106
Spanish - Honduras	18442
Spanish - Mexico	2058
Spanish - Nicaragua	19466
Spanish - Panama	6154
Spanish - Paraguay	15370
Spanish - Peru	10250
Spanish - Puerto Rico	20490
Spanish - Spain (Modern Sort)	3082
Spanish - Spain (Traditional Sort)	1034
Spanish - Uruguay	14346
Spanish - Venezuela	8202
Swedish - Finland	2077
Swedish - Sweden	1053
Thai - Thailand	1054
Turkish - Turkey	1055
Ukrainian - Ukraine	1058
Vietnamese - Vietnam	1066

'system' user

The **system** user is created automatically. By default, the system user has all function privileges. This user can log in to process administration, ARIS Administration, User Management, and ARIS Process Board. In ARIS Architect and ARIS Designer, this user has all access privileges for all database groups of all databases. This user only uses up a license if a license privilege is activated for this user. The default password is **manager**. You should change the default password to prevent unauthorized access. You can change all user data except for the user name.

- Having more than one system user can avoid problems, if, for example, your single system user has forgotten his password. You can create additional system users or copy the existing system user. If your only system user was deleted accidentally, create a new one by using the superuser.

T

Tenant

A tenant is a container providing its own ARIS Administration and ARIS data set, such as configuration, ARIS method, databases, scripts, etc.

Each tenant provides users with a particular set of functionalities and specific data depending on their licenses and privileges.

After the installation two tenants are available. The infrastructure master tenant manages administrative users and all other tenants. The **default** tenant is available for operational use. It handles databases, documents, users/user groups, licenses etc. A single physical ARIS installation can host multiple operational tenants. Users of a specific tenant cannot access data from other tenants. A tenant is a kind of logical ARIS installation. Tenants do not share any data.

TLS

Transport **L**ayer **S**ecurity (**TLS**).

TLS is known under the name of **S**ecure **S**ockets **L**ayer (**SSL**). It is an encryption protocol to ensure a secure data transfer through the Internet.

U

Update

Adjusting an installed system to the next minor version including the previous content.

Example: Update the version **10.3** to version **10.4**.

Upgrade

Synonym for Migration:

Installing a new major version and including the previous content.

Example: Upgrade from version **9.8 Service Release 7** to version **10.0**.

7   Disclaimer

ARIS products are intended and developed for use by persons. Automated processes, such as the generation of content and the import of objects/artifacts via interfaces, can lead to an outsized amount of data, and their execution may exceed processing capacities and physical limits. For example, processing capacities are exceeded if models and diagrams transcend the size of the modeling area or an extremely high number of processing operations is started simultaneously. Physical limits may be exceeded if the memory available is not sufficient for the execution of operations or the storage of data.

Proper operation of ARIS products requires the availability of a reliable and fast network connection. Networks with insufficient response time will reduce system performance and may cause timeouts.

If ARIS products are used in a virtual environment, sufficient resources must be available there in order to avoid the risk of overbooking.

The system was tested using scenarios that included 100,000 groups (folders), 100,000 users, and 1,000,000 modeling artifacts. It supports a modeling area of 25 square meters.

If projects or repositories are larger than the maximum size allowed, a powerful functionality is available to break them down into smaller, more manageable parts.

Some restrictions may apply when working with process administration, ARIS Administration, ARIS document storage, and ARIS Process Board, and when generating executable processes. Process Governance has been tested and approved for 1000 parallel process instances. However, the number may vary depending on process complexity, for example, if custom reports are integrated.

ARIS document storage was tested with 40.000 documents. We recommend monitoring the number and overall size of stored documents and archiving some documents if needed.