ARIS

CLOUD CONTROLLER (ACC) COMMAND-LINE TOOL

VERSION 10.0 - SERVICE RELEASE 10

October 2019

Contents

1 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 as **<bold text in angle brackets>**.
- Example texts that are too long to fit on a single line, such as a long directory path, are wrapped to the next line by using ↵ 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.

2   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. You can use it in multiple modes.

ARIS Cloud Controller can be used in multiple modes (page 3).

To start ACC under a Windows operating system click **Start > All Programs > ARIS > Administration > Start ARIS Cloud Controller**. If you have changed agent user credentials you must enter the user name and/or the password.

To start ACC under a Linux operating system, execute the **acc10.sh** shell script instead.

2.1 How to start 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.

To start ACC under a Windows operating system click **Start > All Programs > ARIS > Administration > Start ARIS Cloud Controller**. If you have changed agent user credentials you must enter the user name and/or the password.

To start ACC under a Linux operating system, execute the **acc10.sh** shell script instead.

Enter **help** or **help <command>** to get information about the usage of the commands.

> **Warning**
>
> Using ACC commands will deeply affect your system. This requires profound knowledge of the technical ARIS infrastructure and environment. 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). If you use ACC commands without this knowledge or without the services of Software AG, according to the standard Software AG software maintenance agreement, we cannot guarantee proper functioning.

ARIS Cloud Controller (ACC) can be used in three modes:

- **Interactive mode (default)**

  ACC runs with an interactive shell, allowing you to manually issue commands.

- **Batch mode**

  Activated by specifying a command file with the **-f** command line parameter (see ACC command line parameters below). ACC will execute the commands in the file in the given sequence and exit after execution or if one of the commands fails.

  A command file line starting with **#** will be interpreted as a comment line and ignored by ACC.

- **Command mode**

  You can directly pass a single command to ACC as a command line parameter. The command will be executed and ACC will exit afterwards.

  When passing commands directly as an ACC command line parameter, you have to be careful when escaping strings in your command, for example, double-quote-delimited parameters. The operating system command **shell** will consume the double quotes, leaving your string parameter unescaped. So please escape the quote characters.

  If you issue the command in command mode, for example:

  ```
  set remote.repository.url="http://something.com/repo"
  ```

  You should enter:

  ```
  acc.bat -h localhost -u <user name> -pwd <remoteAccessPassword> set
  remote.repository.url=\"http://something.com/repo\"
  ```

  If you enter:

  ```
  acc.bat -h localhost -u <user name> -pwd <remoteAccessPassword> set
  remote.repository.url="http://something.com/repo"
  ```

ACC will return an error message, for example:

```
line 1:52 mismatched character '<EOF>' expecting '\n'
Invalid or erroneous command "set
remote.repository.url=http://something.com/repo ": line 1:30 extraneous
input ':' expecting EOF
```

▪ Use "help" to display a list of available commands.

2.2 How to connect nodes

When you start ACC in one of the three usage modes without any additional command line parameter, it will by default connect to the node installed by the setup program. There are three options to specify nodes you want to control with ACC:

▪ You can use the **add node** command to put the individual cloud nodes under ACC's control. This requires profound knowledge of the technical ARIS infrastructure and environment. The required know-how can be acquired only by attending the training course **ARIS Server Installation**.

▪ Alternatively, you can list all your cloud nodes in a node file and pass this file to the ACC with the **\-n** (or **--nodefile**) command line option.

▪ If you only want to connect to a single node and issue commands there, you can also use the ACC's **-h** (or **--host**) command line option to directly specify the host or IP name of the node you want to control with ACC.

2.3 How to list runnables

Start ACC and enter **list** to monitor the status of all runnables. This example shows ACC of a current ARIS Server installation for a medium number of users.

```
ACC+ localhost>list
Node localhost - 16 installed runnables.
ID                  State   Version  Type
zoo_m                STARTED 10.0.8 com.aris.runnables.zookeeper-run-prod
postgres_m            STARTED 10.0.8 com.aris.runnables.PostgreSQL-run-prod
cloudsearch_m         STARTED 10.0.8 com.aris.cip.y-cloudsearch-run-prod
elastic_m             STARTED 10.0.8 com.aris.runnables.elasticsearch-run-prod
umcadmin_m            STARTED 10.0.8 com.aris.umcadmin.y-umcadmin-run-prod
adsadmin_m            STARTED 10.0.8 com.aris.adsadmin.y-adsadmin-run-prod
abs_m                STARTED 10.0.8 com.aris.modeling.components.y-server-run-prod
octopus_m             STARTED 10.0.8 com.aris.octopus.y-octopus_server-run-prod
apg_m                STARTED 10.0.8 com.aris.age.age-run-prod
copernicus_m          STARTED 10.0.8 com.aris.copernicus.copernicus-portal-server-
run-prod
ecp_m                STARTED 10.0.8 com.aris.runnables.ecp-run-prod
simulation_m          STARTED 10.0.8
com.aris.modeling.components.simulationserver.y-simuserver-run-prod
loadbalancer_m       STARTED 10.0.8 com.aris.runnables.httpd.httpd-run-prod
dashboarding_m       STARTED 10.0.8 com.aris.dashboarding.dashboarding-run-prod
businesspublisher_m STARTED 10.0.8
com.aris.modeling.components.businesspublisher.y-bp-server-run-prod
arcm_m               STARTED 10.0.8 com.aris.arcm.arcm-run-prod
```

The state of all runnables represented by their instance IDs is listed. Possible states are:

- **UNKNOWN**: The runnable state is not yet known. This state is shown directly after ARIS Agent was started.

- **STOPPED**: The runnable is currently not running.

- **STARTING**: The runnable is starting, but this process is not complete yet.

- **STARTED**: The runnable is running.

- **STOPPING**: The runnable is stopping, but this process is not complete yet.

- **DEACTIVATED**: The runnable is not in use. It has been deactivated manually and can be activated if necessary. If the **dashboarding** runnable is in this state, that does not have to be an error. This runnable is deactivated if ARIS Server was installed without ARIS Aware.

- **DOWN**: This runnable started and crashed. ARIS Agent will attempt to automatically restart the runnable momentarily.

- **FAILED**: This runnable has crashed. ARIS Agent has given up trying to restart the runnable.

If a runnable does not start properly, read the **Basic Troubleshooting** guide.

2.4   What runnables are available?

This table lists all runnables run by ARIS Server or ARIS Publisher Server (Publisher) and the locally installed server installed by the ARIS Client Setup (LOCAL) for a medium number of users installation. That's why all runnables end with **_m**. Installations for a small or a large number of users are typified with **_s** or **_l**. If ARIS was installed using the setup program, the default instance IDs are used as shown in the table.

Runnables run by the server **LOCAL** are not accessible by ACC. This server is only available in combination with ARIS Client installations.

Runnable	ARIS Server	ARCM	Publisher	LOCAL
	Runnables run by different server types			
Instance ID: **zoo_m** Name: Service registry Description: This runnable is a server component managing the communication, configuration and status information of all available runnables and external services.	x	x		x
Instance ID: **postgres_m** Name: Modeling database Description: 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.	x	x		x
Instance ID: **cloudsearch_m** Name: Search index Description: Main full-text search and graph structure index for modeling data. It allows fast access to the data stored in the modeling database, Oracle® or Microsoft® SQL database.	x	x		x

Runnable	ARIS Server	ARCM	Publisher	LOCAL
Instance ID: **elastic_m** Name: Document index (Elasticsearch) Description: Main full-text search index for documents and collaboration data. It also stores users, user groups, licenses, and privileges.	x	x		x
Instance ID: **adsadmin_m** Name: ARIS document storage management Description: Server component managing ARIS document storage.	x	x		
Instance ID: **umcadmin_m** Name: ARIS Administration/User Management Description: Server component managing users, permissions, licenses, LDAP connectivity and SSO.	x	x		x
Instance ID: **loadbalancer_m** Name: Load balancer Description: Central point of entry for all ARIS clients to the entire ARIS application, typically accessed via HTTP ports 80 or 1080, or HTTPS ports 443 or 1443. It distributes the workload across the installed components.	x	x		
Instance ID: **abs_m** Name: Modeling/publishing/reporting Description: Main server component for modeling and operations on modeling data including report execution.	x	x		x

Runnable	ARIS Server	ARCM	Publisher	LOCAL
Instance ID: **hds_m** (optional; not by setup) Name: Heavy-duty Server (HDS) Description: HDS is an additional component that reduces the load of ARIS reports running on you **abs** instance.	x			
Instance ID: **cdf_m** (optional; not by setup) Name: Cloud Decoupling Framework (CDF) Description: CDF is a queue that can be used to decouple synchronous accesses to services. It is required for communication between the **abs** instance and the **hds** instance. If multiple **arcm** runnables are installed, a **cdf** runnable is mandatory.	x			
Instance ID: **apg_m** Name: Process Governance Description: Process Governance server component. Executes processes and provides managing user interfaces.	x			
Instance ID: **copernicus_m** Name: Portal Description: Server component providing the portal in ARIS Connect.	x			
Instance ID: **octopus_m** Name: Analysis Description: Server component processing ad hoc analyses and queries triggered in ARIS Architect or ARIS Designer.	x			x

Runnable	ARIS Server	ARCM	Publisher	LOCAL
Instance ID: **ecp_m** Name: Collaboration Description: Server component of the collaboration component in ARIS Connect.	x			x
Instance ID: **simulation_m** Name: Simulation Description: Server component of the simulation functionality in ARIS Architect.	x			x
Instance ID: **dashboarding_m** Name: Dashboards (ARIS Aware) Description: Server component of the dashboarding component in ARIS Connect.	x			
Instance ID: **businesspublisher_m** Name: ARIS Publisher server Description: Server component of the ARIS Publisher functionality in ARIS Architect.			x	
Instance ID: **arcm_m** Name: ARIS Risk & Compliance Manager server Description: Server component of ARIS Risk & Compliance Manager.		x		

2.5   Use cases

In these chapters product-related examples for configuring the system are available.

2.5.1   Change the default agent user's password

The ARIS Agent user has access to ARIS Cloud Controller (ACC). If you did not change the default password during the setup process you should do so manually to prevent unauthorized access.

Procedure

1.   Start ARIS Cloud Controller (ACC) (page 3).

2.   Change the password: **set password = "<enter the new password>"**

3.   Stop ACC. Enter: **exit**

4.   Restart ACC.

5.   Enter the new password.

6.   If you use the **Start** icon for ARIS Cloud Controller (**Start > All Programs > ARIS > Administration > ARIS Cloud Controller**) you can change the **password** command line parameter within the **ACC** shortcut. If you do not change the password it will be prompted every time you start ACC.
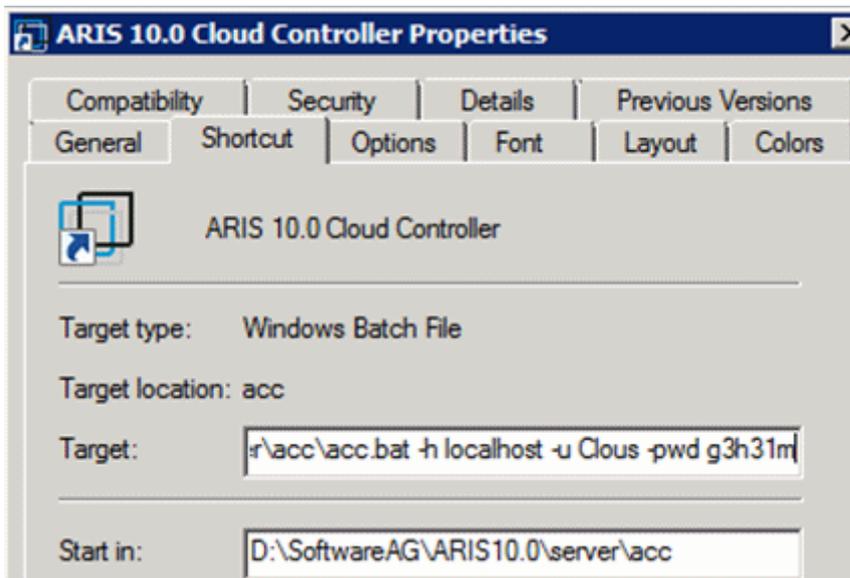
If you run an ARIS server setup after you have changed the password, enter the changed credentials.

2.5.2 Start and stop runnables

The start modus had been selected during the setup process. If you have chosen the option **Start automatically** all runnables will be started in the right order.

Runnables can also be started and stopped independently, but most runnables will not work on their own. You must start all needed runnables in the right order.

- Enter s**tartall** to get all runnables started in correct order.
- Enter **start <instanceId>**, for example, **start abs_m** to start only the runnable **abs** (Modeling & Publishing (Business server))
- Enter **stopall** to stop all runnables.
- Enter **stop <instanceId>**, for example, **stop abs_m** to only stop one runnable.

If you run ARIS on a laptop (8 GB) for demonstration purposes you might want to stop runnables you do not need to ensure more memory for the system.

2.5.3 Deactivate runnable

Deactivation is useful, if you do not yet use a certain runnable, but maybe need it later. If you activate the runnables again, you can still use the setup program to update your ARIS version. To deactivate runnables is safer than removing or shutting them down.

A deactivated runnable cannot be started with a **start** command. They will be ignored by the **startall** command and the agent's runnable autostart.

Prerequisites

Runnables are in **STOPPED** or **FAILED** state.

Procedure

1. Start ARIS Cloud Controller (ACC) (page 3).
2. To deactivate the runnable enter, for example: **deactivate simulation_m**

The **simulation** runnable will not be started, until you have activated it again (page 11).

2.5.4 Activate runnable

You can activate runnables that have been deactivated (page 11). This is required before starting an update setup.

Procedure

1. Start ARIS Cloud Controller (ACC) (page 3).
2. To activate the runnable enter, for example: **activate simulation_m**

The **simulation** runnable can be started again.

2.5.5 Provide additional memory

If you have performed an installation for small (s), medium (m) or large (l) memory requirement, you can provide additional memory for runnables.

Procedure

1. Start ARIS Cloud Controller (ACC) (page 3).

2. Enter **reconfigure <runnable> +JAVA-Xmx="<**memory requirement**>"**.

The affected runnables will be started after the settings have been updated.

Examples

- **reconfigure abs_s +JAVA-Xmx="1152m"**

   The memory settings for the modeling runnable of an s installation will be increased to max. 1152 MB.

- **reconfigure abs_m +JAVA-Xmx="6G"**

   The memory settings for the modeling runnable of an m installation will be increased to 6 GB.

2.5.6 Make SSL certificate available for ARIS Server

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 the ***.key** file and the ***.crt** file into a ZIP archive.

2. Copy this ZIP file to a local directory that can be accessed by ARIS Cloud Controller (ACC).

3. Start ARIS Cloud Controller (ACC) (page 3).

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 (see: **Basic Troubleshooting Guide**).

2.5.7 Redirect ports

In case of port conflicts (see **Basic Troubleshooting Guide**) redirect the ports, for example, the default HTTP port **80** or the HTTPS port **443**.

Procedure

1. Start ARIS Cloud Controller (ACC) (page 3).

2. Run a **reconfigure** command on the **loadbalancer** runnable.

   To make the **loadbalancer** runnable know through which ports users are now accessing it, you need to run an ACC **reconfigure** command with the following syntax:

   reconfigure loadbalancer_<SIZING>
   HTTPD.zookeeper.application.instance.http.port=<externalHttpPort>
   HTTPD.zookeeper.application.instance.port=<externalHttpsPort>

   Replace **<SIZING>** with the sizing you used to install ARIS Server, such as **s**, **m**, or **l**.

   Replace **<externalHttpPort>** with the port from which you redirect to the physical HTTP port of the **loadbalance**r runnable (usually port **80**).

   Replace **<externalHttpsPort>** with the port from which you redirect to the physical HTTPS port of the **loadbalance**r runnable (usually port **443**).

   This example, tells the **loadbalancer** runnable in an **m** size installation that users are now accessing it through the redirected ports **80** and **443**:

   reconfigure loadbalancer_m HTTPD.zookeeper.application.instance.http.port=80
   HTTPD.zookeeper.application.instance.port=443

ARIS users acces ARIS using the redirected ports.

If runnables do not start up properly, resolve possible port conflicts.

2.5.8   Redirect HTTPS port

To make ARISaccessible under a privileged port on a Linux system, a user with root privileges has redirect the ports, for example, the HTTP port **80** or the HTTPS port **443**.

If you have forced the **loadbalancer** runnable to use HTTPS using an ACC command, such as:

reconfigure loadbalancer_m +HTTPD.EnforceHTTPS="true"

connections cannot be established. This is because users are forwarded to **https://<server name>:1443/** instead of **https://<server name>**.

You must redirect the HTTPS port to **443**.

Procedure

1. Start ARIS Cloud Controller (ACC).

    ARIS Cloud Controller can be used in multiple modes (page 3).

    To start ACC under a Windows operating system click **Start > All Programs > ARIS > Administration > Start ARIS Cloud Controller**. If you have changed agent user credentials you must enter the user name and/or the password.

    To start ACC under a Linux operating system, execute the **acc10.sh** shell script instead.

2. Enter:

    reconfigure loadbalancer_m HTTPD.redirect.https.port=":443"

    You must enter a colon followed by the port number.

Users are forwarded correctly.

2.5.9　　　Collect log files (ACC)

If problems occur during operation, you can use log files to find and resolve errors. You can download zipped log files related to each runnable or you can download all available log files.

Procedure

1. Start ARIS Cloud Controller (ACC) (page 3).

2. To collect log files, for example related to the **abs_l** runnable, enter: **collect log files for abs_l**

   To collect all log files, enter: **collect log files** or **collect logfiles**

   You can use additional parameters. Enter **help** or **help <command>** to get information about the usage of the commands.

All log files are stored as a ZIP archive.

If you cannot solve the problems and have a maintenance agreement, please send an error description and the ZIP archives containing collected log files as well as the entire contents of the **log** and **config** directories to the ARIS Global Support via Empower (http://www.softwareag.com/premiumsupport).

2.5.10　　　Delete log files

Log files may contain private data of ARIS users, such as IP addresses, MAC addresses, or user names. In order to comply with the **G**eneral **D**ata **P**rotection **R**egulation (GDPR), you can collect log files using ACC or the ACC interface, find personal data related to deleted users, and manually delete or anonymize log file entries in source files.

Warning

If you delete log files (page 16), Software AG might no longer be able to support you in order to resolve software problems.

In order to delete all log files, you must stop (page 11) the related runnables to allow unhindered access to all files. If you do not stop the runnables, some files may be locked and cannot be deleted.

Procedure

1. Start ARIS Cloud Controller (ACC) (page 3).

2. To delete log files, for example related to the **abs_l** runnable, enter: **delete log files for abs_l**

   To delete all log files, enter: **delete log files** or **delete logfiles**

All log files that are not accessed by a runnable are deleted. Log files that were not deleted are listed.

2.5.11 ARIS Administration/ARIS Risk & Compliance Manager

If you have installed ARIS Risk & Compliance Manager and ARIS Server you can force ARIS Risk & Compliance Manager to use the ARIS Administration of the ARIS Server.

2.5.11.1 Specify a white list for ARIS Administration

You can specify a white list for ARIS Administration.

A white list or black list is a positive or negative list with which systems can be protected. White lists and black lists pursue opposing strategies.

A white list contains all permitted URLs. A blacklist, on the other hand, specifically excludes URLs.

Procedure

1. Navigate to **<ARIS installation path>\server\bin\work\work_umcadmin_m**, for example, **C:\ARIS10.0\server\bin\work\work_umcadmin_m**.

2. Start ARIS Cloud Controller (ACC) (page 3).

   To start ACC under a Windows operating system click **Start > All Programs > ARIS > Administration > Start ARIS Cloud Controller**. If you have changed agent user credentials you must enter the user name and/or the password.

   To start ACC under a Linux operating system, execute the **acc10.sh** shell script instead.

3. Stop the ARIS Administration runnable. Enter, for example, **stop umcadmin_<s**, **m**, or **l>**.

4. You must use regular expressions for the white list. A regular expression is a character string used to describe sets of character strings using certain syntactic rules.

   Enter reconfigure **umcadmin_<s, m, or l> "JAVA-Dcom.aris.umc.whitelist.url.regex.pattern"="<comma-separated ist of regular expressions>"**.

   Example

   If you want to allow a URL whose name consists of one word in lowercase letters and begins with **https://** and ends with **.com**, use the following regular expression:

   https://[a-z]+.com

   if you want to allow graphics of **jpg** type whose name consists of uppercase and lowercase letters and numbers and which are located in subdirectories of a URL that begins with **https://** and ends with **.com**, use the following regular expression:

   https://([a-z]*.)[a-z]*[.com](/[a-z]*)(/[a-z]*)(/[A-Za-z0-9_]+.jpg)

5. Start the ARIS Administration runnable. Enter, for example, **start umcadmin_<s**, **m**, or
    l>.

you have specified a white list for ARIS Administration.

You can remove the white list again. To do so, proceed as described above and configure
reconfigure umcadmin_m -"JAVA-Dcom.aris.umc.whitelist.url.regex.pattern".

2.5.11.2 Use existing ARIS document storage and ARIS Administration for ARIS Risk & Compliance Manager

After you have installed ARIS Risk & Compliance Manager this installation uses a separate set
of runnables, for example, ARIS Administration or ARIS document storage. This means that
the administrator has to manage users and documents. If you already use ARIS Server and
have installed ARIS Risk & Compliance Manager later you can reconfigure your ARIS Risk &
Compliance Manager runnable to your productive ARIS Server installation. This will make ARIS
Risk & Compliance Manager available to all users of your productive system and only one ARIS
document storage will be in use.

1. Start ARIS Cloud Controller (ACC) (page 3). on your ARIS Risk & Compliance Manager
    installation.

2. To reconfigure ARIS Risk & Compliance Manager and force that runnable to use the ARIS
    Administration of your ARIS Server installation, enter: **reconfigure arcm_<s,m or l>**
    zookeeper.connect.string="<ARISServer>\\:14281"

ARIS Risk & Compliance Manager is now accessible via the ARIS Server name, for example,
http://arisserver/arcm by all users managed within the ARIS Administration of your
productive system.

To ensure more memory for the ARIS Risk & Compliance Manager system you can shut down
all other runnables or remove them.

2.5.12   Process Governance

For information on Process Governance customization, please refer to the **Process Governance Command-Line tool.PDF** and the **Process Governance Customizing. PDF**. Technical documents are available on:

- ARIS DVD (...Documents\English\5 Customizing)
- Empower (https://empower.softwareag.com/) (login required)
- ARIS Download Center (https://aris.softwareag.com/)

2.5.13   ARIS Aware

You can make custom widgets available for ARIS Aware.

2.5.13.1   Make enhancements available

If you want to use self-designed widgets, **LESS** files, or **CSS** files in your ARIS Aware dashboards you must enhance each **dashboarding** runnable of your ARIS Server installation with these files. Enhanced files are not affected by an update setup. They will be preserved.

Procedure

1. Start ARIS Cloud Controller (ACC) (page 3).

2. To make the custom resource available enter, for example: **enhance dashboarding_m with customResource local file "C:\\mywidgets.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.

The **ZIP** file including its contained folder structure is automatically extracted to the path:

%INSTANCEDDIR%\base\webapps\mashzone

2.5.14   ARIS Publisher

In this chapter product-related examples for configuring the system are available.

2.5.14.1   Provide ARIS Publisher license files

You can provide license files for ARIS Publisher Server using ACC. All other licenses are managed by ARIS Administration.

Procedure

1. Save the zip file to a local directory that can be accessed by ARIS Cloud Controller (ACC), for example: **d:/Publisher_Server_key**.**zip**

2. Start ARIS Cloud Controller (ACC) (page 3).

3. Stop the **businesspublisher** runnable. Enter, for example: **stop businesspublisher_l**

4. Provide the license using this command: **enhance <runnable> with license local file <path to the saved file>**

   Example: **enhance businesspublisher_l with license local file "d:\\Publisher_Server_key**.**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: **"d:/Publisher_Server_key**.**zip"**.

5. Start the **businesspublisher** runnable. Enter, for example: **start businesspublisher_l**.

The license is available.

2.5.14.2 Reconfigure ARIS Publisher settings

Settings entered during the setup process can be adjusted. Use the **reconfigure** ACC command (page 22) (see ARIS Cloud Controller (ACC) Command-Line Tool.pdf document) to change settings. When performing an update setup all modifications made manually in CFG or XML files will be lost.

In this example, the Oracle connection parameters of ARIS Publisher Server will be modified and the user management of another ARIS Server will be used. Also, the connection parameters to Process Governance can be adjusted.

Procedure

1. Start ARIS Cloud Controller (ACC) (page 3).

2. Reconfigure **businesspublisher_<s**, **m**, or **l>** and force that runnable to use the ARIS Administration of your ARIS Server installation.

   Ensure that all values used in the **reconfigure** command, for example, for the keys **username** or **password** actually match to the values used in the <ARIS installation path>\server\bin\work\work_businesspublisher_<s, m or l>\base\webapps\businesspublisher\config**webappserver.cfg** file and the **umcconfig.cfg** file. If typing errors happened during the setup process the affected values must be adjusted.

   For better readability, the parameters of the reconfigure command are shown with line-wraps. For execution you must enter a single-line command.

   #Database connection parameters (in this example an Oracle database system is used)

   bp.ado.database="**com.idsscheer.aris.businesspublisher.application.dao.database. AOracleDAO**"

   bp.db.driver="**oracle.jdbc.OracleDriver**"

   bp.db.url=**"jdbc:oracle:thin:@//oracle-srv.domain.tld:1521:oracle_sid"**

   bp.db.validation.query="select 1 from dual"

   bp.db.username="**ARISBP**"

   bp.db.passwd="**ARISBP**" (You can also enter encrypted passwords.)

   bp.arisbpdata="**ARISBPDATA**"

   bp.arisbpindex="**ARISBPINDEX**"

   #ARIS Administration connection parameters

   bp.login.module="**UMCLogin**"

   "**UMCLogin**" can be found in the **webappserver.cfg** file. This parameter value switches the ARIS Publisher Server's user management to the User Management of the defined ARIS Server ARIS Administration.

   bp.umc.server.url="**http://<aris-design-or-connect-srv>.domain.tld:**<port number>**/umc**"

This URL can be found in the **umcconfig.cfg** file. It directs to the user management of the ARIS Server ARIS Administration. Enter the port number used during setup. The **default** port number is 80 (Windows operating systems) or 1080 (page 14) (Linux operating systems).

bp.umc.admin.login="**superuser**"

bp.umc.admin.passwd="<**superuser's password>**"

The ARIS Administration user name and password can be found in the **umcconfig.cfg** file. By default the **superuser** user has access to the user management and holds all required permissions. For security reasons, you are recommended to encrypt the password using the ARIS Server Administrator command **encrypt** (see ARIS Server Administrator Command-Line Tool.pdf).

 # APG

bp.age.host="<**aris-design-or-connect-srv>.domain.tld**"

bp.age.port=80

3. For execution enter a single-line command. For better readability, the parameters of the reconfigure command are shown with line-wraps, for example:

    reconfigure businesspublisher_**<s**, **m**, or **l>**

    bp.ado.database="com.idsscheer.aris.businesspublisher.application.dao.database.AOracle DAO"

    bp.db.driver="oracle.jdbc.OracleDriver"

    bp.db.url="jdbc:oracle:thin:@//oracle-srv.domain.tld:1521:oracle_sid"

    bp.db.validation.query="select 1 from dual"

    bp.db.username="ARISBP"

    bp.db.passwd="ARISBP"

    bp.arisbpdata="ARISBPDATA"

    bp.arisbpindex="ARISBPINDEX"

    bp.login.module="UMCLogin"

    bp.umc.server.url="http://<aris-design-srv>.domain.tld:<port number>/umc"

    bp.umc.admin.login="superuser"

    bp.umc.admin.passwd="<**superuser's password>**"

    bp.age.host="<aris-design-srv>.domain.tld"

    bp.age.port=80

This **businesspublisher_<s**, **m**, or **l>** runnable is reconfigured. Publisher users are authenticated via ARIS Administration and ARIS document storage will be available if it has been connected to the ARIS Publisher Server.

These modifications will not be affected by update setups. When performing an update setup all modifications made manually in CFG or XML files will be lost.

2.5.14.3   Configure the service 'Create static ARIS Publisher export' for Process Governance

Settings entered during the setup process can be adjusted. Use the **reconfigure** ACC command (page 22) (see ARIS Cloud Controller (ACC) Command-Line Tool.pdf document) to change settings. When performing an update setup all modifications made manually in CFG or XML files will be lost. You can configure, that the **Create - Static ARIS Publisher export** service supports the port information.

Procedure

1. Start ARIS Cloud Controller (ACC) (page 3) on your <_apg_server>.

2. Enter the folllowing command, for example: **reconfigure apg_m JAVA-Dcom.idsscheer.age.serviceenabling.staticExport.wsServer="<myARIShost>:<port>/aris/apgstatic"**

    Ensure that all values used in the **reconfigure** command, for example, for the keys **username** or **password** actually match the values used in the <ARIS installation path>\server\bin\work\work_apg_<s, m or l>. If typing errors happened during the setup process the affected values must be adjusted.

This **apg_m** runnable is reconfigured.

These modifications will not be affected by update setups. When performing an update setup all modifications made manually in CFG or XML files will be lost.

2.5.15　Collaboration

In this chapter related examples for configuring the system are available.

2.5.15.1　Specify a black list for Collaboration

You can specify a black list for Collaboration. Collaboration is the platform for cooperation across teams. With Collaboration, information can be exchanged faster, knowledge can be shared, and cooperation across borders is improved. Collaboration is a forum in which users can mention any URL in posts. It is therefore more appropriate to define a black list.

A white list or black list is a positive or negative list with which systems can be protected. White lists and black lists pursue opposing strategies.

A white list contains all permitted URLs. A blacklist, on the other hand, specifically excludes URLs.

Procedure

1. Navigate to **<ARIS installation path>\server\bin\work\work_ecp__<s, m**, or **l>**, for example, **C:\ARIS10.0\server\bin\work\work_ecp_m**.

2. Start ARIS Cloud Controller (ACC) (page 3).

   To start ACC under a Windows operating system click **Start > All Programs > ARIS > Administration > Start ARIS Cloud Controller**. If you have changed agent user credentials you must enter the user name and/or the password.

   To start ACC under a Linux operating system, execute the **acc10.sh** shell script instead.

3. Stop the Collaboration runnable. Enter, for example, **stop ecp_<s, m**, or **l>**.

4. You must use regular expressions for the white list. A regular expression is a character string used to describe sets of character strings using certain syntactic rules.

   Enter reconfigure **ecp_<s, m, or l> "JAVA-Dcom.aris.umc.blacklist.url.regex.pattern"="<comma-separated ist of regular expressions>"**.

   Example

   If you want to block yahoo.com, use the following regular expression:

   (http(s)?://)?([\\\w-]+\\.)+[\\\w-]+[\\yahoo\\.com]+(/[/?%&=]*)?

5. Start the Collaboration runnable. Enter, for example, **start ecp_<s**, **m**, or **l>**.

you have specified a black list for ARIS Administration.

You can remove the black list again. To do so, proceed as described above and configure **reconfigure ecp_m -"ecp.blacklist.url.regex.pattern"**.

2.5.15.2   Create synchronization user

The synchronization user serves technical purposes only. No function or license privileges are assigned to this user. The synchronization user is required for synchronization processes executed in the background of Collaboration, for example, to synchronize the user data between ARIS Administration and Collaboration.

The synchronization user is automatically generated for every newly created tenant. If the synchronization user is not available, the **system** user is used instead, provided that the default password of the **system** user was not changed. If the **system** user cannot be used, you must manually create the synchronization user using ARIS Cloud Controller. By default, the synchronization user name is **_aris_tech_user_ecp_techuser**.

Procedure

1. Start ARIS Cloud Controller (ACC) (page 3).

2. To create the synchronization user enter, for example:

   enhance umcadmin_m with createUser trigger only options tenant.name=<tenant name> tenant.user.name="<user name>" tenant.user.pwd="<user password>" affected.user="<synchronization user name>" affected.email="<synchronization user e-mail>" affected.pwd="<synchronization user password>" as.technical.user="true"

   set tenant default data for app umc ecpTechnicalUserName="<synchronization user name>" ecpTechnicalUserPassword="<synchronization user password>"

The user is created and made available for the **ecp** runnable.

2.5.15.3   Anonymize Collaboration user

You can anonymize deleted Collaboration users according to GDPR.

Prerequisites

The user was deleted in ARIS Administration.

Procedure

1. Start ARIS Cloud Controller (ACC) (page 3).

2. To anonymize, for example, the deleted **y4711** user on **ecp_m** enter: **invoke anonymizeUser on ecp_m anonymize.user=y4711**

Activities of this Collaboration user, such as posts, comments, groups, are shown with **Anonymized user** instead with the **y4711** user name. If several users are anonymized a number is added, such as **Anonymized user 2**.

2.5.16   Tenant Management

In this chapter related examples for configuring the system are available.

2.5.16.1   Create a tenant

After the installation of ARIS Connect the **default** tenant is available. If you need additional tenants to provide different sets of databases, users, configurations or ARIS methods you can easily create tenants. If you are going to create additional tenants for ARIS10.0 to migrate data from ARIS 9.8.7 or later, make sure to use identical names in both ARIS versions. You can also create tenants using the ARIS Administration's command line tools or Tenant Management.

Prerequisites

- ARIS Server installation

- Users need the **User administrator** function privilege

- If you do not use the standard database system, make sure to create additional schemes in your Oracle or Microsoft SQL database management system and assign the tenants (page 41) to these schemes (see ARIS Server Installation Guide).

Warning

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

Procedure

1. Start ARIS Cloud Controller (ACC) (page 3).

2. Enter: **create tenant <tenant name> username=<user name of a user holding the required privileges> password=<this user's password>**.

    Example: **create tenant test01 master.tenant.user.name = admin master.tenant.user.pwd= tenantmanager123**

    You can even change parameters for the new tenant. You must specify additional parameters in case you use an external database management system, for example:

    create tenant test01 dba.user="system" dba.user.pwd="manager" dbinstanceid="db0000000000" default.tbl.space="ARISDATA" temp.tbl.space="TEMP" schema.name=aris_<tenant ID>" schema.pwd="*ARIS!1dm9n#yy"

    The tenant **test01** will be created.

3. The administrator must import licenses, create users and user groups and assign privileges and licenses for the **test01** tenant.

4. Start a ARIS client and log in using this tenant. The system database will be created for that tenant.

The tenant is created and can be backed up (page 28).

2.5.16.2 Back up a tenant

You can back up tenant data (page 32) using the ARIS Cloud Controller (ACC). If you want to include the user statistics, the property **User statistics in backup** (**com.aris.umc.user.statistics.backup**) must be enabled in the configuration (see ARIS help: ARIS Administration > Configuration > User management > Security > Advanced settings). Please note that no user can work on this tenant during the backup process.

Prerequisites

- ARIS Server installation
- Users need the following function privileges. The function privileges depend on the license. Therefore, you may not be able to assign all of the function privileges shown.

  - Analysis administrator
  - ARCM administrator
  - Collaboration administrator
  - Database administrator
  - Dashboard administrator
  - Document administrator
  - License administrator
  - Portal administrator
  - Process Governance administrator
  - Server administrator
  - Technical configuration administrator
  - User administrator

Warning

Tenant data is fully backed up only if the user executing the commands has sufficient privileges for all components in every tenant and if all components were selected for the backup.

User administration audit events are not part of the tenant backup.

Extensions, for example, SSL certificates (page 12), SAP® Java Connector, and JDBC drivers (page 39), added using the **enhance** ACC command are not backed up.

To avoid data inconsistencies and possible data loss, you must not perform any of the following activities in parallel, neither manually nor scheduled:

- Deleting any Process Governance process instance, process version, or process

- Archiving Process Governance process instances

- Backup/restore tenant (containing Process Governance or ARIS document storage data)

Procedure

1. Start ARIS Cloud Controller (ACC) (page 3).

2. Enter: **backup tenant <tenant name> to <pathToBackUpFile> encryption.key <encryption password or encryption key> username=<user name of a user holding the required privileges>password=<this user's password>**

   such as: **backup tenant default to "f:\\backupDefault.acbcrypt" encryption.key=str3ngG3h31m username=y1234 password=managery1234.**

   Notice the double backslashes. Alternatively, use a single forward slash. If no file name is specified, the file name is generated as for unencrypted files, but with the file extension **acbcrypt** instead of **acb**. The encryption password must be at least 8 characters long and contain at least 3 out of the 4 following character classes: lower-case letter, upper-case letter, digit, special character (such as any non-whitespace, non-letter, non-digit character).

The backup is started. The complete backup is written to one single **acb** archive file. If you encrypted the backup file, the file extension is **acbcrypt**.

You can restore (page 31) this tenant using the related archive file. Using the **restore tenant** command will copy the content to an existing tenant. Process Governance backup archives greater than 2 GB might lead to insufficient TEMP space issue when restoring them into ARIS with Oracle back end. For such large backups, extend the temp tablespace size before restoring operation executed.

You can manage tenants also using the ARIS Administration's command line tools or Tenant Management tool.

2.5.16.3   Delete a tenant

If you delete a tenant all tenant information are lost:

- Databases
- User data (users, privileges and licenses)
- ARIS document storage data including all access rights
- Process Governance data
- Ad hoc analyses and queries

Prerequisites

- ARIS Server installation
- Users need the following function privileges. The function privileges depend on the license. Therefore, you may not be able to assign all of the function privileges shown.

    - Analysis administrator
    - ARCM administrator
    - Collaboration administrator
    - Database administrator
    - Dashboard administrator
    - Document administrator
    - License administrator
    - Portal administrator
    - Process Governance administrator
    - Server administrator
    - Technical configuration administrator
    - User administrator

Warning

If you delete a tenant all tenant information are lost.

Procedure

1. Back up (page 28) the tenant in order to be able to restore (page 31) data again.
2. Start ARIS Cloud Controller (ACC) (page 3).
3. Enter: **delete tenant <Tenant name> username=<user name of a user holding the required privileges> password=<this user's password>**

    Deletes the specified tenant and all its associated data from the system. User name and password of an administrative user have to be specified using the parameters **master.tenant.user.name** and **master.tenant.user.pwd**, respectively.

    Warning

    If the optional **force** keyword is used, the security question **Are you sure?** is not displayed and the tenant and its data will be deleted without further prompting the user.

The tenant has been deleted.

You can also manage tenants using the ARIS Administration's command line tools or Tenant Management.

2.5.16.4   Restore a tenant

You can restore tenant data (page 32) or copy the content of this tenant (page 35) to a different ARIS server. You need to have access to the relevant back-up archive file containing the data of a tenant:

Warning

No user can work on this tenant during the restore process. All current data of a running tenant will be deleted and replaced by the data of the backup file. Data related to ARIS Administration will not be deleted but merged. The tenant name and current user data will be untouched. If users were deleted after the tenant has been backed up, these users will be available again. Make sure to delete those users.

Process Governance backup archives greater than 2 GB might lead to insufficient TEMP space issue when restoring them into ARIS with Oracle back end. For such large backups, extend the temp tablespace size before restoring operation executed.

To avoid data inconsistencies and possible data loss, you must not perform any of the following activities in parallel, neither manually nor scheduled:

- Deleting any Process Governance process instance, process version, or process

- Archiving Process Governance process instances

- Backup/restore tenant (containing Process Governance or ARIS document storage data)

Prerequisites

- You need access to the relevant back-up archive file.

- ARIS Server installation

- Users need the following function privileges. The function privileges depend on the license. Therefore, you may not be able to assign all of the function privileges shown.

    - Analysis administrator

    - ARCM administrator

    - Collaboration administrator

    - Database administrator

    - Dashboard administrator

    - Document administrator

    - License administrator

    - Portal administrator

    - Process Governance administrator

    - Server administrator

    - Technical configuration administrator

    - User administrator

Procedure

1. Start ARIS Cloud Controller (ACC) (page 3).

2. To restore the tenant, enter: **restore tenant <tenant name> from <pathToBackUpFile> encryption.key <encryption password or encryption key> username=<user name of a user holding the required privileges> password=<this user's password>**

   such as: **restore tenant default from "f:\\backupDefault.acbcrypt" encryption.key=str3ngG3h31m username=y1234 password=managery1234**

   or as an example for the us of an unencrypted **acb** file: **restore tenant default from "f:\\backupDefault.acb" username=y1234 password=managery1234**

   Notice the double backslashes. Alternatively, use a single forward slash.

   The tenant will be restored.

3. Make sure to change the standard user's passwords again.

The tenant is restored. You can also manage tenants using the Tenant Management tool or the ARIS Administration's command line tools.

If you have restored a tenant from an ARIS 10 SR5 backup file or earlier containing ARIS document storage data, you must adjust the timestamps manually (page 38) (see **y-admintool.bat** command-line tool).

2.5.16.5   What data is backed up and restored?

If you back up tenants, the current state of the following data is saved in different folders in the tenant backup zip file.

Tenant data is fully backed up only if the user executing the commands has sufficient privileges for all components in every tenant and if all components were selected for the backup. Extensions, for example, SSL certificates (page 12), SAP® Java Connector, and JDBC drivers (page 39), added using the **enhance** ACC command are not backed up. In ARIS 10 all started runnables are automatically taken into account when executing tenant backup/restore commands.

To avoid data inconsistencies and possible data loss, you must not perform any of the following activities in parallel, neither manually nor scheduled:

- Deleting any Process Governance process instance, process version, or process

- Archiving Process Governance process instances

- Backup/restore tenant (containing Process Governance or ARIS document storage data)

Content	Required function privileges	Component (runnable)
Data from ARIS Administration, for example, users, privileges. User statistics are not includes by default. If you want to include the user statistics, the property **User statistics in backup** (**com.aris.umc.user.statistics.backup**) must be enabled in the configuration (**ARIS Administration >** 🔲 **Configuration > User management > Security > Advanced settings**).	User administrator Technical configuration administrator	ARIS Administration/User Management (umcadmin_<s, m, or l>)
Licenses User administration audit events are not part of the tenant backup.	License administrator	
System database Contains filters, templates, and font formats, but also ARIS Method and all evaluation scripts, macros and scheduled reports.	Server administrator	Modeling & Publishing (abs_<s, m, or l>)
ARIS databases	Database administrator	
Ad hoc analyses and queries	Analysis administrator	Analysis (octopus_<s, m, or l>)
ARIS document storage data, including Process Governance archives Documents and access privileges	Document administrator Technical configuration administrator	ARIS document storage (adsadmin_<s, m, or l>)
Process Governance data	Process Governance administrator	Process Governance (apg_<s, m, or l>)
Collaboration data	Collaboration administrator	Collaboration (ecp_<s, m, or l>)

Content	Required function privileges	Component (runnable)
ARIS Risk & Compliance Manager data	ARCM administrator	ARIS Risk & Compliance Manager (arcm_<s, m, or l>)
Dashboards and feeds	Dashboard administrator	ARIS Aware (dashboarding_<s, m, or l>)
ARIS Connect portal views, modification sets, and configuration sets.	Portal administrator	ARIS Connect portal (copernicus_<s, m, or l>)

2.5.16.6   Copy a tenant to a different server

You can copy the content of a backed up tenant to a different ARIS Server. This procedure can also be used to migrate data in case of an upgrade installation. You need to have access to the relevant back-up archive file containing the data of a tenant:

- All databases

- All user data (users, privileges and licenses)

- All ARIS document storage data including all access rights

- All Process Governance data

- All ad hoc analyses and queries

Extensions, for example, SSL certificates (page 12), SAP® Java Connector, and JDBC drivers (page 39), added using the **enhance** ACC command are not backed up.

Prerequisites

- You need access to the relevant back-up zip file

- ARIS Server installation

- Users need the following function privileges. The function privileges depend on the license. Therefore, you may not be able to assign all of the function privileges shown.

  - Analysis administrator

  - ARCM administrator

  - Collaboration administrator

  - Database administrator

  - Dashboard administrator

  - Document administrator

  - License administrator

  - Portal administrator

  - Process Governance administrator

  - Server administrator

  - Technical configuration administrator

  - User administrator

Procedure

1. Create a tenant (page 27) on the ARIS Server where the tenant will be copied to and import the licenses.

2. Start ARIS Cloud Controller (ACC) (page 3).

3. To restore Process Governance data, stop the Process Governance runnable first. To do so enter, for example: **stop apg_m**

4. Enter: **restore tenant <Tenant name> from <pathToBackUpFile> encryption.key <encryption password or encryption key> username=<user name of a user holding the required privileges> password=<this user's password>**

   or as an example for the us of an unencrypted **acb** file: **restore tenant default from "f:\\backupDefault.acb" username=y1234 password=managery1234**

   Notice the double backslashes. Alternatively, use a single forward slash. You must enter the user credentials of the server's ARIS Administration you have created the new tenant. If you are about to migrate data, you might use the standard name and password **system/manager**.

5. In case you restored Process Governance data, restart the Process Governance runnable. To do so enter, for example: **start apg_m**

All data of the backup file will be copied to the new tenant. Current data will be deleted except the name of the new tenant, as well as user credentials. The current user data will be untouched. If users were deleted after the tenant has been backed up, these users will be available again. Please make sure to delete those users.

In case of a migration process the default credentials will automatically be in use. To prevent unauthorized access to the ARIS system, after installation or data migration, always change the default passwords of the **arisservice** user, the **guest** user, the **system** user and the **superuser** user on all operational tenants, as well as on the infrastructure tenant (master).

You can also create tenants using the ARIS Administration's command line tools or Tenant Management.

2.5.16.7   Define backup folder

By default, backups are stored in the ARIS Server installation directory
(..\server\bin\work\work_umcadmin_<s, m, or l>**backup**). Define a different folder on a
physical drive in order to keep data update-proof. As the default **backup** folder is overwritten
by the update, all backups are lost.

Prerequisite

You have access to ARIS Cloud Controller (ACC)

Procedure

1. Start ARIS Cloud Controller (ACC) (page 3).

2. Enter, for example: **reconfigure umcadmin_m JAVA-Dtm.backup.folder =
    "C://backups"**

    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.

    Make sure to use a physical drive. Mapped drives cannot be accessed.

3. Exit ACC.

All backup files are saved in the **backups** subfolder on drive **C**.

2.5.16.8 How to adjust timestamps related to ARIS document storage

In previous ARIS versions, ARIS document storage stored timestamps, for example **Creation time** and **Update time**, referred to documents and folders in local server time and without any time zone information. If data was moved between ARIS Servers or if a tenant was restored from a backup file, timestamps were likely adjusted using a wrong time offset.

Since ARIS 10 SR6, **Coordinated Universal Time** (UTC) is mandatory for timestamps stored by ARIS document storage. Because time zone information in existing data is not available, the timestamps of existing documents and folders cannot be adjusted automatically. After the update to ARIS 10 SR6, you must manually adjust timestamps. In a Windows-based installation with local time UTC-2, for example, use the **y-admintool.bat** command-line tool and, considering UTC offset of your ARIS Servers>, enter the following:

y-admintool.bat -s https://localhost -t default adjustTimestamps –offset "-120" -u system -p manager

If you have restored a tenant from backup file created with ARIS 10 SR5 or earlier, you must adjust the timestamps as well.

2.5.17   Database connection

This chapter provides information on configuring ARIS Server in order to use an external database management system.

2.5.17.1   Provide JDBC drivers

During the setup procedures of ARIS Server or ARIS Publisher Server using Oracle or Microsoft SQL Server the JDBC driver is provided automatically. You can enhance JDBC drivers manually.

Procedure

1. Download the JDBC driver from the Microsoft or Oracle Web Sites to local directory that can be accessed by ARIS Cloud Controller (ACC).

    For example: **d:\ojdbc<number>.jar**.

2. Start ARIS Cloud Controller (ACC) (page 3).

3. Stop the server runnables. Enter: **stopall**.

4. Provide the JDBC driver using the **enhance** command. 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.

5. Example: **enhance abs_l with webappsClasspath local file "d:\\ojdbc<number>.jar"**

    The file has been made available. The source file can be deleted.

6. Start the server runnables. Enter: **startall**

The driver is available.

2.5.17.2   Update external service (database clusters)

If you have performed an installation using an Oracle or Microsoft SQL database cluster you need to reconfigure the external service after the installation process.

This procedure shows an example for an Oracle database.

Procedure

1. Start ARIS Cloud Controller (ACC).

    ARIS Cloud Controller can be used in multiple modes (page 3).

    To start ACC under a Windows operating system click **Start > All Programs > ARIS > Administration > Start ARIS Cloud Controller**. If you have changed agent user credentials you must enter the user name and/or the password.

    To start ACC under a Linux operating system, execute the **acc10.sh** shell script instead.

2. To connect to an Oracle cluster using a JDBC URL you may use this example:

    update external service <dbserviceID> url="jdbc:oracle:thin:@(DESCRIPTION=ADDRESS_LIST=(ADDRESS=(PROTOCOL =TCP) (HOST=<virtual-ip-oracle-cluster>)(PORT = <target port>)))(CONNECT_DATA=(SERVICE_NAME=cluster-database-name)))" driverClassName="oracle.jdbc.OracleDriver" username="<cip_app_user>" password="<new_cip_app_pwd>" maxIdle=15 maxActive=100 maxWait=10000 removeAbandoned=false removeAbandonedTimeout=600 logAbandoned=true defaultAutoCommit=false rollbackOnReturn=true host=<target_host> jmxEnabled=true validationQuery="select 1 from dual" testOnBorrow=true

ARIS Server can be started using the Oracle cluster.

2.5.17.3   Configure the database connection for additional schemes

ASSIGN TENANT TO DATABASE SCHEMA

During the setup process you have created an empty Oracle or Microsoft SQL schema for an additional tenant (see ARIS Server Installation Guide). Additionally created tenants must be assigned to the database schema.

1. Start ARIS Cloud Controller (ACC).

    ARIS Cloud Controller can be used in multiple modes (page 3).

    To start ACC under a Windows operating system click **Start > All Programs > ARIS > Administration > Start ARIS Cloud Controller**. If you have changed agent user credentials you must enter the user name and/or the password.

    To start ACC under a Linux operating system, execute the **acc10.sh** shell script instead.

2. To discover the database service ID (<dbserviceID>, such as db000000000), enter:

    list external services

    assign tenant <tenant name> to service <dbserviceID> com.aris.cip.db.schema =<schema name>

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

3. To create a new tenant, enter:

    create tenant <tenant name>

The new tenant is available on ARIS Server.

ADDITIONAL SETTINGS

To enable **validationQuery** for external DB connections (Oracle & Microsoft SQL) please use the correct validation query for the DBMS.

For Oracle use:

validationQuery="select 1 from dual" and testOnBorrow=true

For Microsoft SQL use:

validationQuery="select 1" and testOnBorrow=true

During registration of external service add parameters, for example, for Oracle:

register external service db
url="jdbc:oracle:thin:@<target_host>:<target_port>:<oracle_sid>"

driverClassName="oracle.jdbc.OracleDriver"

username="<cip_app_user>

password="<cip_app_pwd>"

maxIdle=15

maxActive=100

maxWait=10000

removeAbandoned=false

removeAbandonedTimeout=600

defaultAutoCommit=false

rollbackOnReturn=true

host=<target_host>

port=<target_port>

jmxEnabled=true

validationQuery="select 1 from dual"

testOnBorrow="true"

After the external service was already registered, for example, for Oracle:

update external service <dbserviceID>
url="jdbc:oracle:thin:@<target_host>:<target_port>:<oracle_sid>"

driverClassName="oracle.jdbc.OracleDriver"

username="<cip_app_user>"

password="<cip_app_pwd>"

maxIdle=15

maxActive=100

maxWait=10000

removeAbandoned=false

removeAbandonedTimeout=600

defaultAutoCommit=false

rollbackOnReturn=true

host=<target_host>

jmxEnabled=true

validationQuery="select 1 from dual"

testOnBorrow="true"

ENABLE VALIDATIONQUERY FOR EXTERNAL POSTGRESQL CONNECTION

1. Enter: **stopall**

2. Enter: **reconfigure <postgres_runnable> dbsp.validationQuery="select 1" dbsp.testOnBurrow=true**

3. Enter: **startall**

The database connection is configured.

2.5.17.4 Move the database management system

If you run ARIS using an external database management system and the operational database server has moved, you must update the settings, for example, the IP address and the server name.

Procedure

1. Start ARIS Cloud Controller (ACC) (page 3).

2. Stop all runnables, except the **zoo** runnable (service registry).

3. Determine the service ID of the external database service to be changed. Enter: **list external services**

4. Check the current settings of the external database settings. Enter: **show external service <service ID>**

   Example: **show external service db0000000000**

   Depending on the database system in use different settings are displayed.

   Output example (Oracle):

   Service db0000000000 (Type DB)

   Parameters:

   ...

   host sbrva100.com.ad.aaf

   ...

   url jdbc:oracle:thin:@//sbrva100.com.ad.aaf:1521/aris

   ...

   Output example (Microsoft SQL Server):

   Service db0000000000 (Type DB)

   Parameters:

   ...

   host sbrva100.com.ad.aaf

   ...

   url jdbc:sqlserver://sbrva100.com.ad.aaf;DatabaseName=aris10db;instanceName=aris

   ...

5. Change the required settings using the **update external service** command.

   Example (Oracle):

   update external service <service ID> url="jdbc:oracle:thin:@//<Oracle server>:<listener port>/<instance name>" host=<Oracle server>

   Example (Microsoft SQL Server):

   update external service <service ID> url="jdbc:sqlserver://<Microsoft SQL Server>:<listener port>;DatabaseName=<database name>;instanceName=<instance name>" host=<Microsoft SQL Server>

6. Check the applied database schema. Enter: **list tenant <name> data for service db**

   Output example (**default** tenant):

   ```
   Data of tenant default tenant for application db
   Key Value
   com.aris.cip.db.schema aris_default
   com.aris.ecp.db.schema aris_default
   name default
   ```

7. Change the schema settings for all tenants, if required. Enter:

   set tenant <tenant name> data for service db com.aris.cip.db.schema=<new schema name>

   Example (**master** tenant):

   set tenant master data for service db com.aris.cip.db.schema=aris10_master (com.aris.ecp.db.schema not needed)

   Example (**default** tenant):

   set tenant default data for service db com.aris.cip.db.schema=aris10_default com.aris.ecp.db.schema=aris10_default

8. Check the new settings using the commands:

   show external service <service ID>

   list tenant <tenant name> data for service db

9. Start all runnables. Enter: **startall**

2.5.18   Elasticsearch authentication

The Document index (Elasticsearch) is a basic component that contains the full-text search index for documents and collaboration data. It also stores users, user groups, licenses, and privileges. By default, the **elastic_<s**, **m**, or **l>** runnable (Elasticsearch) uses generic user credentials required for communication with other ARIS runnables.

2.5.18.1   Check user name and password (Elasticsearch)

By default, the **elastic_<s**, **m**, or **l>** runnable (Elasticsearch) uses generic user credentials required for communication with other ARIS runnables. You can check the user name and password in use.

Procedure

1. Navigate to **<ARIS installation path>\server\bin\work\work_elastic_m**, for example, **C:\ARIS10.0\server\bin\work\work_elastic_m**.
2. Open the **instanceId.elasticsearch** file with a text editor.
3. Copy the instance ID, for example:

    elasticsearch0000000000
4. Start ARIS Cloud Controller (ACC).

    ARIS Cloud Controller can be used in multiple modes (page 3).

    To start ACC under a Windows operating system click **Start > All Programs > ARIS > Administration > Start ARIS Cloud Controller**. If you have changed agent user credentials you must enter the user name and/or the password.

    To start ACC under a Linux operating system, execute the **acc10.sh** shell script instead.
5. Once ACC is initialized, enter **show service elastisearch<ID>**, for example:

    show service elasticsearch0000000000

User name and password are displayed.


```
ACC+ localhost>show service elasticsearch0000000000
Service elasticsearch0000000000 (Type ELASTICSEARCH)
Parameters:
Key        Value
ajpPort    8009
context    /
host       daetstdocu02.eur.ad.sag
password   ngCIolG6rcysQksQwWlhnsgpVmLQubei
port       14220
scheme     http
username   aris
```

You can change (page 47) the user name and the password if required.

2.5.18.2   Change user name and password (Elasticsearch)

By default, the **elastic_<s**, **m**, or **l>** runnable (Elasticsearch) uses generic user credentials required for communication with other ARIS runnables. You can check (page 46) and change the user name and the password if required.

Procedure

1. Start ARIS Cloud Controller (ACC).

    ARIS Cloud Controller can be used in multiple modes (page 3).

    To start ACC under a Windows operating system click **Start > All Programs > ARIS > Administration > Start ARIS Cloud Controller**. If you have changed agent user credentials you must enter the user name and/or the password.

    To start ACC under a Linux operating system, execute the **acc10.sh** shell script instead.

2. Once ACC is initialized, enter:

    reconfigure elastic_<s, **m**, or **l> +ELASTICSEARCH.aris.api.user.name="<new user name" +ELASTICSEARCH.aris.api.user.password="<new password>**"

    for example:

    reconfigure elastic_m +ELASTICSEARCH.aris.api.user.name="administrator" +ELASTICSEARCH.aris.api.user.password="Thssmynwpsswrd"

3. Stop the Collaboration runnable **ecp_<s**, **m**, or **l>**. Enter, for example:

    stop ecp_m

4. Restart the Collaboration runnable. Enter, for example:

5. **start ecp_m**

You have changed the user credentials required for the Elasticsearch.

2.5.18.3   Disable authentication for Elasticsearch

You can switch off the authentication for the Elasticsearch.

Warning
Disabling authentication is not recommended and must be considered carefully. It bears a potentially risk to data security.

Procedure

1. Start ARIS Cloud Controller (ACC).

   ARIS Cloud Controller can be used in multiple modes (page 3).

   To start ACC under a Windows operating system click **Start > All Programs > ARIS > Administration > Start ARIS Cloud Controller**. If you have changed agent user credentials you must enter the user name and/or the password.

   To start ACC under a Linux operating system, execute the **acc10.sh** shell script instead.

2. Once ACC is initialized, enter: **reconfigure elastic_<s**, **m**, or **l> +ELASTICSEARCH.aris.api.deactivate.authentication="true"**

   for example: **reconfigure elastic_m +ELASTICSEARCH.aris.api.deactivate.authentication="true"**

You have disabled the authentication for the Elasticsearch.

2.5.19   Health check

You can monitor the health of a specific runnable as well as the health of the whole system.

2.5.19.1   Show node

The **show node** command shows machine monitoring information concerning CPU, memory and disk usage. If a threshold is violated, it will be shown.

Prerequisite

Health monitoring parameters are set (page 51).

Procedure

1. Start ARIS Cloud Controller (ACC) (page 3).

2. Make sure that the runnables have been started.

3. Enter: **show node**

The output will be in tabular format and look like this example:

```
ACC+ localhost>show node
Node localhost
Status: OK
Specified IP or host name: localhost
Resolved IP or host name: localhost/127.0.0.1
Agent port: 14000


Monitored Resource         Current Value  Value Range    Low Thrh.  High Thrh.  State  Last msrd. at  Msrd. evry
CPU Load                   0,19%          0.00%-100.00%  -          80.00%      OK     08:24:02.227   1s 000ms
Memory Usage (Percent)     58,68%         0.00%-100.00%  -          80.00%      OK     08:24:02.227   1s 000ms
Memory Usage (Megabytes)   38401MB        0MB-65442MB    -          -           OK     08:24:02.227   1s 000ms
Free Disk Space (Percent)  92,70%         0.00%-100.00%  3.00%      -           OK     08:24:02.228   1s 000ms
Free Disk Space (Megabytes) 616161MB      0MB-664685MB   1000MB     -           OK     08:24:02.228   1s 000ms

Known used ports:
  Port(s)  Runnable       Port Parameter
  443      loadbalancer_m HTTPD.ssl.port                           Set explicitly
  ''       'ance~ m HT~'    ~~                                     Set  ~~' 'tly
```

2.5.19.2   Monitor runnable's health

The **health** command determines a variety of health values for each runnable.

The exact list of health values available depends on the specific runnable. However, a few basic measurements are available to all runnables, in particular the CPU load and its memory usage. For all Java-based runnables, additional information is available.

Prerequisite

Health monitoring parameters are set (page 51).

Procedure

1. Start ARIS Cloud Controller (ACC) (page 3).

2. Make sure that the runnable has been started.

3. Enter, for example: **show instance zoo_m health**

The output will look like this example:

```
Status: OK
Specified IP or host name: arissrv
Resolved IP or host name: arissrv/127.0.0.1
Agent port: 9001
Monitored Resource          Current Value  Value Range    Low Thrh.  High Thrh.  State  Last msrd. at  Msrd. evry
CPU Load                    11,36%         0,00%-100,00%  0,00%      80,00%      OK     08:05:39.844   1s 000ms
Memory Usage (Percent)      36,81%         0,00%-100,00%  0,00%      80,00%      OK     08:05:39.844   1s 000ms
Memory Usage (Megabytes)    2980MB         0MB-8097MB     0MB        0MB         OK     08:05:39.844   1s 000ms
Free Disk Space (Percent)   63,40%         0,00%-100,00%  3,00%      0,00%       OK     08:05:39.845   1s 000ms
Free Disk Space (Megabytes) 302361MB       0MB-476938MB   1000MB     0MB         OK     08:05:39.846   1s 000ms
Known used ports:
   Port  Runnable  Port Parameter
   2181  zoo_m     clientPort
   9001  (AGENT)   rest.port       DEFAULT
ACC+ arissrv>
```

The first column shows the name of the measured value and its physical unit, for example, megabytes, percent, etc.

The second column shows the current value of the health value. Note that this is not measured the moment the command is executed. The agent plugin will take measurements periodically, and this column will show the result of the last measurement.

The third column shows the range of possible values, for example, minimum and maximum value. If no minimum or maximum value can be determined or the value does not have an ordinal value scale a **-** is shown instead.

The fourth and fifth columns show the minimum and maximum values, respectively. These values were observed since the runnable or the ARIS Agent had last been restarted, but only if the health value measured has an ordinal value scale. For values measured without an ordinal value scale, - will be shown.

The sixth column shows the low or high warning thresholds for the measured value, if the measured health value has an ordinal value scale and if thresholds have been configured.

The seventh column shows the state of the measured value if the measured health value has an ordinal value scale and if a low and/or high threshold has been configured. The state can be either **OK**, **LOW** or **HIGH**. If in **LOW** or **HIGH** state, the column will also show for how long the value has been in that state already.

2.5.19.3   Configure health monitoring

If you use the health monitoring, using ACC, make sure to configure the system.

Procedure

1. Start ARIS Cloud Controller (ACC) (page 3).

2. Enter the parameters described below.

THRESHOLDS

Thresholds for monitored values can be configured using agent configuration parameters:

Parameter	Description
monitoring.high.cpu.threshold.percent (0.0 – 1.0, default 0.8)	High CPU usage threshold (relative, in percent)
monitoring.relative.low.disk.space.warning.threshold.percent (0.0 – 1.0, default 0.03)	Low memory threshold (relative, in percent)
monitoring.absolute.low.disk.space.warning.threshold.megabytes (default 1000)	Low disk space threshold (absolute, in megabytes) **Warning** ARIS Agent not only warns against insufficient disk space. When the default value (1000 MB) is reached, all runnables are immediately shut down (killall) to avoid data inconsistencies. Runnables cannot be restarted. ARIS Agent autostart is disabled.

THRESHOLD MEASUREMENT

The measurement can be configured by the following parameters:

Parameter	Description
monitoring.interval (default 1000)	Interval in milliseconds, in which the measurement will be done.
monitoring.high.cpu.number.of.intervals. warning.threshold (default 10)	Number of measurements with CPU load above threshold before a warning state is reached
monitoring.high.mem.usage.number.of.in tervals.warning.threshold (default 10)	Number of measurements with memory usage above threshold before a warning state is reached.
monitoring.low.disk.space.number.of.int ervals.warning.threshold (default 10)	Number of measurements with free disk space below threshold before a warning state is reached.

MAIL NOTIFICATION

Mail notification can be configured by the following parameters:

Parameter	Description
mail.notification.enable d (default: **false**)	**true** enables automatic mailing.
mail.smtp.host	Qualified hostname or IP of the mail server.
mail.smtp.port (common: **25**)	Port of the mail server.
mail.smtp.username	User name on the mail server. If this parameter is set, the applications will implicitly enable SMTP authentication. There is **NO** dedicated parameter to explicitly enable SMTP authentication.
mail.smtp.password	Mail server password for the specified user.
mail.sender.address	Sender's e-mail address.
mail.sender.name	Sender's name.
mail.recipients	Recipient's e-mail address. This parameter is multivalued, specify several recipients separated with commas, for example: **set mail.recipients = "a@abc.com","b@abc.com"**

Parameter	Description
mail.recipients.cc	Recipient's e-mail address (**C**arbon **C**opy(CC)). This parameter is multivalued (see **mail.recipients**)
mail.on.system.events	Defining events triggering e-mail notification. This parameter is multivalued, specify several event types separated by comma, for example: **set mail.on.system.events = MACHINE_STATE_CPU_LOAD_HIGH, MACHINE_STATE_** Possible values: ▪ MACHINE_STATE_LOW_DISK_SPACE_PERCENT ▪ MACHINE_STATE_OK_DISK_SPACE_PERCENT ▪ MACHINE_STATE_LOW_DISK_SPACE ▪ MACHINE_STATE_OK_DISK_SPACE ▪ MACHINE_STATE_CPU_LOAD_HIGH ▪ MACHINE_STATE_CPU_LOAD_OK ▪ MACHINE_STATE_MEMORY_USAGE_HIGH ▪ MACHINE_STATE_MEMORY_USAGE_OK

2.5.20   Mailing

This chapter provides information on configuring automatic mailing.

2.5.20.1   Configure ARIS Agent mail server connection

If only ARIS Agent is installed but no ARIS server you can activate automatic mailing in order to receive technical information from ARIS Agent. This will inform administrators, for example, about performance problems concerning ARIS Agent.

1. Start ARIS Cloud Controller (ACC) (page 3) on the machine where ARIS Agent is installed.
2. Enter the following lines one after the other.

    Example:

    set mail.notification.enabled=true

    set mail.smtp.host=mailserver.us

    set mail.smtp.port=25

    set mail.smtp.username=<user name>

    set mail.smtp.password=<password>

    set mail.recipients=aris.administrator1@company.com

    set mail.recipients.cc=aris.administrator2@company.com

    set mail.sender.address=<COMPUTERNAME>@us.co

ARIS Agent mail server connection is set.

Mail notification can be configured by the following parameters:

Parameter	Description
mail.notification.enable d (default: **false**)	**true** enables automatic mailing.
mail.smtp.host	Qualified hostname or IP of the mail server.
mail.smtp.port (common: **25**)	Port of the mail server.
mail.smtp.username	User name on the mail server. If this parameter is set, the applications will implicitly enable SMTP authentication. There is **NO** dedicated parameter to explicitly enable SMTP authentication.
mail.smtp.password	Mail server password for the specified user.
mail.sender.address	Sender's e-mail address.
mail.sender.name	Sender's name.

Parameter	Description
mail.recipients	Recipient's e-mail address. This parameter is multivalued, specify several recipients separated with commas, for example: **set mail.recipients = "a@abc.com","b@abc.com"**
mail.recipients.cc	Recipient's e-mail address (**C**arbon **C**opy(CC)). This parameter is multivalued (see **mail.recipients**)
mail.on.system.events	Defining events triggering e-mail notification. This parameter is multivalued, specify several event types separated by comma, for example: **set mail.on.system.events = MACHINE_STATE_CPU_LOAD_HIGH, MACHINE_STATE_** Possible values: ▪ MACHINE_STATE_LOW_DISK_SPACE_PERCENT ▪ MACHINE_STATE_OK_DISK_SPACE_PERCENT ▪ MACHINE_STATE_LOW_DISK_SPACE ▪ MACHINE_STATE_OK_DISK_SPACE ▪ MACHINE_STATE_CPU_LOAD_HIGH ▪ MACHINE_STATE_CPU_LOAD_OK ▪ MACHINE_STATE_MEMORY_USAGE_HIGH ▪ MACHINE_STATE_MEMORY_USAGE_OK
mail.on.state.change (default: **FAILED**)	Defining events triggering e-mail notification if a runnable is in the state **FAILED**.
mail.on.runnable.monit oring.events	Defining events triggering e-mail notification. This parameter is multivalued (see **mail.on.system.events**). Possible values: ▪ RUNNABLE_MONITORING_HIGH_THRESHOLD_EXCEEDED ▪ RUNNABLE_MONITORING_LOW_THRESHOLD_EXCEEDED

2.5.20.2   Configure SMTP mail server connection

If you did not enter the SMTP server connection parameters during the setup process of a previous ARIS version you need to register your SMTP server manually.

1. Start ARIS Cloud Controller (ACC).

    ARIS Cloud Controller can be used in multiple modes (page 3).

    To start ACC under a Windows operating system click **Start > All Programs > ARIS > Administration > Start ARIS Cloud Controller**. If you have changed agent user credentials you must enter the user name and/or the password.

    To start ACC under a Linux operating system, execute the **acc10.sh** shell script instead.

2. Enter, for example:

    register external service smtp host="YourMailServerAddressWithDomain" port=25

3. Check that setting entering:

    list external services

SMTP mail server configuration is set.

You can modify SMTP configuration parameters using the **update external service** command.

Parameter	Type	Default value	Description
Host host	String		Qualified hostname or IP of the SMTP server.
Port port	Integer	25	Port of the SMTP server.
User name username	String		User name on the SMTP server. If this parameter is set, the applications will implicitly enable SMTP authentication. There is **NO** dedicated parameter to explicitly enable SMTP authentication.
Password password	String		Password for the user on the SMTP server.
Sender address sender.address	String		Sender's e-mail address.
TLS use.tls	Boolean	false	Specifies if SMTP server is TLS enabled.

Parameter	Type	Default value	Description
TLS mode tls.mode	String	STARTTLS	Specifies the method used to secure the connection. Accepted values are **STARTTLS** and **SSL**. STARTTLS upgrades an initially insecure connection to an encrypted one without requiring a dedicated port for secure communication, whereas SSL immediately establishes a secured connection on a dedicated port.

2.5.21 Third-party document management systems (TDMS)

This chapter provides information on configuring ARIS Server to use an external TDMS.

2.5.21.1 Make TDMS available

If you want to use third-party document management systems, you must enhance the ARIS document storage runnable with a custom jar file. The system available is Microsoft® SharePoint 2013. Please contact your local Software AG sales organization (http://www.softwareag.com) for other third-party document management systems.

Procedure

1. Save the custom jar file for the third-party document management system.
2. Start ARIS Cloud Controller (ACC) (page 3).
3. Stop the ARIS document storage runnable. Enter, for example: **stop adsadmin_m**
4. Provide the custom jar file for the third-party document management system using the **enhance** command. 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.

    Example: **enhance adsadmin_m with webappsClasspath local file "d:\\dms-adapter.jar"**

    The file has been made available. The source file can be deleted.
5. Start the ARIS document storage runnable. Enter: **start adsadmin_m**

The third-party document management system is available.

You must configure the settings for the TDMS in ARIS Administration, refer to chapter **Manage ARIS Connect > Configure ARIS Connect > Set up Document storage > Add third-party document management system** of the ARIS Connect online help.

3 Legal information

3.1 Documentation scope

The information provided describes the settings and features as they were at the time of publishing. Since documentation and software are subject to different production cycles, the description of settings and features may differ from actual settings and features. Information about discrepancies is provided in the Release Notes that accompany the product. Please read the Release Notes and take the information into account when installing, setting up, and using the product.

If you want to install technical and/or business system functions without using the consulting services provided by Software AG, you require extensive knowledge of the system to be installed, its intended purpose, the target systems, and their various dependencies. Due to the number of platforms and interdependent hardware and software configurations, we can describe only specific installations. It is not possible to document all settings and dependencies.

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, contact your local Software AG sales organization. Please note that this type of manufacturer-specific or customer-specific customization is not covered by the standard Software AG software maintenance agreement and can be performed only on special request and agreement.

If a description refers to a specific ARIS product, the product is named. If this is not the case, names for ARIS products are used as follows:

Name	Includes
ARIS products	Refers to all products to which the license regulations of Software AG standard software apply.
ARIS Client	Refers to all programs that access shared databases by using ARIS Server.
ARIS Download Client	Refers to an ARIS Client that can be accessed using a browser.

3.2 Data protection

Software AG products provide functionality with respect to processing of personal data according to the EU General Data Protection Regulation (GDPR).

Where applicable, appropriate steps are documented in the respective administration documentation.

3.3 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 your product contains ARIS document storage, the following applies:

ARIS document storage was tested with 40.000 document items. This includes documents, document versions or folders. We recommend monitoring the number and overall size of stored document items and archiving some document items if needed.

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 regarding the use of process administration, ARIS Administration, ARIS document storage, and ARIS Process Board, and the generation of 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 document items. This includes documents, document versions or folders. We recommend monitoring the number and overall size of stored document items and archiving some document items if needed.