

ARIS PATCH SETUP

VERSION 10.0 - SERVICE RELEASE 27 AND HIGHER
OCTOBER 2024

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

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

Copyright © 2010-2024 Software GmbH, Darmstadt, Germany and/or its subsidiaries and/or its affiliates and/or their licensors.

The name Software AG and all Software GmbH product names are either trademarks or registered trademarks of Software GmbH and/or its subsidiaries and/or its affiliates and/or their licensors. Other company and product names mentioned herein may be trademarks of their respective owners.

Detailed information on trademarks and patents owned by Software GmbH and/or its subsidiaries is located at <https://softwareag.com/licenses>.

This software may include portions of third-party products. For third-party copyright notices, license terms, additional rights or restrictions, please refer to "License Texts, Copyright Notices and Disclaimers of Third Party Products". For certain specific third-party license restrictions, please refer to section E of the Legal Notices available under "License Terms and Conditions for Use of Software GmbH Products / Copyright and Trademark Notices of Software GmbH Products". These documents are part of the product documentation, located at <https://softwareag.com/licenses> and/or in the root installation directory of the licensed product(s).

Use, reproduction, transfer, publication or disclosure is prohibited except as specifically provided for in your License Agreement with Software GmbH.

Contents

Contents.....	1
1 General information	1
2 Scope of a patch setup	2
3 Quick start	3
4 How does the patch setup work?	4
4.1 What causes the patch setup to fail?	4
4.2 What happens if a patch setup fails?	6
5 How to prevent the setup to fail	7
5.1 Check all files	7
5.2 Set write attribute to all files.....	8
5.3 Make files accessible that are used by other processes.....	8
6 General prerequisites to be met.....	9
7 Run the patch setup	10
7.1 Windows	10
7.2 Linux	12
8 Check the patched installation.....	13
9 Execute the updatesystemdb ARIS Cloud Controller command	14
10 Troubleshooting	16
10.1 Manually restore installation for a second patch execution.....	16
10.2 Restore a patched ARIS installation	18
10.3 Product not found	19
10.4 Logging	20
11 Legal information.....	21
11.1 Documentation scope.....	21
11.2 Support	22

1 General information

This document describes how to use the ARIS patch setup. If you are an expert user and you do not need detailed information, refer to the **quick start** chapter (page 3).

An ARIS patch setup patches an existing ARIS server installation to a higher build number of the same ARIS version. A patch setup with a certain build number contains all bug fixes of previous patch setups with lower build numbers of the same version. This means that you do not need to execute older patch setups. The one with the highest build number does the job. A patch setup with a higher build number can only patch ARIS versions that have lower build numbers. You cannot patch to a lower version.

The patch setup uses the standard update mechanism to apply patches. Patch setups do not perform a full version update that includes new features and documentation. It only fixes bugs reported in versions with a lower build number. To update your installation, run the ARIS server setup program as an administrator.

Please note that the following setup files are examples and that the version and build numbers may differ from those of your patch setup.

Syntax: **ARIS_Patch_Setup_V<major version>.<minor version>.<bugfix version>.<Build number>.exe**

Example: **ARIS_Patch_Setup_V10.0.27.0.exe**

If you want to patch a customized ARIS Risk and Compliance installation, read the **ARIS Risk and Compliance - Data Migration Guide for Customized Versions**.

Also refer to the **ARIS Update Cookbook**.

Documents are available in the ARIS installation package (see **Documents > English** folder structure). Documents can also be installed locally (see Technical Help: **ARIS client Installation Guide**). Documentation is also contained in the ARIS installation package that is available in the ARIS Download Center (<https://ariscommunity.com/download-center/product-groups>).

Warning

We recommend applying the patch to a test environment before you patch your productive ARIS system.

2 Scope of a patch setup

Patch setups are intended to provide quick code hotfixes for ARIS server installations that do not work properly. Global Support ARIS will let you know if the patch setup completely solves your reported problem or if you need to take additional action. Patch setups collect fixes starting from the first ARIS GA version (General Availability), such as **ARIS 10**, to the current state of the patches. This means the patch will not only solve a specific customer issue, but will provide the most current set of fixes available for an ARIS version.

Patch setups do not perform a full version update that includes new features and documentation. It only fixes bugs reported in versions with a lower build number. To update your installation, run the ARIS server setup program as an administrator.

You can use patch setups for:

- ARIS server single node installations that were installed by the setup program.
- ARIS server multi node installations that were installed manually. In this case, the patch setup must be executed for each node after the runnables were stopped. Currently you cannot run a "rolling update". This means that all runnables of one node are stopped for the patch while the other nodes keep running.

You cannot use patch setups for:

- ARIS single user installations using the **LOCAL** database system. From ARIS 10.0.16.0 on the **LOCAL** database system is no longer delivered.
- an installed ARIS client. To update an installed ARIS client, use the most current ARIS client setup program instead.
- an ARIS agent environment. To update an ARIS agent, use the most current ARIS agent setup program instead.
- updating content that is provided in the ARIS system database. The patch setup does not automatically update the system database. The most current system database is hidden in a **jar** file contained in the patch setup but the database is not automatically updated. If you want to update the content of your system database because related content was fixed as well, you must execute the **updatesystemdb** ARIS Cloud Controller command (page 14) after you ran the patch setup for each tenant.

3 Quick start

You must run the patch setup on the machine where ARIS server is installed. For a distributed ARIS server environment, you must run the patch setup for each node.

Make sure that no file in the installation directory is opened or in use by another process (page 7). Locked files will cause issues (page 4) while the patch setup is running. Refer to the general prerequisites. To receive detailed diagnostic information, execute the **check file system permissions** ARIS Cloud Controller command.

You do not need to activate deactivated runnables before patching the installation. Deactivated runnables are automatically patched and remain deactivated.

You are recommended to save all log files before executing the patch setup. To do so, execute the **collect log files** ARIS Cloud Controller command, save the archive file, and execute the **delete log files** ARIS Cloud Controller command. This will speed up the patch process and ensures that only the latest log files are available.

Note

The progress bar will remain at the 46% mark for some time due to extensive backup processes. This is not an error. Do not abort the patch process under any circumstances. An abort can lead to a system failure and data loss.

WINDOWS

1. Stop all runnables (**Windows Start menu > ARIS > Administration > Stop ARIS Server** or **stopall** ARIS Cloud Controller command).
2. Execute the **<a> Patch Setup**, such as **ARIS_Patch_Setup_V10.0.27.0.exe**.
3. In the user interface, click **Start** to execute the patch process.
4. If the patch setup was completed successfully, a message is displayed or a Web browser window opens that shows diagnostic information. If you have activated a pop-up blocker, this information cannot be displayed.
5. Adapt your modified files if required according to your installation protocol.
6. Check the patched installation (page 13).

LINUX

1. Copy the **aris10-patchsetup-10.0.27.0-1.x86_64.rpm** file to the Linux system. This is a standard rpm package that you can install using rpm tools with **sudo** permissions. Actually, you do not have to stop the runnables to run the patch setup. If you patch a distributed installation, we recommend stopping all runnables.
2. Execute the command: **sudo rpm -i aris10-patchsetup-10.0.27.0-1.x86_64.rpm**
If the patch setup was completed successfully, diagnostic information is displayed.

4 How does the patch setup work?

The patch setup executes the **updateall** ARIS Cloud Controller command. This command deletes specific files from the **<ARIS server installation directory>\bin\work** directory and adds new content.

Before files are deleted from the **work** directory, all runnables are backed up automatically. This allows a rollback to the current state in the unlikely event that a patch failure occurs. The backup files are saved in the **<ARIS server installation directory>\bin\backup** directory. To list these backups, execute the **list runnable backups** ARIS Cloud Controller command.

If the **updateall** ARIS Cloud Controller command detects an error when deleting or writing files, the **restore runnable** ARIS Cloud Controller command is automatically triggered to reset all changes to the previous state. If this automatic mechanism fails because prerequisites (page 9) are not met, you must manually restore your installation.

The patch setup moves the help files and documents before patching. When the patch setup is completed, these files are put back in place. For this reason, the patch setup must be run on each physical machine that has a corresponding ARIS node installed.

4.1 What causes the patch setup to fail?

If a patch setup cannot be completed successfully because prerequisites (page 9) were not met, messages are logged as shown in the following examples:

```
2020-11 14:38:51,067|INFO |ACC execAsync thread
UpdateAllCommand{checkOnly=false, requestedNewVersion='null',
sizing='null'} AbstractRunnableManagementCommand{nodeName='node'}|
com.aris.prov.patch.Acc - Unexpected error trying to update runnable abs_1
on node node. Error [ message="Could not update runnable abs_1 on node node
to version 10.0.12.<build number>."
Update failed. A rollback was not possible. Reason: Ant updateNewVersion
exited with 1. Error during restore:
F:\ARIS\server\bin\.\work\work_abs_1\base\webapps\abs\static\dev-apps\app
logs: The process cannot access the file because it is being used by another
process.
.", error code= UPDATE_ERROR]"
...
Unexpected error trying to update runnable abs_1 on node n1. Error [
message="Could not update runnable abs_1 on node n1 to version 10.0.12
Update failed. A rollback was not possible. Reason: Ant updateNewVersion exited
with 1. Error during restore:
u:\ARIS10.0\server\bin\.\work\work_abs_1\tools\arisadm\log\arisadm.log:
The process cannot access the file because it is being used by another process.
.", error code= UPDATE_ERROR]"
Updateall aborted."
```

There are two main reasons that can cause the patch setup to fail.

INSUFFICIENT AUTHORIZATION GRANTED

The user account running the **ARIS agent 10.0** Windows service must have the permission to delete and write files. This is the **system** user on **Windows** operating systems and the **ARIS10 user** on **Linux** operating systems. In case of insufficient permissions, the patch setup fails because files as listed as an example cannot be updated.

- 3rd party customizing files copied from an outside source into the ARIS installation directory, such as
/home/ARIS10/cloudagent/./work/work_copernicus_m/base/webapps/ROOT/WEB-INF/config/classicSAP/instances/action/**action_default.xml**.
- SSL certificate files copied into **loadbalancer** or **download client** ARIS installation directory.
- Text files edited by Linux **root** user inside the ARIS directory.

LOCKED FILES

Configuration files that were set to **read only** and writable files that are in use by other processes are locked and therefore cannot be deleted by the patch setup.

- Many runnables contain internal tools, such as the **abs** runnable that contains the **ARIS Administration** or the **umcadmin** runnable containing the **Y-ldapsync.bat** command-line tool. If such tools are running and you forgot to close them before launching the patch, the patch will fail.
- Log files that are opened in a text editor.
- ARIS Java tasks that did not stop properly and remain in the **Not responding** state.

4.2 What happens if a patch setup fails?

If a patch setup failed due to the mentioned reasons (page 4), the last operating version of the installation cannot be recovered automatically because runnables now are in an inconsistent state.

This is the reason of this situation:

- The ARIS agent backed up and updated one runnable after another. Therefore, the ARIS agent deleted the old content from the runnable working directory.
- If the ARIS agent user lacks the permission to delete files or files are locked by any reason, an error occurs.
- Because files were deleted before this error occurred while other files from the earlier version are still available, the currently processed runnable is now in an inconsistent state.
- The ARIS agent now tries to roll back the changes executing the **restore runnable backup** ARIS Cloud Controller command. But this process cannot be completed successfully because the reason that caused the error is still in place.

Warning

The patch setup cannot solve this situation because the runnable least processed is still in an inconsistent state.

You must restore your ARIS installation (page 16) and run the patch setup again.

Do not start the patch setup before the runnables are restored because the setup will fail again. Since the maximum number of backups created by a patch setup is three, you risk data loss after unsuccessfully patching your installation three times.

5 How to prevent the setup to fail

If the prerequisites are not met and files are not writable (page 7), the setup fails because files cannot be updated (page 4). In this case, your installation cannot be automatically restored and ARIS may no longer run. To restore your installation, you must take further action.

It is a good idea to check whether all files stored in the ARIS server installation directory are not locked by other users or processes. You can also force all files to be writable. The user account running the **ARIS agent 10.0** Windows service must have the permission to delete and write files. This is the **system** user on **Windows** operating systems and the **ARIS10 user** on **Linux** operating systems.

5.1 Check all files

If you currently use ARIS 10.0.6 or a later ARIS version, the **check file system permissions** ARIS Cloud Controller command is executed automatically when you run the setup. This command checks whether all files in the ARIS server installation work directory can be deleted. This check takes quite a while if executed on a running ARIS system. As a result, the first 10 detected files causing a problem are listed. If more files were found not to be writable, they are listed in the **agent.log** file.

You can manually execute this command before you start the setup to discover possible problems. If you do so while all runnables are started, this check will take a long time and a lot of wrong warnings are reported. This is because some files are regularly locked when ARIS is running, such as files related to the **elastic** runnable.

To reduce runtime and the number of warnings, you are recommended stopping all runnables before you execute the **check file system permissions** ARIS Cloud Controller command.

This is an example for the **check file system permissions** ARIS Cloud Controller command that was executed on a distributed ARIS server installation containing three nodes.

```
Node n1: Permission problems found in one runnable:
Permission problems found for runnable adsadmin_1:
    Found 1 file that is missing the permission WRITE:
    U:\ARIS10.0\server\bin\work\work_adsadmin_1\tools\bin\Documents.zi
p
```

```
Node n2: No permission problems found.
Node n3: No permission problems found.
```

```
Problems were found on node n1 regarding the file permissions of the runnable
adsadmin_1.
Command failed with exit code 100.
Elapsed Time : 0h 54min
```

5.2 Set write attribute to all files

To force all files to be writable, execute the following commands.

In **Windows** operating systems, this command sets the **write** attribute to all files:

```
attrib -r <Installation Directory>\bin\work\*.* /s
```

In **Linux** operating systems, the following commands are executed by the RPM package. The commands allow the **aris10** user accessing all files:

```
ARIS Version >= 10.2
. /etc/aris10.conf
cd $TARGETDIR
chown -R aris10 *
```

```
ARIS Version < 10.2
cd /home/ARIS10
chown -R aris10 *
```

5.3 Make files accessible that are used by other processes

Even if files are readable, they can be blocked when accessed by other processes. To release all locks make sure to:

- Close all ARIS command-line tools, such as **ARIS Cloud Controller**, **ARIS server Administrator**, **ARIS document storage Command-Line Tool**, or **Process Governance Command-Line Tool**.
- Close all command prompt boxes that you use to start command-line tools, such as **y-datadump.bat**, **y-elasticsearch.bat**, **y-ldapsync.bat**, **y-password.bat**, or **y-tenantmgmt.bat**. Use the task manager or the process explorer to identify processes accessing the files.
- Sign off all other users to release all possible file locks.
- Reboot the machine to assure that no user has access to any file.

6 General prerequisites to be met

Before running the patch, you must assure that the following prerequisites are met:

- You have backed up all data using tenant backup.
- You are recommended to save all log files before executing the patch setup. To do so, execute the **collect log files** ARIS Cloud Controller command, save the archive file, and execute the **delete log files** ARIS Cloud Controller command. This will speed up the patch process and ensures that only the latest log files are available.
- Check your installation protocol. This protocol was written during the installation process and contains all information about modifications made after the installation was completed. Make sure to save all configuration files that were modified regarding to the installation protocol. Modified files are overwritten during the patch setup process and all modifications are lost. Therefore, after the patch is completed, you must modify the patched configuration files regarding to your installation protocol.

Example for modified files

- `<installDir>\server\bin\work\work_abs_<sizing>\base\webapps\abs\downloadClient\config\arisloader.cfg`
- `<installDir>\server\bin\work\work_abs_<sizing>\base\webapps\abs\config\defaultServerSettings.cfg`
- If you use a Windows operating system, you need the password of the ARIS agent user.
- Sufficient free disk space must be available. Depending on the amount of data stored in the runnable directories, up to 100 GB free disk space might be necessary.
- Files are writable.

Make sure that no file in the installation directory is opened or in use by another process (page 7). Locked files will cause issues (page 4) while the patch setup is running. Use the task manager or the process explorer to identify processes that may access related files, such as **notepad** or **notepad++**.

- Close all ARIS command-line tools, such as **ARIS Cloud Controller**, **ARIS server Administrator**, **ARIS document storage Command-Line Tool**, or **Process Governance Command-Line Tool**.
- Close all command prompt boxes that you use to start command-line tools, such as **y-datadump.bat**, **y-elasticsearch.bat**, **y-ldapsync.bat**, **y-password.bat**, or **y-tenantmgmt.bat**.
- Sign off all other users to release all possible file locks.
- The user account running the **ARIS agent 10.0** Windows service must have the permission to delete and write files. This is the **system** user on **Windows** operating systems and the **ARIS10 user** on **Linux** operating systems.

7 Run the patch setup

You must run the patch setup on the machine where ARIS server is installed. For a distributed ARIS server environment, you must run the patch setup for each node.

7.1 Windows

Proceed this instruction for each node in your distributed ARIS installation. If ARIS server was installed by the setup program (single node installation), you must run the patch setup on the machine where ARIS server is installed.

1. Make sure that the prerequisites are met (page 9).

Warning

If the prerequisites are not met and files are not writable (page 7), the setup fails because files cannot be updated (page 4). In this case, your installation cannot be automatically restored and ARIS may no longer run. To restore your installation, you must take further action.

2. Copy the **ARIS_Patch_Setup_V10.0.27.0.exe** to the machines where a related ARIS node is installed.
3. Stop all ARIS runnables. You do not need to activate deactivated runnables before patching the installation. Deactivated runnables are automatically patched and remain deactivated.
4. Execute the **ARIS_Patch_Setup_V10.0.27.0.exe**. The user interface is displayed. If you do not want to use the graphical user interface, add the **-console** parameter. If you do so, you must use the command prompt to enter all input. The parameters **-silent -u "<ARIS agent user name if not default>" -pwd "<ARIS agent user password if not default>"** cause the patch setup to run in the background without any user interaction. To open the ARIS patch setup online help, use the **?** parameter.
5. Click **Start** to execute the patch process. If you changed the default ARIS agent credentials as recommended, you must enter the current ones. The patch setup starts and the progress bar shows the status of the process.

Note

The progress bar will remain at the 46% mark for some time due to extensive backup processes. This is not an error. Do not abort the patch process under any circumstances. An abort can lead to a system failure and data loss.

- If the patch setup was completed successfully, a message is displayed or a Web browser window opens that shows diagnostic information. If you have activated a pop-up blocker, this information cannot be displayed.
 - If the patch setup failed because prerequisites were not met (page 9), try to recover your ARIS installation (page 16) and run the patch setup again.
1. Adapt your modified files if required according to your installation protocol.
 2. Check the patched installation (page 13). To start all runnables, you can use the **startall** ARIS Cloud Controller command or the ARIS > Administration > **Start ARIS Connect Server** link in the Windows **Start** menu.

Your ARIS server installation is patched. All bugs mentioned in the related **Readme** document are fixed.

7.2 Linux

Proceed this instruction for each node in your distributed ARIS installation. If ARIS server was installed by the setup program (single node installation), you must run the patch setup on the machine where ARIS server is installed.

1. Make sure that the prerequisites are met (page 9).

Warning

If the prerequisites are not met and files are not writable (page 7), the setup fails because files cannot be updated (page 4). In this case, your installation cannot be automatically restored and ARIS may no longer run. To restore your installation, you must take further action.

2. Copy the **aris10-patchsetup-10.0.27.0-1.x86_64.rpm** file to the Linux system. This is a standard rpm package that you can install using rpm tools with **sudo** permissions. Actually, you do not have to stop the runnables to run the patch setup. If you patch a distributed installation, we recommend stopping all runnables.

3. Execute the command:

```
sudo rpm -i aris10-patchsetup-10.0.27.0-1.x86_64.rpm
```

Note

The progress bar will remain at the 46% mark for some time due to extensive backup processes. This is not an error. Do not abort the patch process under any circumstances. An abort can lead to a system failure and data loss.

- If the patch setup was completed successfully, diagnostic information is displayed.
 - If the patch setup failed because prerequisites were not met (page 9), try to recover your ARIS installation (page 16) and run the patch setup again.
1. Adapt your modified files if required according to your installation protocol.
 2. Check the patched installation (page 13). To start all runnables, execute the **startall** ARIS Cloud Controller command.

Your ARIS server installation is patched. All bugs mentioned in the related **Readme** document are fixed.

If you use the **rpm -e** command, the patch is not removed. This command only removes meta data from the rpm database.

Use the **rpm -qa | grep aris10-p** command to view the history of all executed patch setups.

8 Check the patched installation

After successful execution of the **ARIS_Patch_Setup_V10.0.27.0.exe** file, use the **list** ACC command to display all runnables. The new build number is shown for the runnables that are still in the **STOPPED** state.

Example

```
Run ACC "list"  
Display of "abs_m           : STOPPED  <_a_version_aris>.3  
(com.aris.modeling.components.y-server-run-prod) "  
Run "ARIS_Patch_Setup_V10.0.27.0.exe"  
Run ACC "list"  
Display of "abs_m           : STOPPED  10.0.27.0  
(com.aris.modeling.components.y-server-run-prod) "
```

If part of your installation, these runnables must show the new build number:

- apg
- arcm
- cdf
- copernicus
- ecp
- adsadmin
- cloudsearch
- hds
- octopus
- abs
- simulation
- umcadmin

9 Execute the `updatesystemdb` ARIS Cloud Controller command

The patch setup does not automatically update the system database. The most current system database is hidden in a **jar** file contained in the patch setup but the database is not automatically updated. If you want to update the content of your system database because related content was fixed as well, you must execute the **updatesystemdb** ARIS Cloud Controller command (page 14) after you ran the patch setup for each tenant.

The system database holds content available for all databases of a tenant, such as the ARIS Method (all model, object, connection, and symbol types), filters, templates, macros, reports, semantic checks, and similar content.

In a new ARIS installation, the system database only contains predefined ARIS content provided by Software GmbH. ARIS users can customize the system database and add new content, for example, by defining custom method extensions, writing reports, or adding other content to the system database.

Each tenant in your ARIS installation has a different system database. Therefore, each ARIS tenant can have a specific set of ARIS method elements, a special set of reports, or other content that is not shared by the tenants.

As the default content of the system database shipped together with ARIS is updated as part of a new ARIS version, the new version of the system database is applied to an existing installation during an update. It only updates filters, default reports and macros, and templates shipped with the standard product. Default semantic checks will no longer be updated except of the following: **Allocation rules, Model attribute rules, Object attribute rules, Relationship attribute rules, Existence rules, and Rules for a BPMN diagram (BPMN 2.0)**. For these six rule types, the code is updated. The configuration of the rules stays untouched. User-defined modifications made in the configuration will not be overwritten. You can import the latest semantic checks from the ARIS installation package (<ARIS installation package>/ARIS_Installation_and_Documentation-<patch>**Content\Reports\Common_files** and **./Semantic Checks**). Usually, you have your own filters and templates and do not need updates for those that came with the standard product.

If you have an issue with any of the default reports, macros or scripts, or default Mini workflows, or you ran a patch setup, you can update the system database. In this case, it might also make sense to create a **test** tenant and only execute this command for this tenant. Then you can export individual report scripts or other content and distribute the required content to other tenants.

Run the **updatesystemdb** ACC command for all operational tenants one after another starting with the **default** tenant. Do not execute this command for the **master** tenant. Enter, for example:

```
invoke updatesystemdb on <abs_instance ID> tenant.name=default \  
tenant.user.name=superuser tenant.user.pwd="<superuser password in default>"  
invoke updatesystemdb on <abs_instance ID> tenant.name=<tenant1> \  
tenant.user.name=superuser tenant.user.pwd="<superuser password in tenant1>"  
invoke updatesystemdb on <abs_instance ID> tenant.name=<tenant2> \  
tenant.user.name=superuser tenant.user.pwd="<superuser password in tenant2>"
```

If you use multiple nodes, you must prefix the **invoke** command with **on <node name>**. Alternatively, use **set current node** to switch to those nodes with **abs** runnables.

If you have more than one **abs** instance in your installation, you only need to update the system database once per tenant on each instance.

If you do not update the system database for all tenants, the system still works but the latest updates and fixes for SAG default reports, semantic checks, macros, etc. will not be available.

10 Troubleshooting

This chapter contains information about basic troubleshooting. Find detailed information if the patch setup does not run properly or you want to restore a patched installation to the previous ARIS version.

10.1 Manually restore installation for a second patch execution

If the patch setup failed because prerequisites (page 9) were not met, you must recover your ARIS installation (page 16) and run the patch setup again.

Procedure

1. Check the tasks, log files, and error messages to locate the locked files and make them writable again (page 7).
2. Check if all files are writable (page 7).
3. List all backups that were made from the runnables on this node and identify the backup ID of the backup you want to use. To do so, execute the **list runnable backups** ARIS Cloud Controller command, such as:

```
ACC+ n1>list runnable backups
On node n1:
for instance abs_1 (GroupId = com.aris.modeling.components, ArtifactId
= y-server-run-prod):
  BackupId = 0    Date = 2020-07-11 Time : 01:11:14 Version = 10.0.12
  BackupId = 1    Date = 2020-07-13 Time : 01:17:10 Version = 10.0.12
  BackupId = 2    Date = 2020-07-14 Time : 11:29:16 Version = 10.0.12
...
```

4. Restore all runnables that caused the patch setup to fail. Therefore, execute the **restore runnable backup** command one after another for each related runnable.

Syntax:

```
<nodeSpecWithAllNodes>? "restore" ("instance" | "runnable")? (backups | backup)
(<instanceId> <backupId>)?
```

This command restores runnable backups on the current node, a specified node, or on all nodes. If only an instance ID is specified, the last backup of this instance is restored. If a backup ID is specified in addition to the instance ID, the backup with the given backup ID is restored. If no instance ID is specified for any of the configured runnables, the last backup available is restored.

Example:

```
ACC+ n1>restore runnable backup abs_1 1
This will restore the backup 1 (created at 2020-07-13 01:17:10) for runnable
abs_1 on n1 (GroupId = com.aris.modeling.components, ArtifactId =
y-server-run-prod, Version = 10.0.12.1).
Are you sure? (Y/N)
Y
Restore confirmed by user.
Successfully restored runnable abs_1 from backup 2020-07-13 01:17:10.
```

5. If the remote repository cannot be accessed, switch to the internal repository. To do so, enter:

set local.repository.only=true

6. When you restored all related runnables, enter **list** and check if all runnables are available in the recovered state.
7. Make sure again that all prerequisites are met so that the patch setup can access and delete the required files.
8. Run the patch setup again (page 10) related to your operating system.

Warning

Do not start the patch setup before the runnables are restored because the setup will fail again. Since the maximum number of backups created by a patch setup is three, you risk data loss after unsuccessfully patching your installation three times.

9. Adapt your modified files if required according to your installation protocol.
10. Check the patched installation (page 13).
11. Start all runnables. Therefore, you can use the **startall** ARIS Cloud Controller command or the ARIS > Administration > **Start ARIS Connect Server** link in the Windows **Start** menu.

Your ARIS server installation is patched. All bugs mentioned in the related **Readme** document are fixed.

10.2 Restore a patched ARIS installation

If you patched your installation successfully, all listed bugs are fixed. If you have problems with these fixes, you can manually restore all runnables to their pre-patched state using the **Restore runnable backup** ARIS Cloud Controller command.

Procedure

1. Stop all runnables using the **stopall** ARIS Cloud Controller command on each node.
2. Check if all files are writable (page 7).
3. List all backups that were made from the runnables on this node and identify the backup ID of the backup you want to use. To do so, execute the **list runnable backups** ARIS Cloud Controller command, such as:

```
ACC+ n1>list runnable backups
On node n1:
for instance abs_1 (GroupId = com.aris.modeling.components, ArtifactId
= y-server-run-prod):
  BackupId = 0    Date = 2020-07-11 Time : 01:11:14 Version = 10.0.12
  BackupId = 1    Date = 2020-07-13 Time : 01:17:10 Version = 10.0.12
  BackupId = 2    Date = 2020-07-14 Time : 11:29:16 Version = 10.0.12
...
```

4. Restore all patched runnables. Therefore, execute the **restore runnable backup** command one after another for each related runnable. You can identify patched runnables by the build number that is related to the patch.

Syntax:

```
<nodeSpecWithAllNodes>? "restore" ("instance" | "runnable")? (backups | backup)
(<instanceId> <backupId>)?
```

This command restores runnable backups on the current node, a specified node, or on all nodes. If only an instance ID is specified, the last backup of this instance is restored. If a backup ID is specified in addition to the instance ID, the backup with the given backup ID is restored. If no instance ID is specified for any of the configured runnables, the last backup available is restored.

Example:

```
ACC+ n1>restore runnable backup abs_1 1
This will restore the backup 1 (created at 2020-07-13 01:17:10) for runnable
abs_1 on n1 (GroupId = com.aris.modeling.components, ArtifactId =
y-server-run-prod, Version = 10.0.12.1).
Are you sure? (Y/N)
y
Restore confirmed by user.
Successfully restored runnable abs_1 from backup 2020-07-13 01:17:10.
```

5. If the remote repository cannot be accessed, switch to the internal repository. To do so, enter:
set local.repository.only=true
6. When you restored all related runnables, enter **list** and check if all runnables are available in the recovered state.

The patch was rolled back and your installation is in the same state as before the patch.

10.3 Product not found

If the patch setup cannot detect the installed ARIS server to be patched, the installation path in the registry might point to a wrong directory. In this case, ask **Global Support ARIS** for the **ARISRegistryFix-<version number>.exe** tool. Use this tool to fix the registry entry and start the patch setup again.

If the ARISRegistryFix tool does not work without parameters and the product can still not be found, run the ARISRegistryFix tool using the **dr** and **f** parameters one after another. When proceeded, run the patch setup again.

Example

ARIS Registry Fix V1.0.0.0.1197474.exe -dr

ARIS Registry Fix V1.0.0.0.1197474.exe -f

Usage: ARISRegistryFix [-f] [-dr] [-du] [-ds] [-da]

-f: Fix ARIS registry entries

-dr: Delete ARIS registry entries

-du: Delete ARIS registry entries including uninstall information

-ds: Delete ARIS service (service has to be stopped)

-da: Delete all (-dr -du -ds)

10.4 Logging

You can find the related log files in the <ARIS server installation directory>/bin/log). If you cannot solve the problems and have a maintenance agreement, please send an error description and the log files to the ARIS Global Support via Empower (<https://empower.softwareag.com/>).

If you installed ARIS server on a Linux operating system, the ARIS server **logs** directory cannot be directly read. Therefore, **sudo** permissions are required as provided for the **aris10**.

- **patch.log**

Contains messages from the ARIS Cloud Controller command-line tool concerning the patch setup. Use the listed exceptions to spot the action in the patch process that caused an error.

- **agent.log**

Contains messages from the ARIS agent concerning the patch setup. If you executed the **check file system permissions** ARIS Cloud Controller command and more than 10 issues were detected as non-writable, the **agent.log** file contains the complete list.

11 Legal information

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

11.2 Support

If you have any questions on specific installations that you cannot perform yourself, contact your local Software GmbH sales organization

(<https://www.softwareag.com/corporate/company/global/offices/default.html>). To get detailed information and support, use our Web sites.

If you have a valid support contract, you can contact **Global Support ARIS** at: **+800 ARISHELP**. If this number is not supported by your telephone provider, please refer to our Global Support Contact Directory.

For issues regarding the product documentation, you can also send an e-mail to documentation@softwareag.com (<mailto:documentation@softwareag.com>).

ARIS COMMUNITY

- Download products, updates and fixes
- Find information, expert articles, issue resolution, videos, and communication with other ARIS users

If you do not yet have an account, register at ARIS Community.

PRODUCT TRAINING

You can find helpful product training material on our Learning Portal.

TECH COMMUNITY

You can collaborate with Software GmbH experts on our Tech Community Web site. From here you can, for example:

- Browse through our vast knowledge base.
- Ask questions and find answers in our discussion forums.
- Get the latest Software GmbH news and announcements.
- Explore our communities.
- Go to our public GitHub and Docker repositories and discover additional Software GmbH resources.

PRODUCT SUPPORT

Support for Software GmbH products is provided to licensed customers via our Empower Portal (<https://empower.softwareag.com/>). Many services on this portal require that you have an account. If you do not yet have one, you can request it. Once you have an account, you can, for example:

- Add product feature requests
- Search the Knowledge Center for technical information and tips
- Subscribe to early warnings and critical alerts
- Open and update support incidents.