



# Miria for Migration Documentation

Miria 4.0

Publication Number: MIRIA-MIG-PDF-EN-0123-REV1

Publication Date: January 2023



©2023 Atempo SAS. All rights reserved.

All names and products contained herein are the trademarks or registered trademarks of their respective holders.

---

The information contained herein is the confidential and proprietary information of Atempo SAS. Unauthorized use of this information and disclosure to third parties is expressly prohibited. This technical publication may not be reproduced in whole or in part, by any means, without the express written consent of Atempo SAS.

Atempo SAS  
23 Avenue Carnot  
91300 Massy - France

# Contents

CHAPTER 1 - About Miria for Migration	1
CHAPTER 2 - Migration Principles	2
What is a Migration Project?	2
Miria as a Migration Solution	2
Migration Steps	2
CHAPTER 3 - Architecture	4
Miria Components	4
Snapshot and FastScan Technologies	5
CHAPTER 4 - Web Interface	6
CHAPTER 5 - Prepare for a Migration Project	8
CHAPTER 6 - Requirements	9
Standard Configuration	9
Computer and Hardware Requirements	9
Server	9
Data Movers	10
Port Number Matrix	11
CHAPTER 7 - Product Installation	13
Prerequisites	13
Install	13
Install Additional Agents or Data Movers (Optional)	13
Manage the License	14
CHAPTER 8 - Launch the Application	16
Logging in with the Two-Factor Authentication	16
CHAPTER 9 - Manage the Infrastructure	19
Add a Storage Manager and Container	19
File Storage Container	20
File Storage One to One	21
SnapStor	23
Virtual Storage	24
Media Storage	24
Easy move Amazon S3	26
Google Cloud Storage	28
Microsoft Azure Blob Block	29
Scality	31

Quantum Active Scale .....	33
Seagate Lyve Cloud .....	35
Cloudian HyperStore .....	36
Add Server and Agent(s) .....	38
Add a New NAS Platform .....	39
Add a Storage Platform .....	40
Add a Shared File System .....	40
Activate My File System .....	41
Available options .....	42
Edit a Platform .....	43
Platforms Permissions .....	43
Metadata .....	44
Applying Metadata to Repositories .....	46
<b>CHAPTER 10 - Organize and Configure the Migration</b> .....	<b>47</b>
Organize Projects .....	47
Project description .....	47
Task description .....	47
Configure the Migration .....	47
Create a New Project .....	47
Create a New Task .....	48
Edit a Project .....	50
Edit a Task .....	51
Start Migration Task(s) .....	51
Duplicate a Task .....	51
Disable a Project or a Task .....	51
<b>CHAPTER 11 - Manage the Migration</b> .....	<b>52</b>
Step 1: First Synchronization .....	52
Step 2: Incremental Synchronization .....	53
Step 3: Final Synchronization (Cutover) .....	54
<b>CHAPTER 12 - Manage Users</b> .....	<b>56</b>
Add a User .....	56
Edit a User .....	57
Add a User Group .....	57
Configure SAP .....	59
Set Password Policies .....	60
Add a LDAP Rule .....	61
Add a LDAPS Rule .....	61
Edit a Rule .....	61
Set the Two-Factor Authentication .....	61

Configuring a Two-Factor Authentication Set as Mandatory .....	62
Configuring a Two-Factor Authentication Set as Optional .....	63
<b>CHAPTER 13 - Advanced Tasks</b> .....	<b>67</b>
Task Types .....	67
Internal Management Tasks .....	67
Data Movement Tasks .....	68
Creating a Task .....	70
Creating a New Task from the Tasks Tab .....	70
Duplicating an Existing Task .....	70
Organizing tasks .....	70
Manage projects .....	71
Move a task .....	71
How Tasks Run .....	71
Testing a Task .....	73
Launching a Task Manually .....	73
Canceling a run .....	73
General Configuration Parameters for Tasks .....	74
General Parameters Common to All Tasks .....	74
Common Tabs .....	76
Task-specific Parameters .....	79
Automatic Catalog Ingest Task .....	79
Automatic Deletion Task .....	82
Automatic Retention Tasks .....	83
Automatic Storage Repack Task .....	84
Database Backup Task .....	85
Maintenance tasks .....	85
Archive Report Task .....	88
Volume Management on Storage Managers Task .....	90
XML Ingest Tasks .....	90
<b>CHAPTER 14 - Monitoring</b> .....	<b>98</b>
Generate an Environment Report .....	98
Explore a Platform .....	98
Test the API Connection of a Platform .....	98
Monitor the Task Progress .....	99
View Project or Task Logs .....	99
Perform Integrity Check .....	99
<b>APPENDIX Configure an Isilon Storage</b> .....	<b>101</b>
Isilon NAS Platform Prerequisites .....	101
Stream Options .....	101

APPENDIX Create a Nutanix User Account	103
APPENDIX Recycling Triggered by Volume on Storage	104
APPENDIX Replications in between two S3 object storages	107

# CHAPTER 1 - About Miria for Migration

Miria for Migration is a software appliance developed by Atempo that allows organizations to migrate and synchronize large numbers of files between heterogeneous, homogeneous and hybrid storages. It is available to all organizations and all IT environments enabling fast, safe and cost-effective data migrations.

This document instructs users on how to prepare, install, configure and manage data migration projects. Atempo recommends that users follow the steps in this document to perform data migration.

# CHAPTER 2 - Migration Principles

This chapter explains the challenges of a migration project and introduces users to the key features of Miria as a migration solution.

## What is a Migration Project?

A migration project refers to the process of moving data from one environment to another. Generally, this migration is required when a system, location or storage provider is changed.

During the migration, it is important that the company's production is not impacted. Data should be synchronized while the source storage remains in production and production downtime should be minimized.

The duration of a migration project may vary significantly and depends on:

- The size and number of files to migrate.
- The number of modifications on the source storage.
- The time available for production downtime on the source storage during cutover.
- The performance of the infrastructure (source and target storage, network bandwidth, etc.).

## Miria as a Migration Solution

Miria utilizes several key features that enable a seamless transfer of data. All the while maintaining timeline requirements, minimizing user impact and ensuring data reliability on all transactions. These key features are:

- Optimizing data transfer through job distribution and parallelization.
- Ability to multithread jobs within data movers.
- FastScan technology, which enables quick identification of all object modifications made between two migration synchronizations.
- Incremental and automatic file migrations between heterogeneous storage.
- Iterative migration cycles enabling the source storage to remain operational during the storage migration.
- Automatic object integrity and migrated file access checks.
- Easily adjust performance by adding or removing a data mover.
- Control of the migration project throughout the different steps outlined below.

During the synchronization, Miria constantly checks that the data and metadata read on the source storage are exactly written on the target storage using a hash mechanism comparison.

## Migration Steps

A migration project consists of 3 steps:

- **Step 1: First Synchronization:** sets off the initial data transfer and performs a first snapshot of the source. The snapshot is used as a reference point in time. The transfer then copies



the source storage data to the target storage.

- **Step 2: Incremental Synchronization** : propagates any modifications made on the source storage (since the previous incremental sync) to the target storage.
- **Step 3: Final Synchronization (Cutover)**: completes the data migration to the target storage while the production is halted on the source storage.

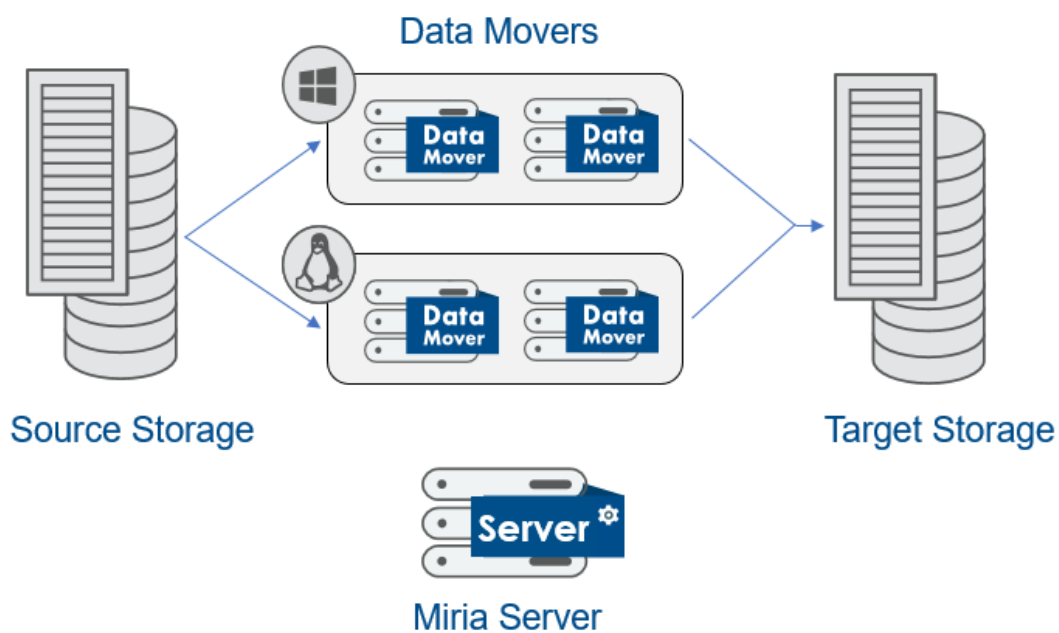
These steps may happen fairly quickly or take days or even weeks. This depends on the volume of data, customer workflow, testing and timeline for cutover.

# CHAPTER 3 - Architecture

This chapter describes the different components of Miria for Migration and explains the Snapshot and FastScan technologies.

## Miria Components

The diagram (Figure 1) illustrates the typical migration configuration with all the Miria components:



**Figure 1:** Miria for Migration components in a configuration

The infrastructure is composed of the following components:

### Miria Server

The Server manages all the data movers and can be installed on a dedicated physical or virtual machine.

Host Miria's database, which stores:

- Configuration settings.
- Necessary information to perform the various steps of the migration project (snapshots, FastScan, copies on the target storage).
- Report information.

### Agents (Data Movers)

Miria Agents manage the data movement, acting as data movers. They are key components for the global performance of the migration operation. Data movers must be sized appropriately (network, CPU, and memory).

# Snapshot and FastScan Technologies

## Snapshot

Snapshot technology is a photograph of a file system taken at a particular point in time (e.g., VSS for Windows). NAS and shared file system snapshots are taken through proprietary API of the specific appliance.

The Snapshot is used at every step of the migration project and freezes a consistent image of the data to transfer.

## FastScan

FastScan is an option integrated within Isilon, Qumulo, OceanStor, Nutanix NAS and GPFS shared file systems.

FastScan enables Miria to optimize the detection of any modifications within a given file system by detecting differences between two snapshots. It then builds a change list that negates the need for scanning or browsing the entire file system looking for any updates and changes. This technology is used when the source storage is still in production during the migration process.

The retrieved list of modifications contains the following information:

- Created objects (files, directories, and links).
- Modified objects.
- Deleted objects.
- Objects whose type has changed (e.g., a directory has become a file or vice-versa, a directory has become a link or vice-versa, etc.).

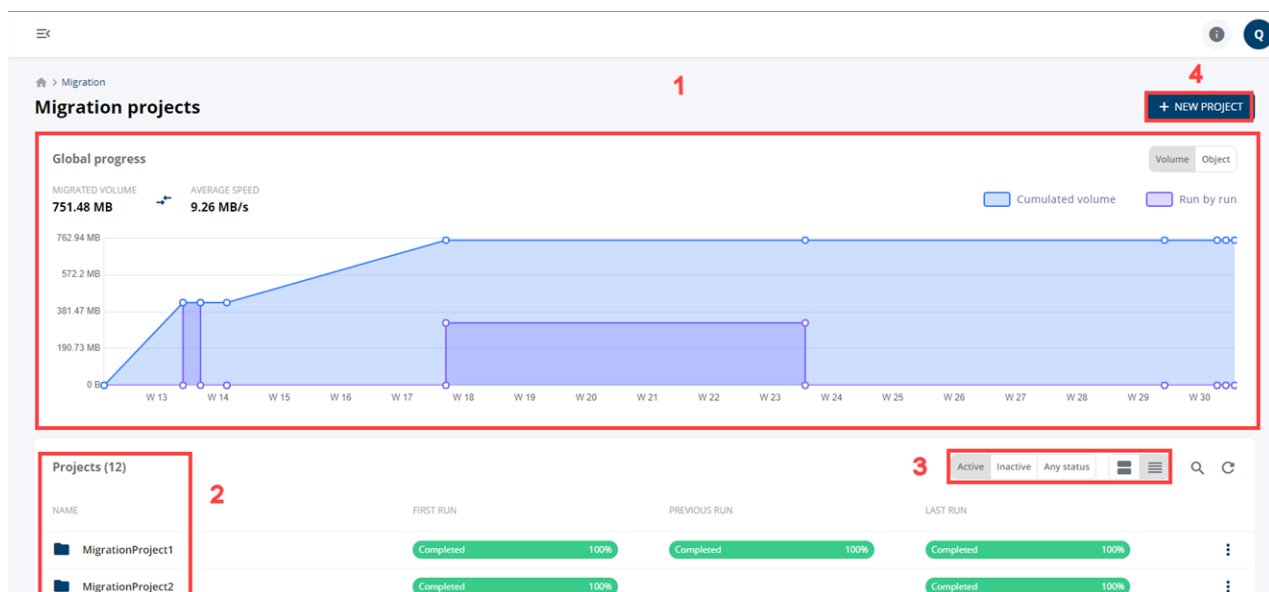
The list retrieved by FastScan is then fully scanned to identify the operations to perform (objects to synchronize, objects to delete, modifications to propagate, etc.) on the target storage. The combination of the FastScan followed by a full scan of the file system is useful when a migration project is interrupted. This feature prevents already transferred data to be transferred again when migration resumes.

# CHAPTER 4 - Web Interface

The Web Interface is designed to enable end-to-end management of the migration project. It allows you to:

- Configure your migrations.
- Supervise operations.
- View and send Activity reports by email.
- View Statistics reports.

When you log on to the Web Interface, the Migration dashboard appears (Figure 2).



**Figure 2:** 1. Global progress; 2. Project overview; 3. Project representation; 4. Add new project

The Web Interface helps administrators and users to supervise migration projects and is divided into two areas:

## Navigation Pane

The navigation pane, located on the left, gives access to 7 different tabs:

- The **Migration** tab lets you:
  - Monitor the general progress.
  - Choose if you want to monitor the general progress by volume or objects.
  - Configure migrations projects.
- The **Infrastructure** tab enables the ability to see and configure the Miria infrastructure.
- The **Users** tab enables to configure users, user groups and a security authentication path (SAP).
- The **Jobs** tab enables to monitor the job progress.
- The **Logs** tab allows examination of the general logs of a migration.
- The **Settings** tab allows management of all your settings (e.g., license, hidden projects and tasks).
- The **Logout** tab.

## Dashboard

The Dashboard displays information about current and past migrations. It is divided into 3 sections:

- The **Global Progress** section allows monitoring of the volume, as well as the number and average speed of the migrated objects.
- The **Volume/Objects** button lets see and change the general reporting by volume or by number of objects.
- The **Projects** section enables to:
  - Display information about projects: name, last run, first run, previous run.
  - Check the status of the last run.
  - Perform actions on projects: Edit, Start All Tasks, New Task, Disable, Show Logs.
  - Create a New project.

The same view is available for projects and tasks.

# CHAPTER 5 - Prepare for a Migration Project

Before starting your migration project, Atempo recommends that you complete the Data Migration Questionnaire. This preparation step will save you time later on.

The following information is required to complete the questionnaire:

- Project information:
  - Company Name.
  - Migration Project information: start date, target end date, maximum expected cutover time.
  - Customer participants information: name and position, phone number, email address.
  - Partner participants information: name and position, phone number, email address.
- Source and Target Storage:
  - Brand and model of the Operating system/appliance OS version.
  - Number of nodes.
  - Data network ports and speed.
  - Production state.
- SMB/CIFS and NFS data to migrate:
  - Number of shares.
  - Total size of data.
  - Type of files.
  - Number of files.
  - Number of directories.
  - Average file size.
- Network environment: bandwidth, firewall, port, LACP configuration, MTU Size, etc.
- Migration: Source storage still in production during the migration, performance constraints during the migration, test users to check data access and integrity, etc.
- Applications: Client applications involved in the migration, etc.

# CHAPTER 6 - Requirements

This chapter outlines the requirements to install and plan migration projects.

## Standard Configuration

The sizing of the Miria hardware infrastructure depends on several factors outlined below:

- Capacity of the data volumes.
- Timeline of expected completion / performance throughput.
- Source platforms (brands, model, capacity, etc.).
- Type of technology: CIFS, NFS, etc.
- Type of networks for management and data access, speeds, bonding, MTU size, etc.
- Destination storage types and capacity.
- Number of files/folders to move.
- Availability of the FastScan: it is strongly recommended that the FastScan Technology is supported by the source storage.

## Computer and Hardware Requirements

The software architecture is based on two major components:

- [Server](#).
- [Data Movers](#).

### Server

#### Platform Requirements

##### **For a small environment (less than 10 million files)**

When the number of files does not exceed 10 million and the data volume is smaller than 200TB, the Miria server can run on a virtual machine with:

- Dual-proc 8-cores.
- 32GB of RAM.

##### **For a large environment (more than 10 million files)**

When the number of files is greater than 10 million, the recommended Server configuration is the following:

- Dual-proc 16-cores.
- 64GB RAM.
- Dual 10Gbe cards (for data movers communication).

### Operating System

See the [Compatibility guide](#) for more information.

## Disk Requirements for Miria database

Workflow configuration, statistics and other relevant information are recorded in a central repository based on a database. The disk space required to store Miria is based on the number of file instances. Information on metadata is not stored in this database. File information is recorded in the database only if Migration Integrity Check is enabled.

## Data Movers

A data mover reads data from a source storage and simultaneously writes it to the target storage, at the maximum available speed. Their key features:

- Guaranteed high-performance throughput.
- Ability to cap or control network bandwidth (configured at operating system level) to ensure there is no impact on the production.
- Optimized scanning by Miria's software.
- Configurable job parallelization and multithreading capabilities.

The association of a pool with a NAS allows to improve the performance during the migration of the data of this NAS. Pooled data movers provide redundancy as the workload is distributed over several machines.

Sizing data movers requires the following information:

- Data volume (size of volume, number of files and directories, and average file size),
- Performance throughput requirement and the type of the target (disk, tape, cloud, object).

## Platform Requirements

### For data volume lower than 200TB

The Miria Server can perform the role of data mover.

### For data volumes between 200 TB and 500TB

The following data mover configuration is recommended:

- Dual-proc 16-cores.
- 32GB RAM.
- Specific attachment to the source storage (10Gbe, 40Gbe, 100Gbe or IB).
- Specific attachment to the target storage (10Gbe, 40Gbe, 100Gbe, IB or FC).

### For data volumes between 500TB and up to 2PB

The recommended architecture contains two data movers (configured in a single pool) with the following configuration per data mover:

- Dual-proc 16-cores.
- 32GB RAM.
- Two HDD 300GB 10K SAS drives (dedicated for Operating System).
- Specific attachment to the source storage (10Gbe, 40Gbe, 100Gbe or IB).
- Specific attachment to the target storage (10Gbe, 40Gbe, 100Gbe, IB or FC).

## Operating system

See the [Compatibility Guide](#) for more information.



## File size & performance throughput

Using Miria software, transfer rates from the source storage to the target storage should be close to the speed of the hardware equipment. However, performance is usually limited by the read or write operations of the file system when there are large numbers of small files or directories.

- **For large files (>10MB)** data movement, one data mover can have a sustained throughput of 3GB/s.
- **For very small files (<10kB)** data movement, one data mover can have a sustained throughput of 1GB/s. However, if there are a very large number of directories containing a few small files, the performance of the scan could decrease the overall performance.

## Port Number Matrix

This matrix identifies the port numbers user for the Miria components ([Table 1](#)).

**Table 1:** Port numbers per component

From Component	From @IP	Destination Component	To @IP	Protocol	Port	FWRule	Comment
<b>Web Interface</b>							
<b>Acces Server</b>	Admin Console @IP	Server	Server @IP	<b>HTTP TCP</b>	80	IN	Port automatically opened by Setup
<b>Acces Server SSL</b>	Admin Console @IP	Server	server @IP	<b>HTTPS TCP</b>	443	IN	Port automatically opened by Setup
<b>Data Mover</b>							
<b>Engine Port</b>	Agent @IP	Server	Server @IP	<b>TCP</b>	2524	IN	Port automatically opened by Setup
<b>Miria Server / DB</b>							
<b>PostgreSQL Server</b>	Server @IP		Server @IP	<b>TCP</b>	5433		PostgreSQL Server / No need to open
<b>Other</b>							
<b>Server</b>	Server @IP	Mail Server	SMTP Server @IP	<b>TCP</b>	25 / 2525	OUT	Port needed for mail notification
<b>External storage</b>	Server @IP	Cloud/S3 like storage	Provider @IP	<b>TCP</b>	Provider dependant	OUT	Port needed in function of target cloud/S3 storage

**Table 1:** Port numbers per component

From Component	From @IP	Destination Component	To @IP	Protocol	Port	FWRule	Comment
<b>NFS</b>	Server @IP	NFS Storage	Storage @IP	<b>TCP/UDP</b>	111	OUT	
				<b>TCP/UDP</b>	2049	OUT	
<b>CIFS</b>	Server @IP	CIFS Storage	Storage @IP	<b>UDP</b>	137-138	OUT	
				<b>TCP</b>	139 / 445	OUT	

# CHAPTER 7 - Product Installation

This chapter helps you to install and to manage the product license upon your first login.

## Prerequisites

Before installing Miria, check the following prerequisites:

- Prepare the operating system and apply any required OS patches.
- Check the [Compatibility Guide](#)
- Read the [Before You Start](#) section.
- Download the latest GA release from <https://support.atempo.com>.
- Gather Host MAC Address to generate the license.
- Prepare all necessary information: login for all components, list of shares to migrate, etc.
- Prepare a desktop or X-term environment to install Miria agents on the servers and data movers. Installation binaries are GUI-based.

## Install

Miria installation uses 1 binary: **installMiria**. This binary holds the server component, including the web interface, additional data movers and PostgreSQL database.

1. Run the **installMiria** binary.
2. Select the language.
3. Accept the license.
4. In the **Installation Type Selection** window, select **Server**.
5. In the **Install set** window, select **Typical**.
6. In the **Install Folder** window, choose a new path or leave default for **Miria's directory**.
7. In the **Atempo Digital Archive Access Server** window, write a port number for the secured HTTPS Port (443 is recommended).
8. In the **Firewall Configuration** window, select **Yes** to configure Firewall automatically (works on both Windows and Red Hat).
9. In the **Pre-Installation Summary** window, review the installation summary and click **Install**.
10. In the **Install Complete** window, check the final status and perform troubleshooting if necessary.

## Install Additional Agents or Data Movers (Optional)

An agent can be a data mover for a source platform and/or a target platform. By default, Miria Server has an agent install.

Additional data movers can be installed to obtain:

- multiprotocol support (needs Windows for CIFS and Linux for NFS).
- improved performances (tasks will be parallelized).

- improved availability (in case of failure of a data mover).

### ***To install Miria agent***

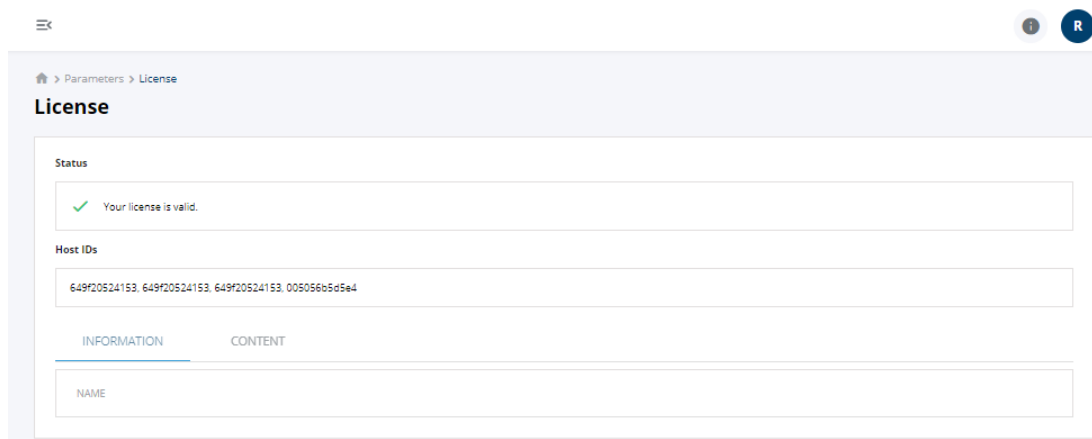
1. Run the **installMiria** binary.
2. Select the language.
3. Accept the license.
4. In the **Installation Type Selection** window, select **Agent**.
5. In the **Install set** window, select **Typical**.
6. In the **Install Folder** window, choose a new path or leave default for **Miria's directory**.
7. In the **Atempo Digital Archive Access Server** window, write a port number for the secured HTTPS Port (443 is recommended).
8. In the **Firewall Configuration** window, select **Yes** to configure Firewall automatically (works on both Windows and Red Hat).
9. In the **Pre-Installation Summary** window, review the installation summary and click **Install**.
10. In the **Install Complete** window, check the final status and perform troubleshooting if necessary.

## Manage the License

When you log in for the first time, you will be redirected to a License entry page. By default, the software comes with a 15-day demo license. It is possible to ask for an extension of the Demo License.

If you do not have a license, contact [LKS@atempo.com](mailto:LKS@atempo.com).

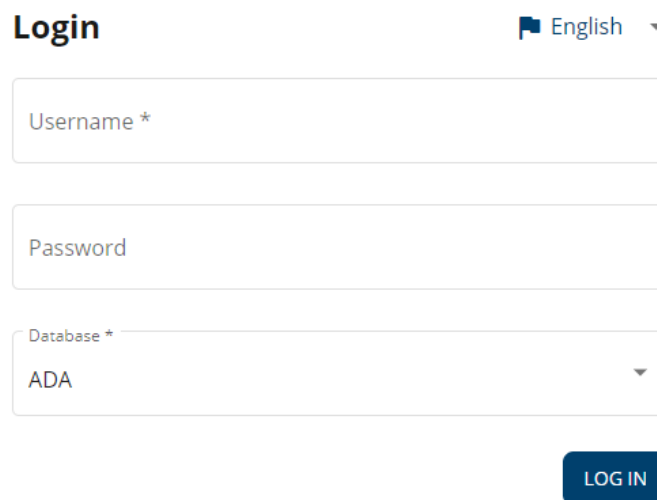
1. Open the generation link provided by Atempo License Key Service (received by email).
2. Enter your License authorization code to log in then click **Generate**.
3. Select **Components**.
4. Select all the Miria items you need.
5. Enter the **HostID** (MAC Address).
6. Click the **Generate** button. You should receive your license file by email, you can also download the license file directly.
7. Connect to the Web Interface.
8. Click the **parameters** tab.
9. On the license section, click the **Content** tab.
10. Copy and paste the license file content.
11. Select **Update License**. The status of a valid license is displayed ([Figure 3](#)).



**Figure 3:** A valid product license in the Web Interface

## CHAPTER 8 - Launch the Application

1. Open a web browser.
2. Type the server URL: <server name>/webapp. The login window appears ([Figure 4](#)).
3. Enter your authentication information:
  - **User name:** At the first connection, type "root". This user has all rights. You will then have to choose a new username that cannot be modified.
  - **Password.**



The screenshot shows a web-based login interface. At the top left is the word 'Login'. To its right is a language selector showing 'English' with a dropdown arrow. Below these are three input fields: 'Username \*', 'Password', and 'Database \*'. The 'Database \*' field is a dropdown menu with 'ADA' selected. At the bottom right is a blue button labeled 'LOG IN'.

**Figure 4:** Authentication window as shown in the HTTP interface

## Logging in with the Two-Factor Authentication

See Set the Two-Factor Authentication to configure this option.

### First connection:

1. Enter your authentication information.  
If the password policy is enabled and is not met when you log in, you have to create a new password. In this case, a window opens to enables you to do so. Once you entered your authentication information, this window appears ([Figure 5](#)):

[< BACK](#)

## Two-Factor Authentication

Securing authentication takes three steps.

### 1. Download an authentication application

For example Authy or Google Authenticator

### 2. Provide the authentication key

Enter the following characters in the Authentication application or scan the QRcode

**RYGV OQ4D ZLDX QQPJ P5QG TKHL WEU6 2GYT**



### 3.Enable the Two-Factor Authentication

Enter the code provided by the authentication application (Make sure your computer clock is on time).

ENABLE

Figure 5: Securing authentication

2. Scan the QR code or enter the key of characters given with it on the Authentication application on your phone.
3. Enter the code provided by the Authentication application or the website and click **Enable**. Make sure your computer clock is on time. This window appears ([Figure 6](#)):

## Two-Factor Authentication



This user is protected by the Two-Factor Authentication



### Recover codes

Five recover codes are provided when activating the Two-Factor Authentication. They will help you connect if you lose access to your authentication application. Keep them in a safe place as they won't be displayed again. A recover code becomes invalid once used.

49346025 - 91053115 - 51178149 - 85585663 - 43474637



I have safely recorded this code

CONTINUE

Figure 6: Recover codes

4. Miria provides 5 recover codes (Figure 6). Write them all down, and keep them. This way, you will be able to connect even if you lose access to your authentication application. Each one of them can be used one single time.
5. Click the toggle to confirm that you safely recorded the codes and click **continue**. You are now connected.



## CHAPTER 9 - Manage the Infrastructure

This chapter explains how to configure the migration infrastructure. The infrastructure may consist of different storage types (e.g. agents, local file system, shared file systems) that have been configured as repository platforms ([Figure 7](#)).

> To access the infrastructure information in the Web Interface, click the **Infrastructure** tab.

The following tiles are available:

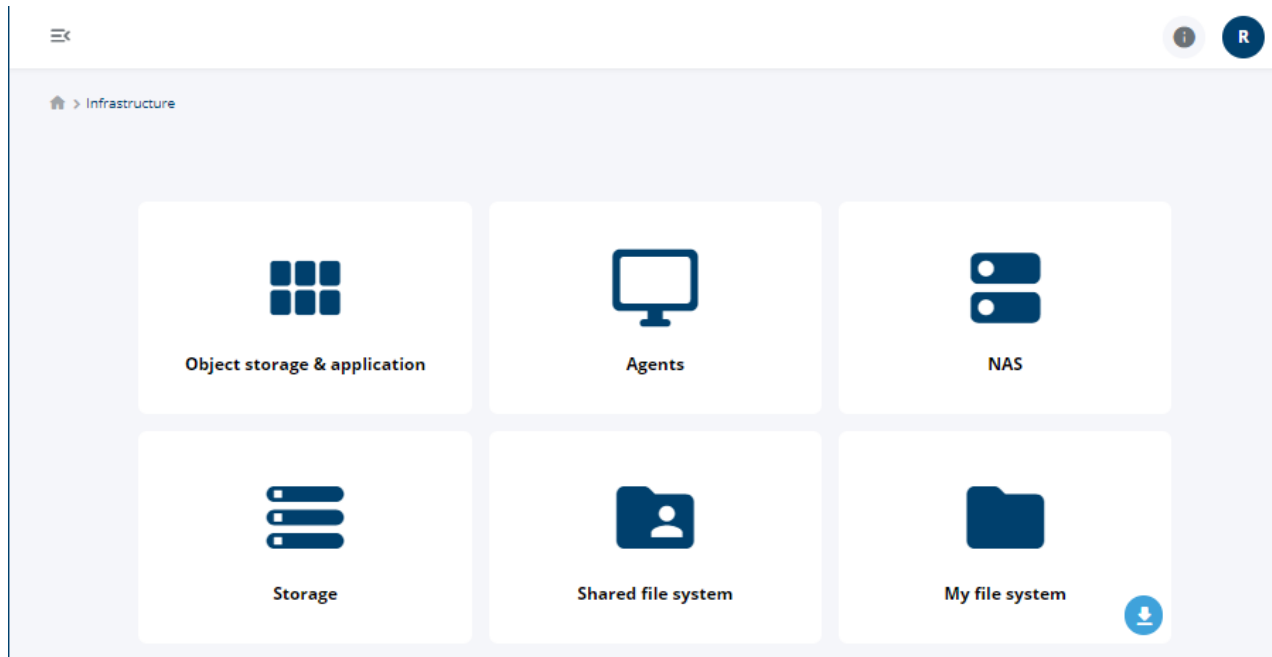


Figure 7: Storage types sorted by list in the **Infrastructure** interface

- **Object storage & Application** View and configure a storage manager and storage manager container.
- **Agent** Add agents or access, explore and verify the status of your own agent.
- **NAS** View and configure a NAS platform.
- **Storage** Declare platforms as storage types.
- **Shared file system** View and configure a shared file system.

## Add a Storage Manager and Container

To configure the infrastructure, the Object storage & Application entry is used to create storage managers and containers.

A storage manager is the storage definition, which can be tape, cloud (e.g., AWS, Google), disk and object storage. It manages the data migration from a primary storage to a secondary storage. Once you have created a storage manager, you must create a storage manager container. The storage manager container defines the location where the data are archived within the storage manager.

This chapter outlines how to add a storage manager and container for File Storage variants and, as an example, Amazon S3, Google Cloud Storage and Microsoft Azure Blob Block. For other third-party storage managers, see [Third Party Storage Managers in Miria Administration documentation](#).




## File Storage Container

When you add a File Storage Container, data are organized by job. Each job corresponds to only one file (container) on the destination file system.

### Step 1: Add a storage manager

1. Click the **Infrastructure** tab, then **Object Storage & Application**.
2. Click **New storage manager**.
3. Select **File Storage Container** and click **Next**.
4. Enter the name of the storage manager.
5. Choose the appropriate status:
  - **Online** Default value if you want to perform an archiving.**Or**
  - **Suspended** This status is useful for maintenance operations.
6. Select a storage platform. This is the name of the destination machine that hosts the files. This machine must be declared as a platform in Miria.
7. Activate **UTF8 Support** if you want to support UTF8 character encoding.
8. If needed, set volume management. This option enables volumes to trigger the configuration and activation of retention. See also [Recycling Triggered by Volume on Storage](#).
  - Set a High Water Mark value in GB.
  - Set a Task High Water Mark in GB only if you want to activate scheduled monitoring.
  - Set a Low Water Mark in GB.
9. Click **Create** to add the storage manager.

### Step 2: Add a storage manager container

1. Select the storage manager for File Storage and click the  button to add a container.
2. Complete the properties of the storage manager container:
  - a. **Storage container name**.
  - b. **Deduplication domain**. A new domain can be created, by clicking the  button.
  - c. **Archiving run lock**. A new one can be created, by clicking the  button.
  - d. **Threads**. Number of threads the storage manager container can manage. Select a numeric value from 1 to 128. When selecting the number of threads, take into account the data mover capacity.
3. Select the directory where the data are archived on the storage manager. This is an absolute path.
4. Set the digest type. This ensures that the object you retrieve has not been modified on the storage and that it is identical to the object that was archived.

The more complex the hash, the slower the calculation times. A complex hash decreases performance. It is recommended to use SHA-256 for the best compromise between performance and security.

5. Choose whether to activate metadata. The metadata associated with the archived object are sent as URL encoded strings. You can send only up to 2 KB of metadata. A log indicates the skipped metadata above 2 KB.
6. Activate **Alternative path** if you want to archive the data on other machines on the network. You must then declare the paths of the mounting points as alternative paths. Click **Add new path** and complete the following parameters:
  - a. **Agent** Name of the Miria platform where the data to archive is located. Select the agent from the list.
  - b. **Path** Absolute path of the directory where you want your data to be archived on the platform specified in the Agent field.
  - c. **User and password** Credentials of a user that has access permissions to this path.
  - d. **Enable On/Off** Disable temporarily the alternative path for an agent.
7. Set a prefix if you want to define how the files are organized on the storage manager container (i.e., what are their paths on the disk).
8. Click **Create** to add the storage manager container.

## File Storage One to One

When you add a File Storage One to One, the archived data are organized in a file tree structure in the same way as the data on the source file system. One file/directory on the source file system corresponds to the same file/directory on the destination file system. Data can be accessed outside of Miria.




### Step 1: Add a storage manager

1. Click the **Infrastructure** tab, then **Object Storage & Application**.
2. Click **New storage manager**.
3. Select **File Storage One to One** and click **Next**.
4. Enter the name of the storage manager.
5. Choose the appropriate status:
  - **Online** Default value if you want to perform an archiving.

**Or**

  - **Suspended** This status is useful for maintenance operations.
6. Select a storage platform. This is the name of the destination machine that hosts the archived files. This machine must be declared as a platform in Miria.
7. Activate **UTF8 Support** if you want to support UTF8 character encoding.
8. If needed, set volume management. This option enables volumes to trigger the configuration and activation of retention. See also [Recycling Triggered by Volume on Storage](#).
  - Set a High Water Mark value in GB.
  - Set a Task High Water Mark in GB only if you want to activate scheduled monitoring.
  - Set a Low Water Mark in GB.
9. Click **Create** to add the storage manager.

**Step 2: Add a storage manager container**

1. Select the storage manager for File Storage and click the  button to add a container.
2. Complete the properties of the storage manager container:
  - a. **Storage container name.**
  - b. **Deduplication domain.** A new domain can be created, by clicking the  button.
  - c. **Archiving run lock.** A new one can be created, by clicking the  button.
  - d. **Threads.** Number of threads the storage manager container can manage. Select a numeric value from 1 to 128. When selecting the number of threads, take into account the data mover capacity.
3. Select the directory where the data are archived on the storage manager. This is an absolute path.
4. Set the digest type. This ensures that the object you retrieve has not been modified on the storage and that it is identical to the object that was archived.  
The more complex the hash, the slower the calculation times. A complex hash decreases performance. It is recommended to use SHA-256 for the best compromise between performance and security.
5. Set the data compression value. This specifies whether the archived data must be compressed in the storage and defines the compression type:
  - **None** No compression.
  - **ADAZip** Optimized internal compression format. Files compressed with this format have a .adazip extension.
6. **Immutable disk repository** This option makes the files immutable. They cannot be modified, deleted, or renamed. No link can be created to these files.  
For more details, regarding immutability flags, please have a look at the XFS CTL Linux Man Page : [3-xfscctl](#)  
To get to know about prerequisites for this option, please refer to the Installation guide, Chapter 1 Preparing to install, in the part Immutable Disk Repository.

**Important:** As immutability is only supported on Linux XFS and Ext3/4, the option will be grayed if the One to One is on Windows OS.

7. If needed, set volume management. This option enables to define a quantity of disk space that is always kept free on the destination volume (e.g., to permit sharing this volume with other applications). You can define its value either as a percentage of the disk space or as a number of GB. By default, archiving to a File Storage container uses all available disk space on the target volume.
8. Activate **Alternative path** if you want to archive the data on other machines on the network. You must then declare the paths of the mounting points as alternative paths. Click **Add new path** and complete the following parameters:
  - a. **Agent** Name of the Miria platform where the data to archive is located. Select the agent from the list.
  - b. **Path** Absolute path of the directory where you want your data to be archived on the platform specified in the Agent field.
  - c. **User and password** Credentials of a user that has access permissions to this path.
  - d. **Enable On/Off** Disable temporarily the alternative path for an agent.

9. Set a prefix if you want to define how the files are organized on the storage manager container (i.e., what are their paths on the disk).
10. Click **Create** to add the storage manager container.

## SnapStor

When you add a SnapStor storage manager, the archived data are organized in a file tree structure in the same way as the data on the source file system *and* located in a snapshot created after the archiving task. An instance of a file/directory in the archive corresponds to the same file/directory in a snapshot. A file or a directory can be retrieved individually.

**Note:** The SnapStor storage manager only supports Windows agents and Qumulo, Dell Isilon, Huawei OceanStor or GPFS Shared File System as storage platforms.




### Step 1: Add a storage manager

1. Click the **Infrastructure** tab, then **Object Storage & Application**.
2. Click **New storage manager**.
3. Select **SnapStor** and click **Next**.
4. Enter the name of the storage manager.
5. Choose the appropriate status:
  - **Online** Default value if you want to perform an archiving.

**Or**

  - **Suspended** This status is useful for maintenance operations.
6. Select a storage platform. This is the name of the destination machine that hosts the archived files. This machine must be declared as a platform in Miria.
7. Click **Create** to add the storage manager.

### Step 2: Add a storage manager container

1. Select the storage manager for Snapstor and click the  button to add a container.
2. Complete the properties of the storage manager container:
  - a. **Storage container name.**
  - b. **Deduplication domain.** A new domain can be created, by clicking the  button.
  - c. **Archiving run lock.** A new one can be created, by clicking the  button.
  - d. **Threads.** Number of threads the storage manager container can manage. Select a numeric value from 1 to 128. When selecting the number of threads, take into account the data mover capacity.
3. Select the directory where the data are archived on the storage manager. This is an absolute path.
4. Configure stream options.
5. Set export share options to be able to remotely access the archived data on a SnapStor storage through several SMB shares and /or NFS exports. When used in an archiving or backup task, SMB shares or NFS exports are created on the storage if they exist on the host source. Permissions applied on the created SMB shares or NFS exports are the same permissions than those used by the SMB shares or NFS exports on the task source host.
6. Set a prefix if you want to define how the files are organized on the storage manager container (i.e., what are their paths on the disk).

- Click **Create** to add the storage manager container.

## Virtual Storage

### Step 1: Add a storage manager

- Click the **Infrastructure** tab, then **Object Storage & Application**.
- Click **New storage manager**.
- Select **Virtual Storage** and click **Next**.
- Enter the name of the storage manager.
- Choose the appropriate status:
  - Online** Default value if you want to perform an archiving.

**Or**

  - Suspended** This status is useful for maintenance operations.
- Select the operating mode:
  - Load balancing** The archived data are distributed among several storage manager containers to achieve better performance. When enabled, the storage manager container used for archiving is a logical container composed of several physical containers.

**Or**

  - Failover** The archived data are sent to the backup storage manager containers if the primary container fails. When enabled, the storage manager container used for archiving is a logical container composed of several physical containers.
- Click **Create** to add the storage manager.

### Step 2: Add a storage manager container

- Select the storage manager for File Storage and click the **+** button to add a container.
- Complete the properties of the storage manager container:
  - Storage container name.**
  - Deduplication domain.** A new domain can be created, by clicking the **+** button.
  - Archiving run lock.** A new one can be created, by clicking the **+** button.
- Click **Add container** to select a storage manager container from the list. Then click **Add**.
- Click **Create** to add the storage manager container.

## Media Storage

To add a storage manager for a media (Media Manager or Optical Disk Archive), you must create the application in Miria Administration console. See also Creating a Media Manager Application in the Administration documentation.

### Step 1: Add a storage manager

- Click the **Infrastructure** tab, then **Object Storage & Application**.
- Click **New storage manager**.
- Select:
  - Media Manager.**

**Or**

- **Optical Disk Archive.**
4. Click **Next**.
  5. Enter the name of the storage manager.
  6. Choose the appropriate status:
    - **Online** Default value if you want to perform an archiving.
  - Or**
  - **Suspended** This status is useful for maintenance operations.
  7. Select the application to be linked to this storage manager.
  8. Select a user or group that will be notified by email when a response to a media request is needed. This can be the case when an archiving job requires a scratch media, or a retrieval job requires media that are offline or in prevent use mode.
  9. If needed, set volume management. This option enables volumes to trigger the configuration and activation of retention. See also [Recycling Triggered by Volume on Storage](#).
    - Set a High Water Mark value in GB.
    - Set a Task High Water Mark in GB only if you want to activate scheduled monitoring.
    - Set a Low Water Mark in GB.
  10. Click **Create** to add the storage manager.

### Step 2: Add a storage manager container

1. Select the storage manager for Media Manager and click the **+** button to add a container.
2. Complete the properties of the storage manager container:
  - a. **Storage container name.**
  - b. **Deduplication domain.** A new domain can be created, by clicking the **+** button.
  - c. **Archiving run lock.** A new one can be created, by clicking the **+** button.
  - d. **Threads.** (*Media Manager only*) Number of threads the storage manager container can manage. Select a numeric value from 1 to 128. When selecting the number of threads, take into account the data mover capacity.
3. Select a library in which Miria stores the archived data.
4. Select a media type only if the library may contain media of several types (e.g., LTO-6 and LTO-7). You can check **Show only WORM media** to display only the WORM media and choose one.
5. Select a scratch media group in which the media needed for archiving is selected. One media group (default) is created automatically and selected by default. This parameter is mandatory if you do not specify a library.
6. Select a barcode. By default, the first blank or scratch media available in the scratch media group is selected. Use the wildcard characters \*, ?, and | to compare the barcodes of the media.

#### Examples:

- A005?? selects any media with a six character barcode beginning with the string A005. You might use this, for example, to select media from A00500 to A00599.
- \*L4 selects any media with a barcode ending in L4. You might use this, for example, to select only media of LTO4 type.
- 162\*|WV\* selects any media with barcode beginning either with the string 162, or with the string WV.



7. Set a media rule.
8. *(Media Manager only)* Specify the media format.
9. Set the digest type. This ensures that the object you retrieve has not been modified on the storage and that it is identical to the object that was archived.

The more complex the hash, the slower the calculation times. A complex hash decreases performance. It is recommended to use SHA-256 for the best compromise between performance and security.

10. Set other configuration options:
  - **Metadata** The metadata associated with the archived object are sent as URL encoded strings. You can send only up to 2 KB of metadata. A log indicates the skipped metadata above 2 KB.
  - **Prevent spanning** Prevent an archived file from being written on a media if it is too large to fit the remaining space.
  - **Custom block size** By default, the media is subdivided into blocks of 128 KB. The block size must be a multiple of 16. The maximum size accepted is 4 MB.
  - **Log level** Set the level of the logs that are displayed.
  - *Also for Optical disk archive* Choose whether to set Pack write and the format of the media.
11. *(Media Manager only)* Set LTFS delivery protocols. If you do not have to comply with specific protocols, do not modify the default parameters.
12. Set a prefix if you want to define how the files are organized on the storage manager container (i.e., what are their paths on the disk).
13. Click **Create** to add the storage manager container.

## Easy move Amazon S3

Amazon Simple Storage Service (S3) is an Internet storage solution designed to make web-scale computing easier for customers.

Details of what is replicated in S3 are described in the appendix: [Replications in between two S3 object storages](#) ".

### Step 1: Add a storage manager

1. Click the **Infrastructure** tab, then **Object Storage & Application**.
2. Click **New storage manager**.
3. Select **Amazon S3** and click **Next**.
4. Enter the name of the storage manager.
5. Choose the appropriate status:
  - **Online** Default value if you want to perform an archiving.

**Or**

  - **Suspended** This status is useful for maintenance operations.
6. Enter the network address of the Amazon S3 storage service (e.g., S3.amazonaws.com).
7. If needed, set a default proxy platform. This platform handles the data movement on behalf of the usual agent or agents pool.
8. Set storage manager options:
  - **HTTP Proxy** Enables the Proxy HTTP to communicate with a remote S3 storage.



- **Transfer acceleration** Sends data to the nearest Amazon S3 node and acknowledges reception. Then, Amazon S3 sends the data to the actual final destination.
9. If needed, set volume management. This option enables volumes to trigger the configuration and activation of retention. See also [Recycling Triggered by Volume on Storage](#).
    - Set a High Water Mark value in GB.
    - Set a Task High Water Mark in GB only if you want to activate scheduled monitoring.
    - Set a Low Water Mark in GB.
  10. Click **Create** to add the storage manager.

### **Step 2: Add a storage manager container**

1. Select the Amazon S3 storage manager and click the **+** button to add a container.
2. Complete the properties of the storage manager container:
  - a. **Storage container name.**
  - b. **Deduplication domain.** A new domain can be created, by clicking the **+** button.
  - c. **Archiving run lock.** A new one can be created, by clicking the **+** button.
  - d. **Threads.** Number of threads the storage manager container can manage. Select a numeric value from 1 to 128. When selecting the number of threads, take into account the data mover capacity.
  - e. **Available as source.** If needed, make the storage manager container available as source. Then enter the name you want to give to the platform associated.
3. Enter Amazon S3 account information:
  - a. **Access Key ID** String that uniquely identifies the Amazon S3 account.
  - b. **Secret Access Key** Password associated with the Access Key ID
  - c. **Bucket name** Logical path under which the data are stored into the Amazon S3 storage. Refer to your Amazon S3 storage configuration.
4. Set the digest type. This ensures that the object you retrieve has not been modified on the storage and that it is identical to the object that was archived.
5. Set the data compression value. This specifies whether the data must be compressed in the storage and defines the compression type.
6. Choose whether to activate metadata. The metadata associated with the archived object are sent as URL encoded strings. You can send only up to 2 KB of metadata. A log indicates the skipped metadata above 2 KB.
7. Choose whether to activate MD5 checksum on the S3 archiving transfer.
8. Set the retention mode for object lock. See also Data Immutability with S3 Object Lock in Administration documentation.
  - **Governance mode** Users with specific Identity and Access Management (IAM) permissions can overwrite or delete protected object versions during the retention period.

**Or**

  - **Compliance mode** No users can overwrite or delete protected object versions during the retention period. To delete objects that have this configuration, you must close the account that they are associated with.
9. Set lifecycle rules and complete following information accordingly:

- a. **Name** Name of the life cycle rule that defines the data migration. This name is any unique string of your choice (e.g., ada\_smc\_amazon, RuleForArchiving, 1toglacier\_200todelete, etc.). When you launch the first job, Miria uses this name to create a rule on the Amazon S3 bucket.
  - b. **Transition days** Number of days at the end of which Amazon S3 will transfer the objects to Glacier or Deep Archive. By default, Amazon S3 performs the transfer at 00:00 the same day. A value of 1 indicates that the transfer is performed at 00:00 the next day, and so on.
  - c. **Retrieval mode** Define the retrieval mode between standard, bulk and expedited. See also [AWS documentation](#).
  - d. **Copy lifetime** Number of copy lifetime.
10. Set a prefix if you want to define how the files are organized on the storage manager container (i.e., what are their paths on the disk).
  11. Click **Create** to add the storage manager container.

## Google Cloud Storage

Google Cloud Storage is an Internet storage solution designed to make web-scale computing easier for customers.

The integration between Miria and the Google Cloud Storage technology enables you to store data into a Google Cloud Storage compatible storage.


### Step 1: Add a storage manager

1. Click the **Infrastructure** tab, then **Object Storage & Application**.
2. Click **New storage manager**.
3. Select **Google Cloud Storage** and click **Next**.
4. Enter the name of the storage manager.
5. Choose the appropriate status:
  - **Online** Default value if you want to perform an archiving.

**Or**

  - **Suspended** This status is useful for maintenance operations.
6. If needed, set a default proxy platform. This platform handles the data movement on behalf of the usual agent or agents pool.
7. If needed, set volume management. This option enables volumes to trigger the configuration and activation of retention. See also [Recycling Triggered by Volume on Storage](#).
  - Set a High Water Mark value in GB.
  - Set a Task High Water Mark in GB only if you want to activate scheduled monitoring.
  - Set a Low Water Mark in GB.
8. Click **Create** to add the storage manager.

### Step 2: Add a storage manager container

1. Select the storage manager for Google Cloud Storage and click the  button to add a container.
2. Complete the properties of the storage manager container:
  - a. **Storage container name**.

- b. **Deduplication domain.** A new domain can be created, by clicking the **+** button.
  - c. **Archiving run lock.** A new one can be created, by clicking the **+** button.
  - d. **Threads.** Number of threads the storage manager container can manage. Select a numeric value from 1 to 128. When selecting the number of threads, take into account the data mover capacity.
  - e. **Available as source.** If needed, make the storage manager container available as source. Then enter the name you want to give to the platform associated.
3. Enter the Google Cloud Storage account information:
  - a. **Authentication File** Select the JSON key of your Google Cloud Storage service account. Keep the JSON file carefully, it cannot be retrieved from Miria because it is encrypted. See also Generate a Google Cloud JSON key in Administration documentation.
  - b. **Bucket Name** Unique name of the bucket that Miria will create in Google Cloud to store the files.
4. Set the digest type. This ensures that the object you retrieve has not been modified on the storage and that it is identical to the object that was archived.
5. Set the data compression value. This specifies whether the archived data must be compressed in the storage and defines the compression type.
6. Choose whether to activate metadata. The metadata associated with the archived object are sent as URL encoded strings. You can send only up to 2 KB of metadata. A log indicates the skipped metadata above 2 KB.
7. Choose whether to activate MD5 checksum on the S3 archiving transfer.
8. Set lifecycle rules:
  - Click the **+** button to add a new rule. Then enter the number of days at the end of which GCS will transfer the objects. By default, GCS performs the transfer at 00:00 the same day. A value of 1 indicates that the transfer is performed at 00:00 the next day, and so on.
  - If no rules are defined, Miria will use the GCS Standard Storage Class.
9. Set a prefix if you want to define how the files are organized on the storage manager container (i.e., what are their paths on the disk).
10. Click **Create** to add the storage manager container.

## Microsoft Azure Blob Block

Microsoft Azure Blob Block is an Internet storage solution designed to make web-scale computing easier for customers.

The integration between Miria and the Microsoft Azure Blob Block technology enables you to store data into a Microsoft Azure Blob Block cloud compatible storage (REST interface).




### **Step 1: Add a storage manager**

1. Click the **Infrastructure** tab, then **Object Storage & Application**.
2. Click **New storage manager**.
3. Select **Microsoft Azure Blob Block** and click **Next**.
4. Enter the name of the storage manager.
5. Choose the appropriate status:
  - **Online** Default value if you want to perform an archiving.

Or

- **Suspended** This status is useful for maintenance operations.
6. Enter the network address of the Microsoft Azure Blob Block storage service (e.g., AZURE-ACCOUNT.blob.core.windows.net).
  7. If needed, set a default proxy platform. This platform handles the data movement on behalf of the usual agent or agents pool.
  8. Enable **HTTP Proxy** to be able to communicate with a remote S3 storage.
  9. Configure an alternative access if you want to add multiple storage manager accesses.
  10. If needed, set volume management. This option enables volumes to trigger the configuration and activation of retention. See also [Recycling Triggered by Volume on Storage](#).
    - Set a High Water Mark value in GB.
    - Set a Task High Water Mark in GB only if you want to activate scheduled monitoring.
    - Set a Low Water Mark in GB.
  11. Click **Create** to add the storage manager.

### **Step 2: Add a storage manager container**

1. Select the Microsoft Azure Blob Block storage manager and click the  button to add a container.
2. Complete the properties of the storage manager container:
  - a. **Storage container name.**
  - b. **Deduplication domain.** A new domain can be created, by clicking the  button.
  - c. **Archiving run lock.** A new one can be created, by clicking the  button.
  - d. **Threads.** Number of threads the storage manager container can manage. Select a numeric value from 1 to 128. When selecting the number of threads, take into account the data mover capacity.
  - e. **Available as source.** If needed, make the storage manager container available as source. Then enter the name you want to give to the platform associated.
3. Enter the Microsoft Azure Blob Block account information:
  - a. **Account name** String that uniquely identifies the Microsoft Azure Blob Block account.
  - b. **Access Key** Key associated with the Account Name. This key can be retrieved from the Account page via Settings > Access Key menu.
  - c. **Container name** Unique name of the container created by Miria in Microsoft Azure Blob Block and where Miria stores the files.
4. Set an access tier for data storage:
  - **Hot** Store data that is accessed frequently.
  - **Cool** Store data that is infrequently accessed and stored for at least 30 days.
  - **Archive** Store data that is rarely accessed and stored for at least 180 days with flexible latency requirements, on the order of hours.
5. Set the digest type. This ensures that the object you retrieve has not been modified on the storage and that it is identical to the object that was archived.
6. Set the data compression value. This specifies whether the archived data must be compressed in the storage and defines the compression type.

7. Choose whether to activate metadata. The metadata associated with the archived object are sent as URL encoded strings. You can send only up to 2 KB of metadata. A log indicates the skipped metadata above 2 KB.
8. Choose whether to activate MD5 checksum on the S3 archiving transfer.
9. Set a prefix if you want to define how the files are organized on the storage manager container (i.e., what are their paths on the disk).
10. Click **Create** to add the storage manager container.

## Scality

When you add a Scality Object Storage, you have to complete the following steps:

### Step 1: Add a storage manager

1. Click the **Infrastructure** tab, then **Object Storage & Application**.
2. Click **New storage manager**.
3. Select **Scality** and click **Next**.
4. Enter the name of the storage manager.
5. Choose the appropriate status:
  - **Online** Default value if you want to perform an archiving.

Or

- **Suspended** This status is useful for maintenance operations.
6. **Default Network Address.** Network Address of the Scality storage service.

You can specify several network addresses so that Miria can connect to another node if the first node is not available.

You must enter the node network addresses, separated by semi-colons, without spaces in between (e.g., `S3-SM.archives.atempo.com;128.221.200.56;128.221.200.57`).

Each node may use one of these syntaxes:

- `<name>` or `<address>`  
Miria uses a non-secure connection (HTTP, with the default port `80`) to the node.
- `<name>:s` or `<address>:s`  
Miria uses a secure connection (HTTPS, with the default port `443`) to the node.
- `<name>:<port_number>` or `<address>:<port_number>`  
Miria uses a non-secure connection (HTTP) with a specific port number.
- `<name>:<port_number>s` or `<address>:<port_number>s`  
Miria uses a secure connection (HTTPS) with a specific port number.

These four lines are examples of a network address:

- `s3.scality.com`
- `s3.scality.com:s`
- `s3.scality.com:1523s`
- `s3.scal1;s3.scal2:s;s3.scal3:1523s`




7. **Default proxy platform** This platform handles the data movement on behalf of the usual agent or agents pool.

Choose the proxy platform to be used by default.

8. **Alternative access** Configure it if you want to add multiple storage manager accesses.

9. **Volume management** This option enables volumes to trigger the configuration and activation of retention. See also Recycling Triggered by Volume on Storage.
  - Set a High Water Mark value in GB.
  - Set a Task High Water Mark in GB only if you want to activate scheduled monitoring.
  - Set a Low Water Mark in GB.
10. Click **Create** to add the storage manager.

### Step 2: Add a storage manager container

1. Select the storage manager for Scalify and click the  button to add a container.
2. Complete the properties of the storage manager container:
  - a. **Storage container name**
  - b. **Deduplication domain** A new domain can be created, by clicking the  button.
  - c. **Archiving run lock** A new one can be created, by clicking the  button.
  - d. **Threads** Number of threads the storage manager container can manage. Select a numeric value from 1 to 128. When selecting the number of threads, take into account the data mover capacity.
  - e. **Available as source** If you select this option, you have to enter the name of the platform associated to the storage manager container.
3. Set the configuration of the storage manager container:
  - a. **Access Key ID** String that uniquely identifies the Scalify account.
  - b. **Secret Access Key** Password associated with the Access Key ID.
  - c. **Bucket name** Logical path under which the data are stored into the Scalify storage. Refer to your Scalify storage configuration.
  - d. **Digest on storage** This ensures that the object you retrieve has not been modified on the storage and that it is identical to the object that was archived. The more complex the hash, the slower the calculation times. A complex hash decreases performance. It is recommended to use SHA-256 for the best compromise between performance and security.
  - e. **Data compression** This specifies whether the data must be compressed in the storage and defines the compression type.
  - f. **Metadata** Choose whether to activate metadata. The metadata associated with the archived object are sent as URL encoded strings. You can send only up to 2 KB of metadata. A log indicates the skipped metadata above 2 KB.
  - g. **MD5 checksum** Choose whether to activate MD5 checksum on the S3 archiving transfer.
4. Set the retention mode on the object lock. If you enable it, you have two options:
  - a. **Enable governance mode** Users with specific Identity and Access Management (IAM) permissions can overwrite or delete protected object versions during the retention period.
  - b. **Enable compliance mode** No users can overwrite or delete protected object versions during the retention period. To delete objects that have this configuration, you must close the account that they are associated with.
5. Set a prefix if you want to define how the files are organized on the storage manager container (i.e., what are their paths on the disk).
6. Click **Create** to add the storage manager container.



## Quantum Active Scale

When you add a Quantum ActiveScale Object Storage, you have to complete the following steps:

### Step 1: Add a storage manager

1. Click the **Infrastructure** tab, then **Object Storage & Application**.
2. Click **New storage manager**.
3. Select **Quantum ActiveScale** and click **Next**.
4. Enter the name of the storage manager.
5. Choose the appropriate status:
  - **Online** Default value if you want to perform an archiving.

Or

- **Suspended** This status is useful for maintenance operations.
6. **Network Address** Network Address of the Quantum Active Scale storage service.

You can specify several network addresses so that Miria can connect to another node if the first node is not available.

You must enter the node network addresses, separated by semi-colons, without spaces in between (e.g., `S3-AS.archives.atempo.com;128.221.200.56;128.221.200.57`).

Each node may use one of these syntaxes:

- `<name>` or `<address>`  
Miria uses a non-secure connection (HTTP, with the default port `80`) to the node.
- `<name>:s` or `<address>:s`  
Miria uses a secure connection (HTTPS, with the default port `443`) to the node.
- `<name>:<port_number>` or `<address>:<port_number>`  
Miria uses a non-secure connection (HTTP) with a specific port number.
- `<name>:<port_number>s` or `<address>:<port_number>s`  
Miria uses a secure connection (HTTPS) with a specific port number.

These four lines are examples of a network address:

- `s3.activescale.com`
- `s3.activescale.com:s`
- `s3.activescale.com:1523s`
- `s3.qsa1;s3.qsa2:s;s3.qsa3:1523s`




7. **Default proxy platform** This platform handles the data movement on behalf of the usual agent or agents pool.

Choose the proxy platform to be used by default.

8. **Connection settings** Select an HTTP REST IP rule; whether Round-robin DNS or TCP/IP latency.
9. **Alternative access** Configure it if you want to add multiple storage manager accesses.
10. **Volume management** This option enables volumes to trigger the configuration and activation of retention. See also Recycling Triggered by Volume on Storage.
  - Set a High Water Mark value in GB.
  - Set a Task High Water Mark in GB only if you want to activate scheduled monitoring.
  - Set a Low Water Mark in GB.

11. Click **Create** to add the storage manager.

### **Step 2: Add a storage manager container**

1. Select the storage manager for Quantum ActiveScale and click the  button to add a container.
2. Complete the properties of the storage manager container:
  - a. **Storage container name.**
  - b. **Deduplication domain** A new domain can be created, by clicking the .
  - c. **Archiving run lock** A new one can be created, by clicking the .
  - d. **Threads.** Number of threads the storage manager container can manage. Select a numeric value from 1 to 128. When selecting the number of threads, take into account the data mover capacity.
  - e. **Available as source** If you select this option, you have to enter the name of the platform associated to the storage manager container.
3. Set the configuration of the storage manager container:
  - a. **Access Key ID** String that uniquely identifies the Quantum ActiveScale account.
  - b. **Secret Access Key** Password associated with the Access Key ID.
  - c. **Bucket name** Logical path under which the data are stored into the Quantum ActiveScale storage. Refer to your Quantum ActiveScale storage configuration.
  - d. **Digest on storage** This ensures that the object you retrieve has not been modified on the storage and that it is identical to the object that was archived. The more complex the hash, the slower the calculation times. A complex hash decreases performance. It is recommended to use SHA-256 for the best compromise between performance and security.
  - e. **Data compression** This specifies whether the data must be compressed in the storage and defines the compression type.
  - f. **Metadata** Choose whether to activate metadata. The metadata associated with the archived object are sent as URL encoded strings. You can send only up to 2 KB of metadata. A log indicates the skipped metadata above 2 KB.
4. **Object lock** Set the retention mode on the object lock. If you enable it, see Data Immutability with S3 Object Lock in Administration documentation.
  - a. **Enable compliance mode** No users can overwrite or delete protected object versions during the retention period. To delete objects that have this configuration, you must close the account that they are associated with.
5. **Lifecycle rules** Set them and complete following information accordingly:
  - a. **Name** Name of the Lifecycle rule that defines the data migration. This name is any unique string of your choice (e.g., ada\_smc\_amazon, RuleForArchiving, 1toglacier\_200todelete, etc.). When you launch the first job, Miria uses this name to create a rule on the Quantum ActiveScale bucket.
  - b. **Transition days** Number of days at the end of which Quantum ActiveScale will transfer the objects to Glacier or Deep Archive. By default, Quantum ActiveScale performs the transfer at 00:00 the same day. A value of 1 indicates that the transfer is performed at 00:00 the next day, and so on.
  - c. **Retrieval copy lifetime** Number of retrieval copy lifetime.
6. Set a prefix if you want to define how the files are organized on the storage manager container (i.e., what are their paths on the disk).



- Click **Create** to add the storage manager container.

## Seagate Lyve Cloud

When you add a Lyve Cloud Object Storage, you have to complete the following steps:

### Step 1: Add a storage manager

- Click the **Infrastructure** tab, then **Object Storage & Application**.
- Click **New storage manager**.
- Select **Seagate Lyve Cloud** and click **Next**.
- Enter the name of the storage manager.
- Choose the appropriate status:
  - Online** Default value if you want to perform an archiving.

Or

- Suspended** This status is useful for maintenance operations.
- Default Network Address.** Enter the network address of the Lyve Cloud storage service.

You can specify several network addresses so that Miria can connect to another node if the first node is not available.

You must enter the node network addresses, separated by semi-colons, without spaces in between (e.g., `S3-SM.archives.atempo.com;128.221.200.56;128.221.200.57`).

Each node may use one of these syntaxes:

- `<name>` or `<address>`  
Miria uses a non-secure connection (HTTP, with the default port `80`) to the node.
- `<name>:s` or `<address>:s`  
Miria uses a secure connection (HTTPS, with the default port `443`) to the node.
- `<name>:<port_number>` or `<address>:<port_number>`  
Miria uses a non-secure connection (HTTP) with a specific port number.
- `<name>:<port_number>s` or `<address>:<port_number>s`  
Miria uses a secure connection (HTTPS) with a specific port number.

These four lines are examples of a network address:

- `s3.lyvecloud.com`
- `s3.lyvecloud.com:s`
- `s3.lyvecloud.com:1523s`
- `s3.lvc1;s3.lvc2:s;s3.lvc3:1523s`




- Default proxy platform.** This platform handles the data movement on behalf of the usual agent or agents pool.

Click Select the up and down arrow to choose the proxy platform to be used by default.

- Alternative access** Configure this pane if you want to add multiple storage manager accesses.
- Volume management** This option enables volumes to trigger the configuration and activation of retention. See also Recycling Triggered by Volume on Storage.
  - Set a High Water Mark value in GB.
  - Set a Task High Water Mark in GB only if you want to activate scheduled monitoring.
  - Set a Low Water Mark in GB.

10. Click Create to add the storage manager.

### Step 2: Add a storage manager container

1. Select the storage manager for Lyve Cloud and click the  button to add a container.
2. Complete the properties of the storage manager container:
  - a. **Storage container name.**
  - b. **Deduplication domain.** A new domain can be created, by clicking the  button.
  - c. **Archiving run lock.** A new one can be created, by clicking the  button.
  - d. **Threads.** Number of threads the storage manager container can manage. Select a numeric value from 1 to 128. When selecting the number of threads, take into account the data mover capacity.
  - e. **Available as source.** If you select this option, you have to enter the name of the platform associated to the storage manager container.
3. Set the configuration of the storage manager container:
  - a. **Access Key ID** String that uniquely identifies the Seagate Lyve Cloud account.
  - b. **Secret Access Key** Password associated with the Access Key ID.
  - c. **Bucket name** Logical path under which the data are stored into the Seagate Lyve Cloud storage. Refer to your Seagate Lyve Cloud storage configuration.
  - d. **Digest on storage** This ensures that the object you retrieve has not been modified on the storage and that it is identical to the object that was archived. The more complex the hash, the slower the calculation times. A complex hash decreases performance. It is recommended to use SHA-256 for the best compromise between performance and security.
  - e. **Data compression** This specifies whether the data must be compressed in the storage and defines the compression type.
  - f. **Metadata** Choose whether to activate metadata. The metadata associated with the archived object are sent as URL encoded strings. You can send only up to 2 KB of metadata. A log indicates the skipped metadata above 2 KB.
  - g. **MD5 checksum**
4. Set the retention mode on the object lock. If you enable it, you have two options:
  - a. **Enable governance mode** Users with specific Identity and Access Management (IAM) permissions can overwrite or delete protected object versions during the retention period.
  - b. **Enable compliance mode** No users can overwrite or delete protected object versions during the retention period. To delete objects that have this configuration, you must close the account that they are associated with.
5. Set a prefix if you want to define how the files are organized on the storage manager container (i.e., what are their paths on the disk).
6. Click **Create** to add the storage manager container.

## Cloudian HyperStore

Cloudian HyperStore is an Internet storage solution designed to resolve your storage issues. Create HyperStore nodes wherever you need more storage.

**Step 1: Add a storage manager**

1. Click the **Infrastructure** tab, then **Object Storage & Application**.
2. Click **New storage manager**.
3. Select **Cloudian HyperStore** and click **Next**.
4. Enter the name of the storage manager.
5. Choose the appropriate status:
  - **Online** Default value if you want to perform an archiving.**Or**
  - **Suspended** This status is useful for maintenance operations.
6. Enter the network address of the Cloudian HyperStore service (e.g., `cloudian.hyperstore.myS3storage.com`).
7. If needed, set a default proxy platform. This platform handles the data movement on behalf of the usual agent or agents pool.
8. Set the **connection settings** Select an HTTP REST IP rule; whether Round-robin DNS or TCP/IP latency.
9. Set the **Alternative access**. Configure it if you want to add multiple storage manager accesses.
10. If needed, set volume management. This option enables volumes to trigger the configuration and activation of retention. See also [Recycling Triggered by Volume on Storage](#).
  - Set a High Water Mark value in GB.
  - Set a Task High Water Mark in GB only if you want to activate scheduled monitoring.
  - Set a Low Water Mark in GB.
11. Click **Create** to add the storage manager.

**Step 2: Add a storage manager container**

1. Select the Cloudian HyperStore storage manager and click the **+** button to add a container.
2. Complete the properties of the storage manager container:
  - a. **Storage container name**.
  - b. **Deduplication domain**. A new domain can be created, by clicking the **+** button.
  - c. **Archiving run lock**. A new one can be created, by clicking the **+** button.
  - d. **Threads**. Number of threads the storage manager container can manage. Select a numeric value from 1 to 128. When selecting the number of threads, take into account the data mover capacity.
  - e. **Available as source**. If needed, make the storage manager container available as source. Then enter the name you want to give to the platform associated.
3. Complete the Cloudian HyperStore account configuration:
  - a. **Access Key ID** String that uniquely identifies the Cloudian HyperStore account.
  - b. **Secret Access Key** Password associated with the Access Key ID
  - c. **Bucket name** Logical path under which the data are stored into the Cloudian HyperStore storage. Refer to your Cloudian HyperStore storage configuration.
4. Set the digest type. This ensures that the object you retrieve has not been modified on the storage and that it is identical to the object that was archived.
5. Set the data compression value. This specifies whether the data must be compressed in the storage and defines the compression type.

6. Choose whether to activate metadata. The metadata associated with the archived object are sent as URL encoded strings. You can send only up to 2 KB of metadata. A log indicates the skipped metadata above 2 KB.
7. Choose whether to activate MD5 checksum on the S3 archiving transfer.
8. Set the retention mode for object lock. See also Data Immutability with S3 Object Lock in Administration documentation.
  - **Enable governance mode** Users with specific Identity and Access Management (IAM) permissions can overwrite or delete protected object versions during the retention period.
- Or**
- **Enable compliance mode** No users can overwrite or delete protected object versions during the retention period. To delete objects that have this configuration, you must close the account that they are associated with.
9. Set a prefix if you want to define how the files are organized on the storage manager container (i.e., what are their paths on the disk).
10. Click **Create** to add the storage manager container.

**Note:** At object level, legal hold flag is not available.

## Add Server and Agent(s)

The infrastructure is composed of a server and agent(s). The server manages all the data movers and can be installed on a dedicated physical or virtual machine.

An agent can be:

- A data mover.
- A source or target platform.

You need to manually add installed agent(s) to be able to select them when setting up the migration.


### *To add an agent*

1. Click on **Infrastructure** tab, then the **Agent** tile. The list of agents and agent pools is displayed.
2. In the top right corner, click **Add** and select **New Agent**.
3. In the **Choose Agents to add** window, select agent(s) you want to add.
4. Click **Add Agents**.

### *To add an agent pool*

An agent pool is a logical grouping of several agents. To create an agents pool, you must first declare each agent.

1. Click on **Infrastructure** tab, then the **Agent** tile. The list of agents and pools is displayed.
2. In the top right corner, click **Add** and select **New Pool**.
3. Enter a name for your pool.
4. Select the protocol linked to the agent used.
5. Choose the agents you want to add.

6. Click **Create**. The agents pool is added to the list.
7. To edit an agents pool, select it from the list and click the  button.

## Add a New NAS Platform

NAS platforms allow you to add the source and target for your migration. For an example, see also [Configure an Isilon Storage](#).

### Step 1: Connection

1. Click the **Infrastructure** tab, then the **NAS** tile. The list of NAS platforms is displayed.
2. In the top right corner, click **Add NAS**.

### Step 2: Configuration

1. Choose the type of NAS (Isilon, Qumulo, etc.) or **Other** for standard CIFS/NFS file servers.
2. For Isilon, Nutanix, OceanStor and Qumulo, activate **Advanced Storage Integration** to enable Snapshot and FastScan.
3. Select the protocol relating to the agent: CIFS or NFS.
4. In the **Datamovers** section, select the agent used for the data movement.
5. Click **Next**.

### Step 3 : Advanced Storage Integration (optional)

**Note:** If you choose Isilon, Nutanix, OceanStor or Qumulo and have activated **Advanced Storage Integration**, one more step is available.

1. In the **Network** section, enter the NAS API credentials. Fields vary depending on the type of NAS.
2. If needed, check **Ignore SSL Check Certificate**.
3. (Nutanix only) Enter the CVM server information.
4. If needed, in the **Options** section, enable **Snapshot**.
5. If needed, enable **FastScan**, enter the maximum number of FastScan and choose if you want to use regular scanning if the last snapshot is missing. Check the following list for the maximum number of FastScan operations (parallel operations) recommended per NAS:
  - Isilon: 3
  - Nutanix: 10
  - OceanStor: 32
  - Qumulo: No limit
6. Click **Next**.

### Step 4: Options and summary

1. In the **Stream Option** section, you can enter stream options depending on the platform type.
2. Click **Next**.
3. Read the **Summary** of the NAS.
4. Enter the name of the NAS.

5. If you chose CIFS protocol, enter the user name and the password of your windows account.
6. Click **Add NAS**.

## Add a Storage Platform

You can declare an archiving platform to use a cloud or an object storage offering access as a source. To create such a platform, you must configure a storage manager and storage manager container.

The storage manager is the storage definition, which can be tape, cloud (e.g., AWS, Google), disk and object storage. The storage manager container is the path to the data of the storage manager (e.g., Bucket name, etc.).

The option **Available as source** can be enabled for certain platforms when configuring the storage manager container. See also [Add a Storage Manager and Container](#).

### *To add a storage platform:*

1. Click the **Infrastructure** tab, then the **Storage** tile. The list of storage platforms is displayed.
2. In the top right corner, click **Add new storage**.
3. Select a storage manager container and click **Next**.
4. Enter the name of the platform associated to the storage manager container.
5. Click **Create**.

## Add a Shared File System

Allows for usage of a shared file system as a source and/or a target for migration.

### **Step 1: Connection**

1. Click the **Infrastructure** tab, the **Shared file system**. The list of shared file systems is displayed.
2. In the top right corner, click **Add new shared file system**.

### **Step 2: Configuration**

1. Choose the type of your Shared File System.
2. (Optional) Enable **Advanced Storage Integration** for Snapshot and FastScan .
3. In the **Datamovers** section, select the agent used for the data movement.
4. Click **Next**.

### **Step 3 : Advanced Storage Integration (optional)**

If you activated **Advanced Storage Integration**, this step is available.

1. If needed, enable **Snapshot**.
2. If needed, enable **FastScan**, enter the maximum number of FastScan and choose if you want to use regular scanning if last snapshot is missing. Check the following list for the

maximum number of FastScan operations (parallel operations) recommended per shared file system:

- GPFS: 10
- Lustre: no limit
- WekaFS
- StorNext

3. Click **Next**.

#### **Step 4: Options and summary**

1. In the **Stream Option** section, you can enter stream options depending on the platform type.
2. Click **Next**.
3. Read the **Summary**.
4. Enter the name of the shared file system.
5. Click **Create**.

## Activate My File System

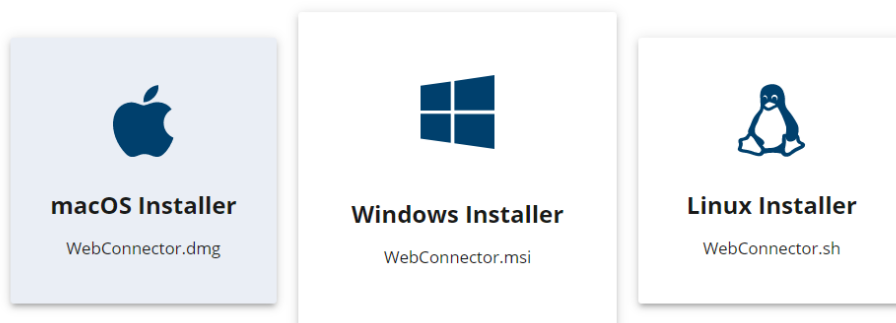
To browse the local file system and perform data-move operations, you need to activate **My file system**. A Web Connector application is used that needs to be installed on your workstation.

The Web Connector is able to handle one request at a time and communicates through port number 8089. You must ensure that this port number is free on your workstation.

#### **Step 1: Download and install the Web Connector**

1. In the Web Interface, click the **Infrastructure** tab.
2. Click the **My file system** card.
  - If the Web Connector has not been installed, download the WebConnector. If you decide to install the Web Connector, follow the procedure.
  - If the Web Connector is already installed, the URL opens in a new tab. You can go directly to step 2.
3. Select and download the installer that matches your operating system ([Figure 8](#)).

To install or update WebConnector, select your operating system below.



Once installed, you can browse My filesystem from the infrastructure menu.

Back to Infrastructure

Figure 8: Installer selection

4. Run the installation.

### Step 2: Verify connection status of My file system

1. Once the WebConnector is installed, click **OK** to go back to the **Infrastructure** page.
2. Click the **My file system** card. The file system can now be explored.
3. Select **My file system** in the **Easy Move** interface as a source or target to perform data-move operations.

## Available options

### Ports Range :

When you have a shared application server, it is not possible for several users to use the same local port, only one user will be able to connect through one port.

Miria enables you to have several users logged all at the same time by using a Ports Range. This means that when you launch Web Connector, the Web browser scans the ports until it finds an available one.

By default, Miria works with TCP port range between 25000 and 26000. The administrator can customize this ports range.

If the administrator set the ports, they all have to be compatible with the Web Connector.

See the Miria's administrator guide for details.


### Timeout :

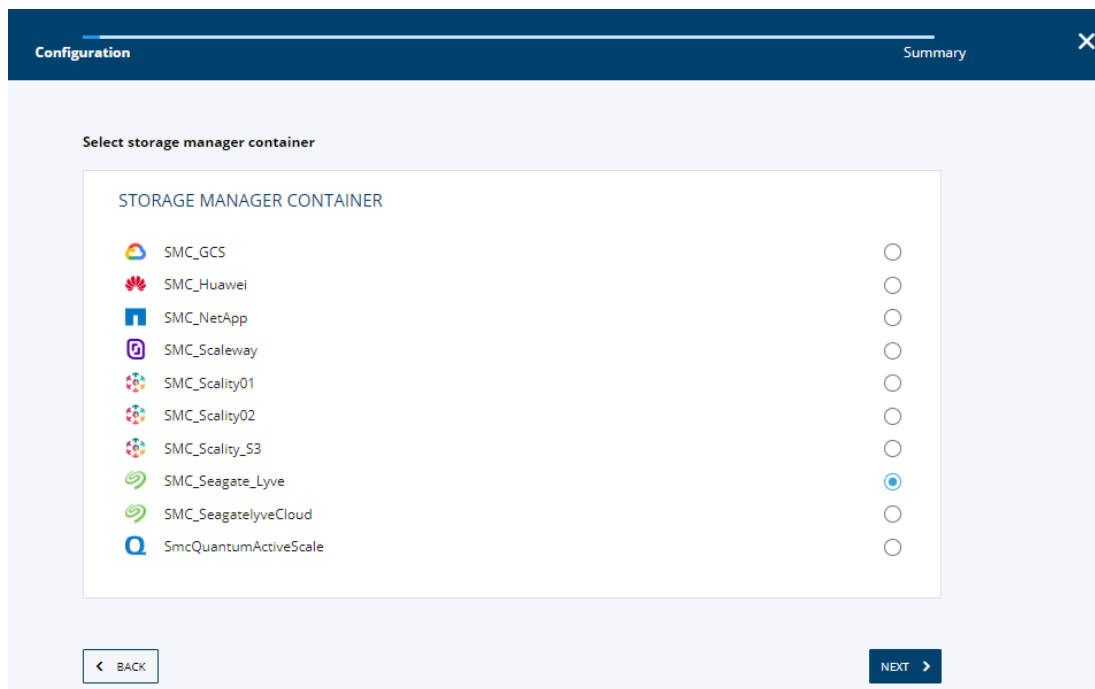
The Web Connector will stop to listen on local port when user disconnects from the Web User Interface or after a timeout on inactivity of 6 hours.



The administrator can change this default timeout. See the Miria's administrator guide for details.

## Edit a Platform

1. Click the **Infrastructure** tab, then select a storage type (e.g., NAS, shared file system)
2. From the list of platforms, click the  button. The current platform configuration is displayed (Figure 9).



**Figure 9:** Example displaying a Nutanix NAS configuration that can be edited in the wizard

3. Update the platform configuration and complete the wizard to save modifications.

## Platforms Permissions

The permissions enable you to grant or deny permissions to individual users, user groups, or overall groups to perform actions on a platform.

You can manage permissions on the following:

- NAS
- Agents
- Storages
- Shared file system

### ***To access to the platforms permissions***

1. Click the **Infrastructure** tab.
2. Select one of the tiles according to which kind of platform you want to set permissions on: either **Agents**, **NAS**, **Storage** or **Shared file system**.  
A list of the platforms appears.

3. Click the  button of one of them and select **Permissions**. Here you have access to all the permissions created.

### ***To create a new permission on a platform***

1. Click the button **+ NEW PERMISSION**. A window appears.
2. Click on the drop down list and select a user or a users group. Click **NEW PERMISSION** to validate.
3. Click **Save changes**.  
The new permission is created, you can now set it.

The interface is divided in two parts:

- **Users and Groups:**  
Lists all the users and groups for which permissions has been created. Select any of them for which you want to set permissions.
- **Permissions:**  
Shows all the available permissions for the corresponding user or users group.

The permissions that you can set, depending on the user or users group, are the following:

- Open
- Add a folder
- Rename an object
- Delete an object
- Move an object
- Copy
- Synchronize

To do so, select each time either **Inherit**, **Deny** or **Allow**. Or select one of those options next to the first line **Apply to all**.

**Note:** The denial of a permission at any level, takes precedence over acceptance. If you select **Inherit**, the values will be those previously set or set by default in the settings. To allow viewing or browsing of a platform, the admin and monitoring rights settings about platforms must also be set to **Monitoring** or **Administration**.

## Metadata

Metadata are descriptive properties associated with files and assets in repositories for the purpose of classifying them and assisting in their retrieval. They are independent from the file's integral properties such as its name, size, or creation date; the Administrator and/or the user must actively define them and associate them with the file.

For more details about the metadata, see section [Manage Metadata](#).


Select the **Parameters** tab, and then the **Metadata** tile to access the Metadata view. It is divided in two parts:

- **Projects.** Enables you to select a folder and organize them. You can create, rename or delete one.
- **Metadata.** Lists all the metadata from the different folders. Here you can edit each one of them.

**To create metadata**

1. Click the **+ NEW METADATA** button at the top right of the metadata view.
2. Complete the appropriate fields ([Table 2](#)) to define the new metadata.
3. Click **NEW METADATA** validate the metadata creation.

**To edit metadata**

1. In the metadata list, click the  button of one of them.  
The **Edit metadata** window opens.
2. You can modify the name, the label, the type, and choose to set it as mandatory or read only (see table).  
If it is already set as read only, you can only modify the field Label.
3. Click **UPDATE METADATA** to save the changes.

The following table describes the fields that you can complete to define a new metadata:

**Table 2:** New metadata settings

Task	Description
<b>Name</b>	<b>Required.</b> Descriptive name of your choosing.
<b>Label</b>	<b>Optional.</b> It enables you to enter a display name for the metadata, which may be different from its Name parameter. When you perform metadata management tasks, such as assigning a metadata value to a repository or running a search, the Label parameter is displayed as the name of the metadata. If Label is not specified, the metadata Name is displayed instead.
<b>Type</b>	Type of metadata. These are the metadata types: <ul style="list-style-type: none"> <li>• <b>Check box.</b> Boolean, for Yes No type values.</li> <li>• <b>Select.</b> Lets you enter a list of values from which the user can make a selection.</li> <li>• <b>String.</b> Lets you enter a free string of characters to find the archived object.</li> <li>• <b>Date.</b> Lets you enter a date to find any archived objects that match it.</li> <li>• <b>Time date.</b> More detailed than the previous type, this type enables you to find any archived objects that match a particular timestamp.</li> <li>• <b>Integer.</b> Lets you enter a number.</li> <li>• <b>Duration.</b> Lets you enter a duration in milliseconds. This type of metadata is useful for media files.</li> <li>• <b>UUID.</b> Lets you enter a Universally Unique Identifier with the xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx format.</li> </ul>
<b>Mandatory</b>	Makes the metadata mandatory. When the box is selected, the user cannot launch an archiving job without setting this metadata.
<b>Read only</b>	If you select this box, users can use only this metadata in searches; they cannot change its value.

## Applying Metadata to Repositories

This discussion assumes that you have already created the repositories.

Once you have created the range of metadata that will be available for use within the Miria instance, you can assign these metadata a value and associate them with repositories, repositories folders, objects, or instances.


You can create associations between metadata and repositories manually, using either of these methods:

- Associate metadata with objects when they are selected.
- Associate metadata with repositories, or with objects and instances that have already been archived.



### *To define setting of metadata values on objects for archiving*

1. Click the **Easy Move** tab.
2. Select a platform or a repository to archive, and a target.
3. Click the **+ADD** button.
4. Click **Validate the basket**.
5. Click **Yes** to validate your basket. A new pop-up appears, enter the values for the metadata that are set as **Mandatory**. You have to complete the Metadata that were set as mandatory. You have to do so every time you perform an archiving.  
See [Metadata](#) to know how to set a metadata on mandatory.

### *To apply metadata to repositories and objects*

1. Select the **Repositories** tab.
2. Click on one of the repositories to open it.
3. Select the repository, or one of the folders or objects in it by clicking the  button.
4. Click **Manage metadata**.
5. Select a metadata and click **ADD**. You can select as many metadata as you want.
6. Select a value for each metadata.
7. Click **Validate** to add them to the repository or to the object(s) selected.

### *To apply metadata to a specific instance of an object*

1. Select the **Repositories** tab.
2. Click on one of the repositories to open it.
3. Click the  button of one of the objects and select **Instance**.  
The list of instances is displayed, ordering by date the past versions of the object.
4. Click an instance  button **Manage metadata**. The manage metadata pane opens. It enables you to view and manage existing metadata on this specific instance, but also to add new metadata.
5. Select metadata in the arborescence and click **ADD** to add a new one.
6. Set a value for each metadata that you add, or change the value of the existing metadata if needed.
7. Click **Validate** to finish the procedure.

# CHAPTER 10 - Organize and Configure the Migration

This chapter outlines how to organize a project and define the tasks within a migration project.

## Organize Projects

Miria is organized by projects. It is possible to manage multiple projects with different tasks within.

### Project description

A project allows to group several tasks together to provide global statistics and management on a migration.

> Access the **Project Overview** by clicking on a project.

The **Project Overview** enables the ability to:

- See the global progress of a migration project.
- Consult information on the tasks inside the project.
- Create a new task.


### Task description

Tasks are automatic jobs that can be scheduled or started manually. A task holds the scope of a Miria job and defines the source and target for migration. In general, a project involves several tasks.

> Access the **Task details** by clicking on a task.

The **Task details** window presents:

- The global progress of a task.
- Information about runs.
- Information about Snapshots.

**Note:** You can obtain a task report. To do so, click the  button of a task run, and select **Download report**.

## Configure the Migration

Once the infrastructure is configured, you can organize the migration. To start a migration, the first step is to create a project and then a set of tasks.

### Create a New Project


1. Connect to the Web Interface.

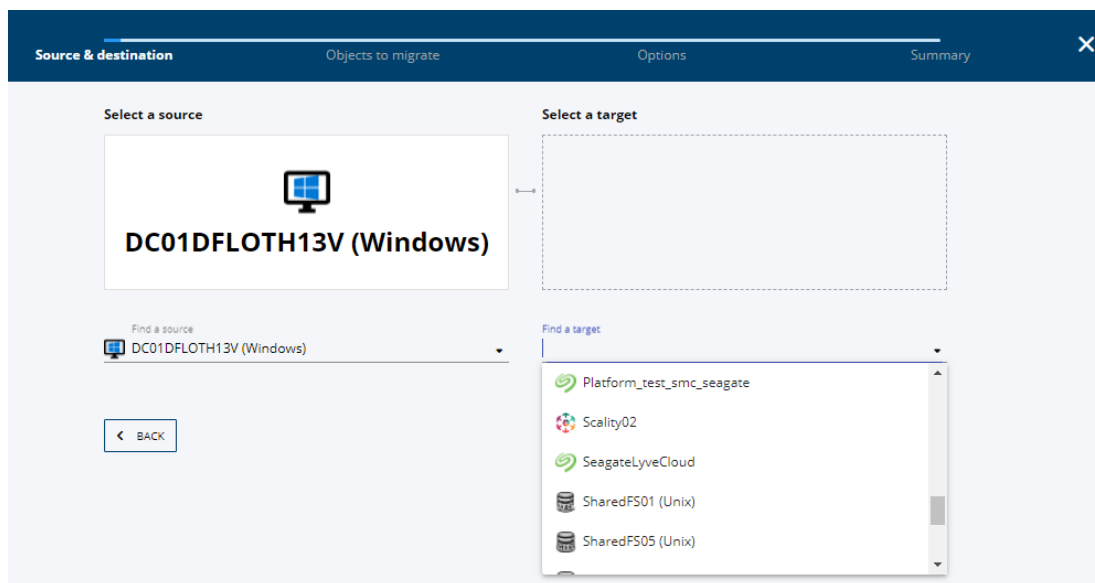
2. In the **Migration** tab, click **New project**.
3. Enter the desired project name and click **New project**

Your project is created.

## Create a New Task

### Step 1: Create a new task

1. Connect to the Web Interface.
2. In the **Migration** tab, select the project to create a task within it.
3. In the upper right corner, select  > **New task**. The task configuration wizard appears [Figure 10](#)



**Figure 10:** The search feature functions as a drop-down menu to select a source and destination

### Step 2: Select a source and a target

1. Select a source.
2. Select a target. Once the migration is finished, the target storage takes over the data protection role. For example, this can be a server, NAS, shared file system, or cloud.
3. Click **Next**.

### Step 3: Migrate objects

1. Select your objects to migrate.
2. Select a target for your objects.
3. Click on **Add**. Repeat this procedure for any additional source and target paths of objects that also require migration.
4. Choose the objects (files and directories) that need to be included or excluded.
5. Click **Next**.

**Step 4: Set additional options**

1. Select the synchronization type required for the workflow: **As Settings**, **Echo**, **Subscribe**, **Contribute**, **Combine**.
2. Set snapshot options. A snapshot is the state of a file system at a particular point in time.
  - **Snapshot** A snapshot of the source directory is taken at the start of the task. This snapshot is then used as the synchronization reference. Any modifications made by the users on the source directory do not impact the synchronization process. The snapshot is used by the current task, and is deleted at the end of the task.
  - **FastScan** The snapshot includes the Snapshot and FastScan features. The snapshot is not deleted at the end of the task. It is used by the next task execution to determine the objects that have changed, and must be archived.
3. To define a schedule, enable **Scheduling**:
  - a. Select the day of the week and the frequency for the task to run.
  - b. Select the hours and minutes of the task to run.
4. To split the current task into multiple tasks, enable **Split tasks**.
5. To activate the multithreading feature, enable **Thread** and write a numerical value from 1 to 128. This parameter sets the maximum number of parallel input / output streams. The higher its value, the better the performance of the source pool when transferring data. The optimum value for the Number of Threads parameter depends on the number of cores available to each of the data movers that make up the source platform pool. To calculate this value, divide by 2 the number of cores of data movers that are part of the pool.

**Example:**

For a pool where each data mover has 8 cores, set this value to 4. For a pool where the number of cores is different between data movers, divide by 2 the number of cores of the data mover with the smallest number of cores. If one of the data movers has 16 cores and another has 32, set this value to 8. The recommended value here is the number of data mover cores divided by two.

6. To parallelize jobs, activate **Jobs Parallelization**. This option enables Miria to accelerate data movements. This is useful for large volumes of data as it allows, for example, the ability to write several files simultaneously on the target file system. By default, the task scans the entire storage to identify the items to be migrated, lists them, and creates a selection of the files. By default, the task cannot trigger the migration job until the selection step is complete. A storage scan can be time consuming if the number of files to be migrated is very high and / or if the deduplication is activated. Using job parallelization changes the default behavior.
7. When job parallelism is enabled, set:
  - a. The maximum number of simultaneous parallel jobs: in general, 2 times the number of data movers that make up the platform pool.
  - b. The number of minutes you want before starting a new job.
  - c. The maximum volumes in GB you want before starting a new job. The default value is 1024 GB.
  - d. The maximum number of files you want before starting a new job. The default value is 250,000 files.
  - e. To set only one of the limits (time, size, or number of files), enter 0 in the field that the Synchronization task should ignore. You must define at least one of the three fields.

**Note:** Each of these limits define when a new job will be started. The selection operation continues in parallel with the copy job until the defined limit is reached again, which in turn will cause a new copy job. This continues until you reach the maximum number of parallel copies allowed.

The limitation(s) on file selection should be sufficient to allow the job to select enough files, but not too much to prevent the data mover from being idle when selecting files. Experience determines the best compromise between these priorities.

Three limits are considered during the synchronization job. They are presented in the following order:

1. Volume of the selection
2. Number of files in the selection
3. Time : even if the selection has not reached volume or number, the copy job is triggered at the end of the set time.

8. Choose the copy mode:

- The following options are available to copy data:
  - **Copy operating system rights** Miria copies all the file and directory data and alternate streams.
  - **Traverse symbolic links** Miria creates the symbolic links while copying the symbolic link data to the appropriate destination for both files and directories.
  - **Manage hardlinks** (Linux/Unix only over NFS) Miria copies the directory structure from the source file system to the destination. The hardlink structure on the source is preserved and rebuilt at the destination location. It is recommended to use this option in **Echo** mode. The task scans and creates the hardlinks, for which the explicit mode is required. This excludes the **Subscribe** and **Combine** modes, where the synchronization is applied from the destination to the source.


Or

- Copy only permissions (ACL), extended attributes (XATTR) and alternate data streams (ADS).
9. To check migration integrity, select a hash algorithm. An integrity check is possible in both normal and cut-over mode and enables monitoring and producing reports on the migration task.
10. Click **Next**.

### Step 5: Summary


1. Read the **Summary** of the task.
2. Enter a name for the task
3. Associate the task to a project.
4. Click **New task**.

## Edit a Project

1. Click the **Migration** tab, then the  button in a project.
2. Click **Edit project**.
3. Enter a new name for the project.
4. Click **Update**.




## Edit a Task

1. Click the **Migration** tab, then select a project.
2. In the **Project overview**, select a task and click the  button.
3. Select **Edit task**. The task configuration wizard is displayed.
4. Modify the section(s) you want to edit and click **Update** to save changes.

## Start Migration Task(s)

A project may consist of multiple tasks. Miria provides the ability to start all tasks at the same time or to start tasks independently.


### *Start an individual task*

1. Select the project.
2. In the **Tasks** section, click the  button of a task.
3. Choose one of the following options:
  - a. **Start task.**
  - b. **Start task in Test Mode.**
  - c. **Start task with Pre-Cutover.**


### *Start all tasks*

1. Select the project.
2. In the upper right corner, click **Start** and choose:
  - **Start all tasks.**
  - **Start all tasks in test mode.**
  - **Start all tasks with pre-cutover.**


## Duplicate a Task

1. Click the **Migration** tab, then select a project.
2. In the **Project overview**, select a task and click the  button.
3. Select **Duplicate task**.
4. Enter the name of the task to be duplicated.
5. Click **OK**. The new task is created within the project.

## Disable a Project or a Task

1. Click the **Migration** tab:
  - Click the  button in a project and select **Disable**.

**Or**

  - Select a project, then click the  button in a task and select **Disable**.
2. Click the **Settings** tab, then **Hidden projects and tasks** to locate and restore disabled projects and tasks.

# CHAPTER 11 - Manage the Migration

This chapter lists the 3 steps of a migration project. To manage a migration, tasks must be started at each step of the migration project:

- If a task is scheduled, it will start automatically. See [Step 4: Set additional options](#).
- If a task is not scheduled, the task will need to be run. See [Start Migration Task\(s\)](#).

## Step 1: First Synchronization

The first step in a migration project consists of synchronizing the initial transfer of data between the source storage and the target.

Before starting the synchronization, define the user workflows on the source storage and the target storage during the data migration.

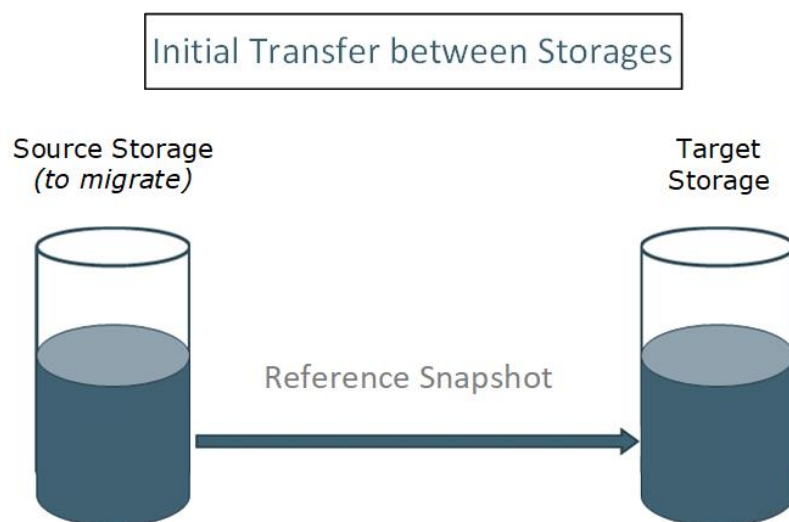
- If production on the target storage is halted, the task can start in **Echo** mode.
- If production on the target storage starts immediately, it is recommended to use **Contribute** mode.

See also the Synchronization Types section in Miria Administration Documentation.

The synchronization will behave differently depending on whether snapshot is enabled or not.

### **With Snapshot:**

1. Miria will make a reference snapshot of the source storage ([Figure 11](#)).
2. Perform a full scan of the snapshot to validate it.
3. Synchronize data from the source to the target storage.



**Figure 11:** Diagram of a reference snapshot from a source to a target storage

### **Without Snapshot:**

If snapshot is not available on the source storage:

1. Scan the entire file system.

2. Synchronize data to the target storage. The first synchronization without a snapshot can take days/weeks depending on the volume, size and number of files.

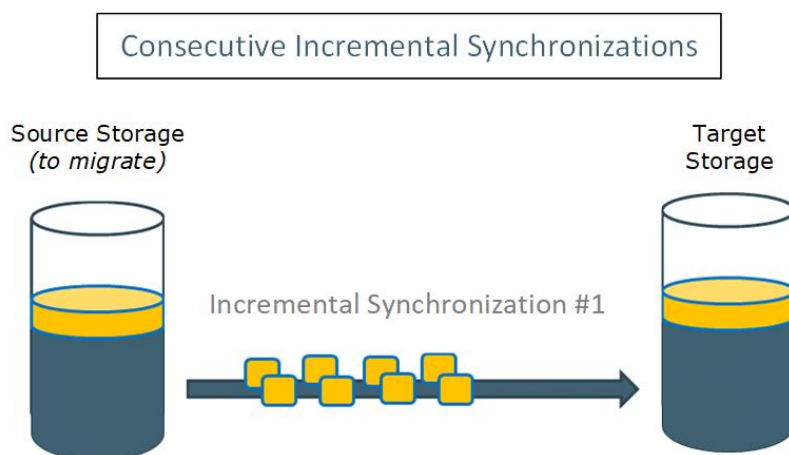
When performing the first synchronization with or without snapshot, it is recommended to split the file system by path on several tasks. This enables to scan the file system in parallel.

**To start the first synchronization:**

1. Open the project or the task you want to migrate.
2. Click [Start Migration Task\(s\)](#).
3. Click the **Activity** tab to verify the job progress.

## Step 2: Incremental Synchronization

The incremental synchronization is the process of running a task to migrate daily updates or changes since the first synchronization task was run ([Figure 12](#)). It can take several days or weeks depending on your data volume.



**Figure 12:** Incremental synchronization from a source to a target storage

**With Snapshot:**

Each synchronization follows 5 sequential stages:

1. Second snapshot of the source storage.
2. FastScan retrieves the list of objects that have been modified since the previous snapshot.
3. Miria validates the list returned by FastScan through comparison between source and target storage. Miria for Migration produces a change list.
4. Detected modifications are propagated (creation, deletion in **Echo** mode, etc.) to the target storage.
5. If the synchronization is successful, the previous snapshot is deleted and the current snapshot will be the reference point for the next task.

**Note:** Adding additional data movers will reduce the time needed for migration.

These incremental synchronizations enable the operations to converge towards the final synchronization.

**With FastScan:**

Scanning begins:

1. First run:
  - If parallelization rules are set:
    - Miria scans until triggering the parallelization rules defined, and spawns a new copy, sync, archive, or backup job.
    - The scan keeps going until triggering once again the parallelization rules, and so on till the maximum parallel jobs defined into the task definition are triggered.
  - If no parallelization rules are defined:
    - All of the source platform is scanned.
    - Once the scanning is over, the data movement is initiated.
2. FastScan incremental runs:
  - Changes list are consolidated against source storage API.
  - Miria scans against this change list.
  - If parallelization rules are set:
    - Miria scans until triggering the parallelization rules defined and spawns a new copy, sync, archive, or backup job.
    - The scan keeps going until triggering a new time the parallelization rules, and so on till the maximum parallel jobs defined into the task definition are triggered.
  - If no parallelization rules are set:
    - Miria scans all.
    - Once scanning is over, the data movement is initiated.

**To manage the incremental synchronization:**

1. Open the project or the task you already run in the [Step 1: First Synchronization](#).
2. Click [Start Migration Task\(s\)](#).
3. Click the **Activity** tab to verify the job progress.
4. Start the tasks as many times as necessary.

## Step 3: Final Synchronization (Cutover)

The final synchronization is performed to complete the data migration to the target storage while the production is stopped on the source storage ([Figure 13](#)). It ensures that the source and target storage are fully synchronized. During the final synchronization, Miria does a full scan of the reference snapshot without creating or deleting one.

The final synchronization task is supported only in **Echo** mode. When launching the task, all new data on the target storage (which does not exist on the source storage) will be deleted.

**Note:** During the final synchronization, the source storage must be on read-only mode in accordance with the customer's constraints. This should have been predefined in the preparation and planning phase and the Statement of Work.

Cutover times are dependent on the size of the data sets being migrated and the daily change rate.

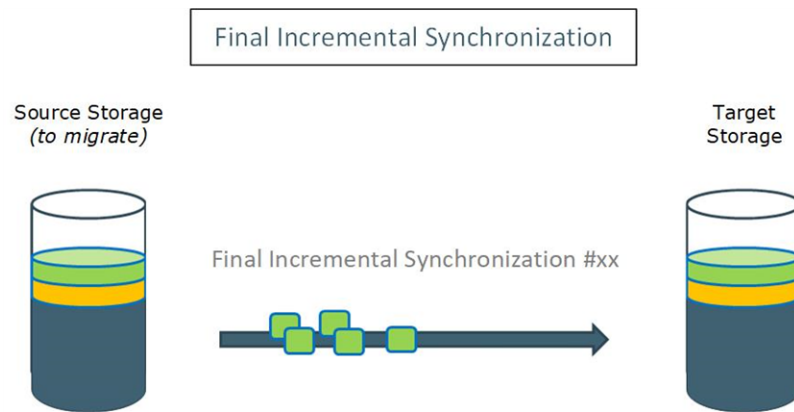



Figure 13: Final synchronization process


**Step 1: Start the final synchronization**

1. Stop production on the source storage or set to read only.
2. Open the project or the task you have already run.
3. Click the  button of a task.
4. Select **Start task with Pre-Cutover**.

Once the data on the target storage is fully synchronized, proceed with the copy of the ACLs and alternate streams in the next step. This allows to:

- Replicate the rights and permissions on the source storage.
- Restore the modification dates of the folders on the target storage.

**Step 2: Copy permissions, extended attributes and alternate streams**

1. Select the task for which the data synchronization is run and click the  button.
2. Select **Edit task**.
3. In the Task creation wizard, click **Next** until the task options are displayed.
4. In the **Copy mode** section, select the option to copy only permissions (ACL), extended attributes (XATTR) and alternate data streams (ADS) (Figure 14).

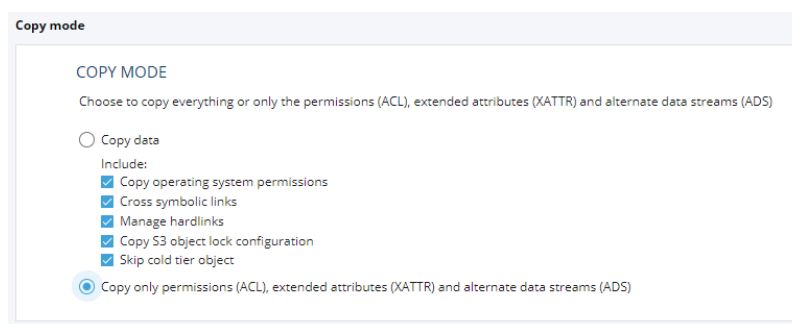



Figure 14: Copy mode options

5. Click **Next** and then **Update task** to save modifications.
6. In the task overview, click the  button and select **Start task**.

Once the migration task is successfully completed, production on the target storage can start.

# CHAPTER 12 - Manage Users

You must create a user to access and, for instance, manage permissions. A user unknown to Miria does not have the permission to access the software.

Users are created either:

- **Manually** Declare each user individually and enter all the user parameters and permissions manually.
- **Automatically** Define a Reference User as a pattern. Auto-creation of users is only possible with the LDAP access modes. The first time a user logs in, a user is created with the profile and permissions of the Reference User.

## Add a User


1. Click the **Users** tab, then the **Users** tile. The list of users is displayed.
2. Click the **+ New user** button in the top right corner. The user creation wizard is displayed (Figure 15).

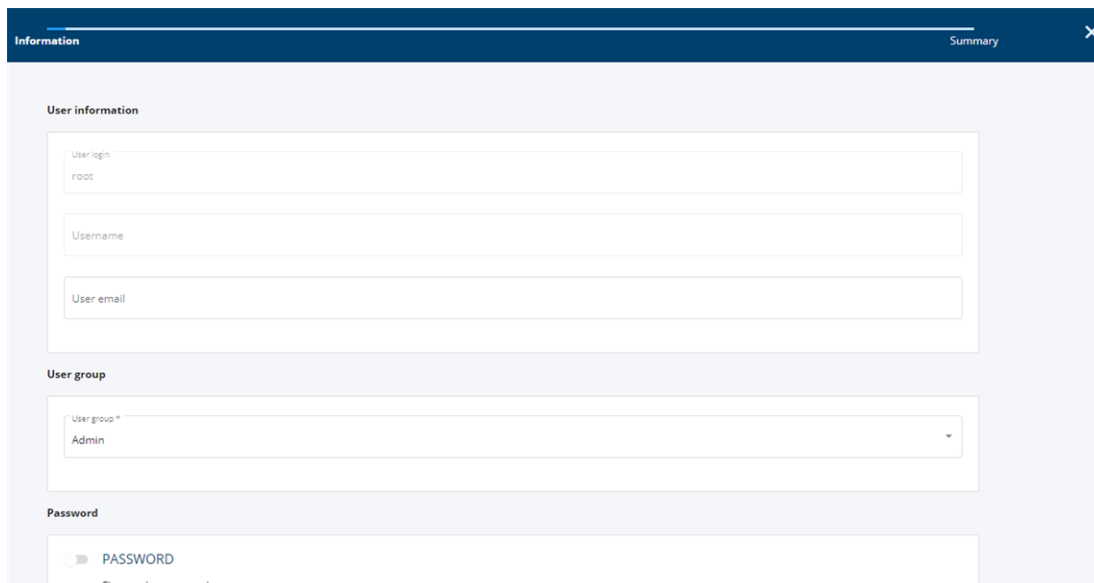
Figure 15: The user creation wizard

3. Enter the user information:
  - **User login** Name by which Miria knows the user. The user must use this name to connect. You cannot use the backslash (\) character.
  - **Username** (Optional) Name of the person to whom the user login is assigned. For example, the person who logs in as *ntillb* is Norbert Tillbury.
  - **User email** (Optional) Email address that can be used to notify the administrator of any action by this user.
4. In the **User group** list, select the user group to which the user belongs. The user can belong to only one user group.
5. Activate the **Password** button to assign the user a password. By default, you can enable empty passwords by letting the button turned off.

6. Define the user options:
    - **Active user** If this option is enabled, the user has the permission to connect to Miria. If it is disabled, the connection is denied.
- Note:** If you disable the **Active user** option after users have already archived data, they can no longer access Miria, but any data previously archived is not deleted from the system.
- **Super user** The user can log as the administrator and have full administration rights over the application. By contrast, standard users have only the right to perform operations on their own repositories.
  - **User repository** Creates a personal repository for the new user as soon as the form is validated. Only this user or a super user has access to this personal file.
7. Click **Next**. A summary of the user configuration is displayed.
  8. Click **Create** to confirm the user creation.

## Edit a User

1. Click the **Users** tab, then the **Users** tile. The list of users is displayed.
2. From the list of users, click the  button. The User configuration wizard is displayed ([Figure 16](#)).



The screenshot shows a 'User configuration wizard' window with a dark blue header containing 'Information' and 'Summary' tabs, and a close button. The main content area is divided into three sections:

- User information:** Contains three text input fields labeled 'User login' (with 'root' entered), 'Username', and 'User email'.
- User group:** Contains a dropdown menu labeled 'User group \*' with 'Admin' selected.
- Password:** Contains a toggle switch labeled 'PASSWORD' which is currently turned off, and a link below it that says 'Change the password'.

**Figure 16:** Example displaying a user configuration that can be edited

3. Update the user configuration and complete the wizard to save modifications.

## Add a User Group

User Groups inherit the setting values from the default settings.

Conversely, if you specify a setting on a user group, the value applies to that user group, but also to all of these objects that are lower in the hierarchy.

There are three types of user groups:

- User group, which can contain only users. See [To add a user group](#) for its creation procedure.
- Overall group, which is a group of groups. It can contain user groups and users, but not other overall groups. See [To add a user group](#) for its creation procedure.
- LDAP group, which is a kind of overall group that represents an existing LDAP group on an LDAP server. It enables you to assign permissions to users of this group. See [To add a user group](#) for its creation procedure.

### ***To add a user group***

1. Click the **Users** tab, then the **Groups** tile.
2. Click the **+ Add** button at the top right and select **Add user group**. The user creation wizard is displayed.
3. Enter the group name.
4. Click **Next**.
5. Select the group authorizations:
  - **None**.
  - **Monitoring** Enables the group to read information.
  - **Administration** Enables the group to edit information.
6. Click **Next**. A summary of the group configuration is displayed.
7. Click **Create** to confirm the group creation.

### ***To add an overall group***

1. Click the **Users** tab, then the **Groups** tile.
2. Click the **+ Add** button at the top right and select **Add overall group**. The user creation wizard is displayed.
3. Enter the group name.
4. Click the **Members** list to display the entire list of users and user groups to add to your overall group.
5. Select each item that you want to add.
6. Click the **+** button to validate your selections.
7. Click **Next**. A summary of the group configuration is displayed.
8. Click **Create** to confirm the group creation.

### ***To add an LDAP group***

1. Click the **Users** tab, then the **Groups** tile.
2. Click the **+ Add** button at the top right and select **Add LDAP group**. The user creation wizard is displayed.
3. Enter the group name.
4. (Optional) Activate **Secure mode** to select a certificate.
  - Choose the path to the certificate to be used to connect to the LDAP server with SSL.
  - Check the **Ignore SSL check certificate** box if you do not wish to establish SSL verification of the machine.
5. Define the group configuration:



- **Server type** In the drop-down list, choose the type of server between **Active Directory** and **LDAP**.
- **Server address** Enter the IP address or the name of the LDAP server. This server must host the LDAP directory that contains the users you want to import.
- **User and Password** (Optional for Active Directory server) Enter a username and password to authenticate to the LDAP server. If both fields are filled in, you must fill in the User Base DN field before selecting the Base DN. If both fields are empty, an anonymous connection will be used.
- **Base DN** Select the root directory of a server.

Each entry stored in LDAP databases requires a unique identification or Distinguished Name (DN). The top hierarchy in an LDAP directory tree is called the Base DN.

6. Click **Next** and define the advanced configuration options:
  - **User key** Automatically pre-filled according to the type of server. It contains the attribute name to be used to retrieve the user's name. This is the attribute to be used by default when autocreating the LDAP user. Its value is `sAMAccountName` for Active Directory and `uid` for LDAP.
  - **Internal user key** Enter a specific attribute if you want the user's name to be different from the one used to connect to LDAP. During autocreation, the value of this attribute will be used instead of the value of the attribute entered in the user key.
  - **Bind DN** Automatically pre-filled according to the type of server.
  - **Group base DN** Mask used to authenticate to the LDAP server. It is used to reformat connection credentials during authentication. Its value is different depending on the type of server:
    - For Active Directory: `[DomainName]\{LoginName}`. The prefix `[DomainName]` is not mandatory, and it will be replaced by the domain name used (if it exists). For example: `TEMQLDAP\{LoginName}`.
    - For LDAP: `uid={LoginName}`.
  - **User base DN** Select the group or domain containing all users of the domain. This field is mandatory for LDAP servers.
  - **Group** Select a group from the level at which users are to be searched. The Group must have a Distinguished Name. This field is mandatory for all types of servers.
7. Click **Next**. A summary of the group configuration is displayed.
8. Click **Create** to confirm the group creation.

## Configure SAP

A security authentication path (SAP) defines an authentication authority that is in charge of determining whether a user has the permission to access Miria.

These are the three types of authority authentication:

- Miria internal security system.

This is the default authentication authority that corresponds to the Free Login access mode. With this system, user names and passwords are stored in the Miria database.

- LDAP server.

If the authentication is delegated to an LDAP server, the passwords are not stored in Miria.


- LDAPS server.

This is the same as LDAP server, but adds encryption between the Miria server and the LDAP server.

You can declare several authentication authorities, and sort them in order of priority. Miria checks user access with the first authentication path, then with the second path if the access is denied with the first one, etc.

Only unique usernames are supported. Configurations in which the same user name exists in several domains associated with different passwords are not supported.

## Set Password Policies

1. Click the **Users** tab, then the **Access** tile. The list of rules is displayed.
2. Click the  button of the local rule. The rule creation wizard is displayed.
3. Enter the rule name.
4. Set a password policy. If enabled, complete these parameters:
  - Number of figures.
  - Number of lower cases
  - Number of upper cases.
  - Numbers of special characters.
  - Length of the password.

If the admin change the password policy, the user will be asked to set a new password that comply with the new policy, at the next connection.


You can define only one path of Local type, but several paths of LDAP or LDAPS types. See [Add a LDAP Rule](#) and [Add a LDAPS Rule](#) for their creation procedure.


## Reorder Rules

1. Click the **Users** tab, then the **Access** tile. The list of rules is displayed.
2. If needed, drag and drop the SAPs to define its order of priority. The path that to be checked first must be on top of the list.

**Note:** If you decide that user authentication must be delegated to an LDAP server, and place LDAP on top of the list, the users connecting to Miria must use their LDAP credentials.

## Test Rules

1. Click the **Users** tab, then the **Access** tile. The list of rules is displayed.
2. Click the  button next to the list to test the authentication paths.
3. In the window that displays, enter the name and password of the user for whom you want to test the path.
4. Click **Continue** to validate the testing.

The  icon turns green on the successful paths, whereas it turns red on the paths that fail. The icon remains gray for the paths that are not tested.


## Add a LDAP Rule

1. Click the **Users** tab, then the **Access** tile. The list of rules is displayed.
2. Click the **+ Add** button at the top right and select **Add LDAP rule**. The rule creation wizard is displayed.
3. Enter the rule name.
4. Select the LDAP group member corresponding to the LDAP server group that has the permission to access Miria. All users belonging to this group are auto-created at first login using LDAP access mode. The LDAP Group must have been previously created.
5. Check **Enable auto-creation of users** if you want to create a reference user.
  - a. Click the list and select the user that you want to use as a model. The auto-created user belongs to the same user groups and has the same advanced settings and permissions as the reference user.
6. Click **Next**. A summary of the rule configuration is displayed.
7. Click **Create** to confirm the rule creation.

## Add a LDAPS Rule

1. Click the **Users** tab, then the **Access** tile. The list of rules is displayed.
2. Click the **+ Add** button at the top right and select **Add LDAPS rule**. The rule creation wizard is displayed.
3. Enter the rule name.
4. Select the LDAPS group member corresponding to the LDAPS server group that has the permission to access Miria. All users belonging to this group are auto-created at first login using LDAPS access mode. The LDAPS Group must have been previously created.
5. Check **Enable auto-creation of users** if you want to create a reference user.
  - a. Click the list and select the user that you want to use as a model. The auto-created user belongs to the same user groups and has the same advanced settings and permissions as the reference user.
6. Click **Next**. A summary of the rule configuration is displayed.
7. Click **Create** to confirm the rule creation.

## Edit a Rule

1. Click the **Users** tab, then the **Access** tile. The list of rules is displayed.
2. From the list of rules, click the  button. The current rule configuration is displayed.
3. Update the rule configuration and complete the wizard to save modifications.

## Set the Two-Factor Authentication

In the Web User Interface, you can set the Two-Factor Authentication:

1. Click the top right corner of your screen on the user profile icon. This menu appears ([Figure 17](#)):

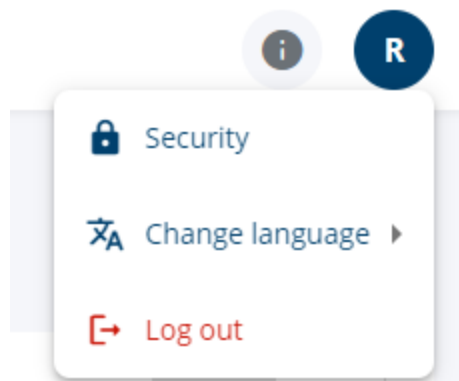


Figure 17: User profile menu

2. Select **Security**.
3. Click the **Two-Factor Authentication** tab, you now have two possibilities; the Two-Factor Authentication was set as mandatory or as optional. These options are defined in the settings by the administrator.

**Note:** If you are logged in LDAP mode and if Two-Factor Authentication is forbidden, **Security** is hidden in the menu.

## Configuring a Two-Factor Authentication Set as Mandatory

In this case, this is how the tab is displayed (Figure 18):

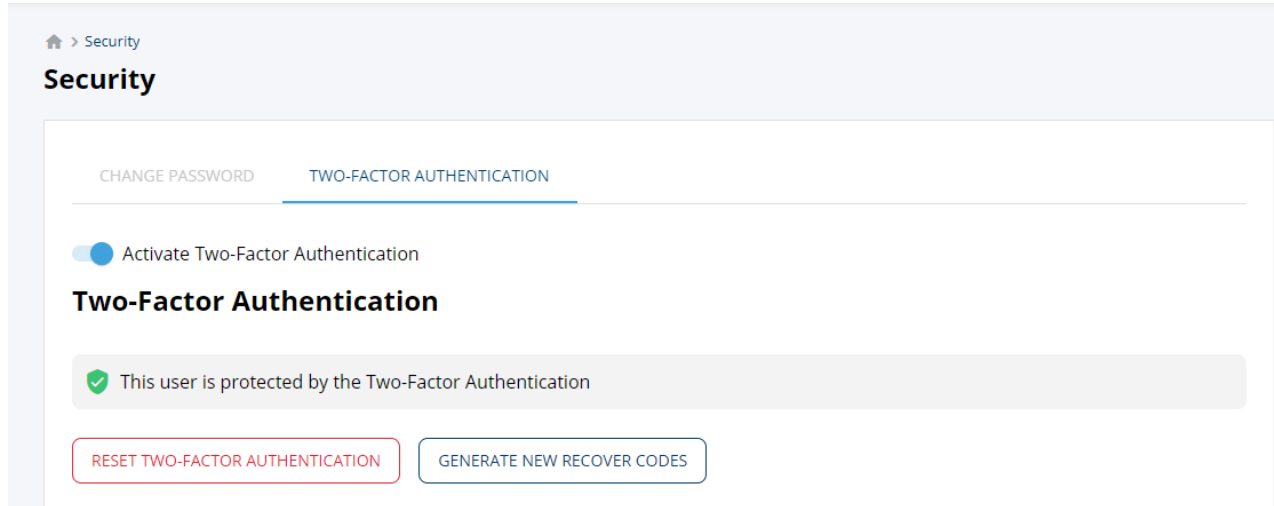


Figure 18: Mandatory Two-Factor Authentication

You cannot change the toggle, it remains activated.

But you can execute other actions:

- Generate new recover codes.
- Reset the configuration.

**Note:** When Two-Factor Authentication is mandatory, if you reset the configuration, you have to configure it again. It can be straight away, or on your next log in.


### To reset Two-Factor Authentication

1. Click **Reset Two-Factor Authentication**.
2. Enter the security code that is generated on the authentication application and valid for thirty seconds.
3. Reconfigure the Two-Factor Authentication (Figure 19):

Activate Two-Factor Authentication

## Two-Factor Authentication

Securing authentication takes three steps.

- 1. Download an authentication application**  
 For example Authy or Google Authenticator
- 2. Provide the authentication key**  
 Enter the following characters in the Authentication application or scan the QRcode  
 RYGV OQ4D ZLDX QQPJ P5QG TKHL WEU6 2GYT  

- 3.Enable the Two-Factor Authentication**  
 Enter the code provided by the authentication application (Make sure your computer clock is on time).  

ENABLE

Figure 19: Securing authentication

4. Scan the QR code and enter the code returned by the authenticator.  
The Two-Factor Authentication is set.

## Configuring a Two-Factor Authentication Set as Optional

In this case, the Two-Factor Authentication is not mandatory, you can choose by yourself to enable this option or not. You have more possibilities.

## To activate the Two-Factor Authentication

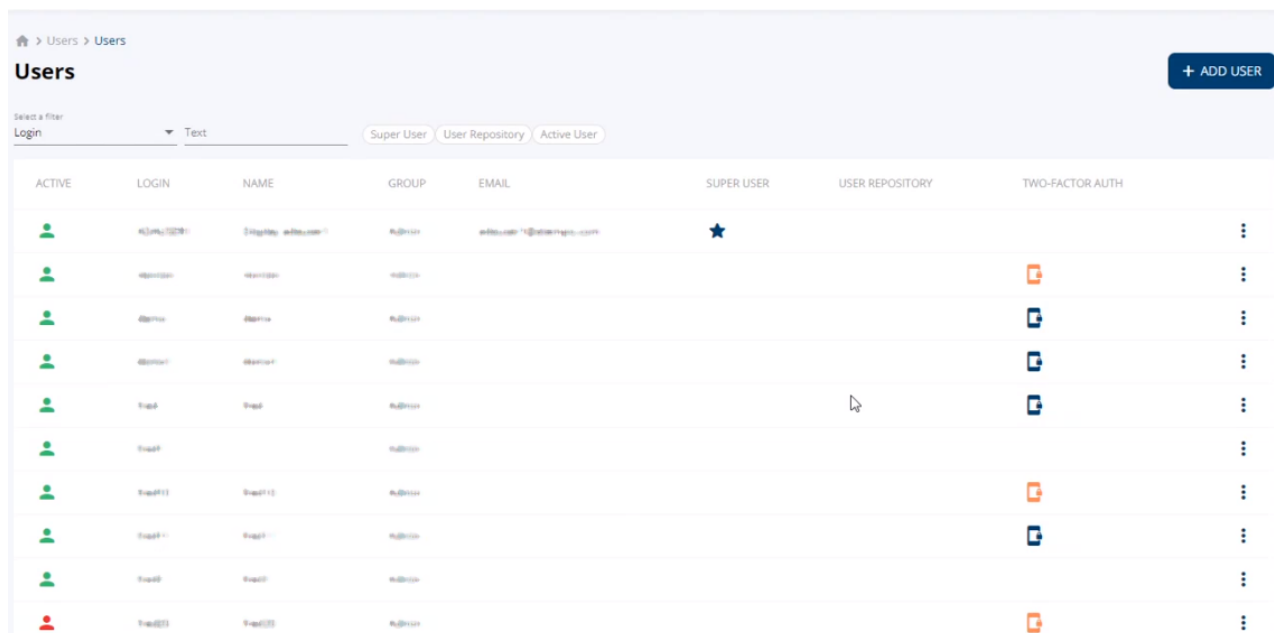
1. Click the toggle to define this option as enabled.
2. Scan the QR code on your Authentication App.
3. Enter the code returned by the authenticator.  
You can always choose to deactivate the Two-Factor Authentication as it is not set as mandatory.

## Checking the status when you are allowed to administrate the users

In the **Users** tab, you can check the status of the Two-Factor Authentication option for each user (Figure 20). But you can also change the parameters for any user.

You can select the user tile and check the status of the activation for each user:

- Red: the Two-Factor Authentication is enabled and set.
- Orange: the Two-Factor is enabled but not configured by the user yet.

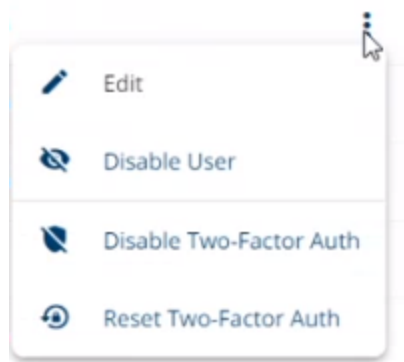


The screenshot shows the 'Users' management page. At the top, there's a breadcrumb 'Users > Users' and a '+ ADD USER' button. Below the header, there's a filter section with 'Select a filter' and 'Login' dropdown, and a 'Text' input field. There are also three tabs: 'Super User', 'User Repository', and 'Active User'. The main table has columns: ACTIVE, LOGIN, NAME, GROUP, EMAIL, SUPER USER, USER REPOSITORY, and TWO-FACTOR AUTH. The 'TWO-FACTOR AUTH' column shows status icons: a blue star for 'Super User', a red icon for 'enabled and set', and an orange icon for 'enabled but not configured'. Each row has a three-dot menu icon on the right.

ACTIVE	LOGIN	NAME	GROUP	EMAIL	SUPER USER	USER REPOSITORY	TWO-FACTOR AUTH
	admin@miria.com	Super User	admin	admin@miria.com	★		
	admin	admin	admin				
	admin	admin	admin				
	admin	admin	admin				
	Test	Test	admin				
	Test	Test	admin				
	Test(1)	Test(1)	admin				
	Test(1)	Test(1)	admin				
	Test(1)	Test(1)	admin				
	Test(1)	Test(1)	admin				

Figure 20: Users Two-Factor Authentication status

If you are a SuperUser, you can disable or reset the Two-Factor Authentication for a user without any code needed. To do so, select one of the rows. This menu appears (Figure 21):



**Figure 21:** Rows menu

**Note:** You can also configure Two-Factor Authentication on external users, for example AD or LDAP users.





# CHAPTER 13 - Advanced Tasks

Tasks are automatic jobs that you can schedule or start manually. A task defines the scope of a Miria job, the source and destination of the data that it processes, its scheduling, and many other options.

Miria embeds basic maintenance tasks. Thus there is no need for you to create them for the product to be operational; however, you may customize basic tasks or create new tasks with specific characteristics.

## Task Types

There are two categories of tasks:

- **Internal management tasks**  
The internal management tasks are automatic tasks (i.e., they launch jobs based on a schedule).
- **Data movement tasks**  
The data movement tasks let you select and move the data to and from the repository. You can launch these tasks either manually or automatically.

## Internal Management Tasks

The following table ([Table 3](#)) describes the template that you can use to create internal management tasks:

**Table 3:** Internal management task template

Task	Description
<b>Automatic deletion</b>	<p>Deletes the source data that matches a set of constraints once you have archived the source data. A deletion task only deletes the source data archived through an automatic archiving task.</p> <p>See <a href="#">Automatic Deletion Task</a> for details.</p>
<b>Automatic retention</b>	<p>Keeps archives tidy by permitting the deletion of objects that are no longer needed from the Miria database. It only applies to archives fed by automatic archiving tasks, which replace the archived file with a stub after archiving.</p> <p>See <a href="#">Automatic Retention Tasks</a> for details.</p>

Table 3: Internal management task template

Task	Description
<b>Maintenance</b>	<p>Scans the database and deletes useless data. You can choose the items to delete (e.g., expired instances, sub-job metadata, jobs, events, etc). A Maintenance default task is scheduled to perform all maintenance operations, except job and event deletion, on every first Sunday of the month at 12:00 P.M.; however, you can reconfigure it according to your needs, or create a new one.</p> <p>See <a href="#">Maintenance tasks</a> for details.</p>
<b>Retention</b>	<p>Task automatically launched by the Maintenance task. Create this task only if you need to configure behaviors that will apply to all retention operations launched by the Maintenance task (e.g., to send an email each time it is performed).</p> <p>See <a href="#">Creating a Task</a> for details.</p>
<b>Storage proxy maintenance</b>	<p>Archiving and retrieval jobs in client mode create temporary files in a cache space on a storage proxy. This space is normally deleted after the jobs complete, but if a job terminates on error or is canceled, some files may remain.</p> <p>The Storage proxy maintenance task scans the directories of the storage manager containers and deletes any temporary files that archiving and retrieval jobs in client mode have left. It requires no configuration.</p>
<b>Volume management on storage manager</b>	<p>Checks the space used on one or all of the storage managers. A high and a low water marks are defined in the storage manager configuration.</p> <p>See <a href="#">Recycling Triggered by Volume on Storage</a> and <a href="#">Volume Management on Storage Managers Task</a> for details.</p>
<b>Miria Database backup for PostgreSQL</b>	<p>Backs up the Miria database.</p> <p>See <a href="#">Database Backup Task</a> for details.</p>
<b>Archive Report</b>	<p>Generates a report on the archive volume.</p> <p>See <a href="#">Archive Report Task</a> for details.</p>

## Data Movement Tasks

The Data movement tasks can be launched either manually or automatically. They enable you to select and move the data to and from the repository.

### Data Movement Manual Tasks

These are the templates that you can use to create a manually launched task:

- Archiving

- Copy
- Delete
- Move
- Retention
- Retrieval
- Synchronization

Create a manually launched task only if you need to configure a behavior (e.g., to send an email each time the task is performed) that will apply to all manual operations of that kind of tasks. For the tasks created based on manual templates, you do not define any schedule.

See [Creating a Task](#) for details.

## Data Movement Automatic Tasks

The automatic tasks launch jobs that are based on a schedule. For the tasks that you create based on automatic templates ([Table 4](#)), you can either set the Scheduler to launch them automatically or launch them manually.

This table describes the templates that you can use to create data movement automatic tasks:

**Table 4:** Data movement automatic tasks template

Task	Description
<b>Automatic Archiving</b>	Launches archiving jobs based on a schedule.
<b>Automatic catalog ingest</b>	Launches Catalog Ingest jobs to import external LTFS media into the Miria database.
<b>XML Ingest</b>	<p>XML ingest tasks use XML files to run enriched automatic archiving. The XML files enable the customizing of archiving workflows and ingest interfaces.</p> <p>In addition to the archiving task scheduling, the XML ingest tasks enable you to perform these operations:</p> <ul style="list-style-type: none"> <li>• Archiving of specific files rather than whole directories.</li> <li>• Attributing metadata to files and folders.</li> <li>• Archiving into different archives and folders with a single run of the task.</li> </ul> <p>You are responsible for creating the XML files that launch the task. If they are not written directly with the Atempo format, you can translate them to the proper format applying a style sheet that you can request from Atempo Professional Services.</p>

[XML Ingest Tasks](#) for details.

Table 4: Data movement automatic tasks template

Task	Description
<b>Interplay Dispatcher</b>	<p>Task available only for users of the Miria for Avid Interplay application. You must obtain a specific license from Atempo.</p> <p>See the Partner Applications Documentation for details on the Miria for Avid Interplay application.</p> <p>See Interplay Dispatcher Migration Task for details on configuring the Interplay Dispatcher task.</p>

## Creating a Task

The User Web Interface provides three ways to create a new task:

### Creating a New Task from the Tasks Tab

#### *To create a task*

1. From the Web User Interface left pane, select **Tasks**.
2. Click the **+ NEW** button at the top right and select a kind of task among the list.
3. Set the configuration parameters set in [General Configuration Parameters for Tasks](#)

### Duplicating an Existing Task

You can duplicate an existing task and then customize it to exactly fit to your new needs.

#### *To duplicate a task*

1. From the Web User Interface left pane, select **Tasks**. The tasks list opens.
2. Click the **⋮** button of one of them and select **Duplicate**.
3. Enter the name of the new task and click **OK**.  
The duplicated task displays in the tasks list. You can modify its parameters to suit your needs.

## Organizing tasks

You can classify the tasks into projects. This help you navigate when there are many tasks. The tasks are displayed in a tree-like structure with the projects as a kind of folder, into which you can drag the existing tasks ([Figure 22](#)).

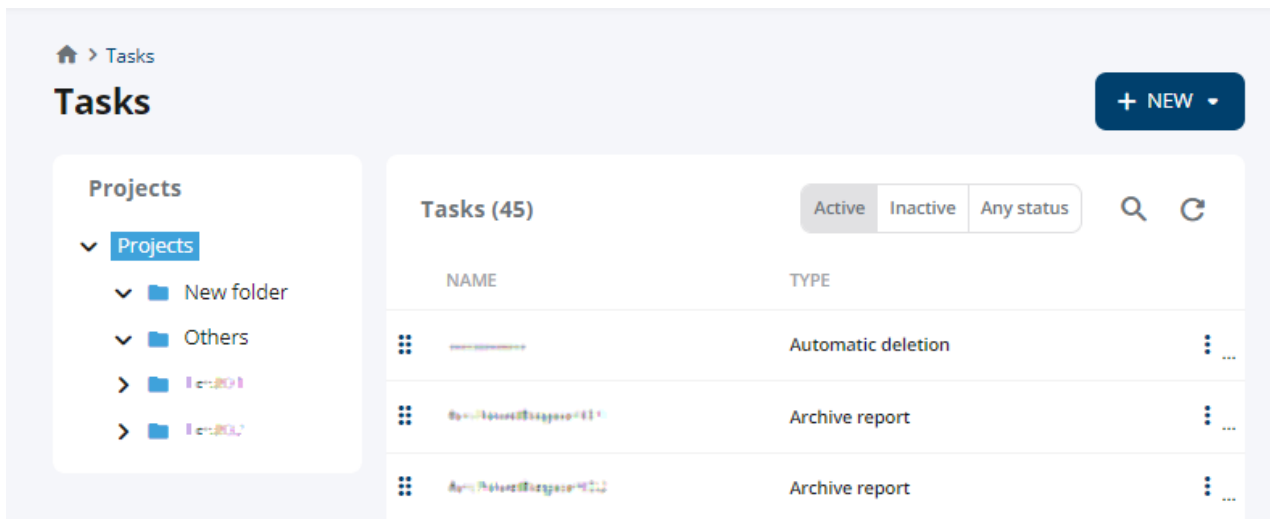


Figure 22: Tasks view

## Manage projects

Here are the different options the projects pane gives you:

- Projects:
  - **Add folders.** Create a new folder and name it.
  - **Refresh.** Give the arborescence an update.
- Folders:
  - **Refresh.** Give a folder an update.
  - **Rename.** Change a folder's name.
  - **Delete.** Delete a folder.

## Move a task

When you click on a folder, the tasks it contains appear on the right side of your screen.

You can drag and drop any task to move it from one folder to another.

This topic describes the running phases of Miria tasks.

## How Tasks Run

Although you can launch tasks manually, characteristically the Scheduler launches them at regular scheduled intervals.

**Note:** This process of selection alone can be quite lengthy. For example, if whole file deduplication has been configured on the archiving, the task must read every file selected to calculate the deduplication hash code on it. By default, the task waits until it has finished selecting files. It then gathers them into a single job and launches the job. If you have configured the parallelization parameters, the task launches several jobs before it has finished the selection of the files.

In the List of Jobs window the task displays on several lines ([Figure 23](#)).

ID	ACTION	STATUS	VOLUME	RATE	REPOSITORY	DATE
1245	Task	Completed			ArchOneToOne	Nov 8, 2022, 11:50:16 AM
1243	Task - Test mode	Completed			ArchAmm	Nov 8, 2022, 10:47:13 AM
1235	Task	Completed	1.9 GB			Nov 4, 2022, 11:28:14 AM
1226	Task	Completed	1.9 GB			Oct 28, 2022, 4:03:14 PM
1225	Task	Completed				Oct 28, 2022, 3:59:16 PM
1224	Task (Full)	Completed			Test	Oct 28, 2022, 2:57:35 PM
1223	Task (Full)	Completed			Test	Oct 28, 2022, 2:57:16 PM
1221	Task	Completed	1.9 GB			Oct 28, 2022, 2:55:28 PM
1216	Task	Completed			ArchOneToOne	Oct 27, 2022, 5:55:24 PM

Figure 23: Job List

Depending on the number of files to select, the use of deduplication, the size of the files, etc., the selection process can take long enough that the automatic task restarts before the previous iteration of the same task is finished, and before all the files have actually been archived. In order to prevent overlapping scheduled tasks from treating the same files, the default behavior is for only one instance of a task to run at any one time. Here is an example:

- The Scheduler launches an automatic archiving task, scheduled to run at midnight every 24 hours.
- The task takes 48 hours to select all the files to be archived.
- Twenty-four hours after the first launch of the task, the Scheduler is ready to relaunch it, but the first task is still collecting files.

If a second instance of the same task were to launch at its scheduled time, it would start to select the same files that the first instance has not finished selecting.


For this reason, the second instance of the task is not permitted to run until all the jobs launched by the first instance have completed. The first instance of the task remains in Running status until the last of its jobs is finished.

Any post-processing, such as the sending of e-mail notifications, thus occurs when both the task itself, and all of its jobs, are complete.

## Testing a Task

Once you have created a task, you can preview whether it is configured correctly and if the files and directories included in the task are appropriate. Testing a task creates a task job, but does not archive or delete any data. The List of Jobs displays the task job.


### *To test a task*

1. Click the **Tasks** tab in the left pane of your screen.  
The tasks view opens, and a list of tasks displays.
2. Click the  button and select **Start task in test mode**. A pop up opens.
3. Click **Yes** to validate. In the jobs list
4. Go to the jobs tab, in the jobs list, you can see your task. Its status is indicated. You can see the details, open the logs or download a report from this task.

## Launching a Task Manually

You can manually launch all tasks configured in Miria. Therefore, you can launch a task at any time without waiting for the task to reach its start date as entered in the scheduler.


### *To launch a task manually*

1. Select the Tasks tab in the left pane. The tasks view opens.
2. Click the  button of one of the tasks in the tasks list.
3. Select **Start task**.
4. Click **Yes** on the confirmation dialog box.  
The task creates and launches the corresponding job.

## Canceling a run

You can cancel a run in the same manner as a job.

### *To cancel a current run*

1. Select the **Jobs** tab in the left pane. The jobs view opens.
2. Click the  button of one of the current runs in the jobs list.
3. Select **Cancel**.
4. Click **Yes** on the confirmation dialog box.  
The run is then displayed in the History section of the List of Jobs with a Canceled status.


For all task types except Automatic Retention and Maintenance, Miria takes into account the Cancel request every five minutes. The effect of a Cancel request is to half the task selection process. No new job is created. Any jobs that the task has already launched continue running until completed, unless you cancel them too.

## General Configuration Parameters for Tasks

This topics describes the configuration parameters and tabs that are common to all types of tasks.

### General Parameters Common to All Tasks

#### From the Tasks List

In the tasks interface, choose a task from the task list and click the  button to access to the following options ([This topic describes the running phases of Miria tasks.](#)):

**Table 5:** Tasks list menu

Parameter	Description
<b>Edit Task</b>	When creating a new task, you have first to select a task type. See <a href="#">Creating a Task</a>
<b>Start Task</b>	Immediate manual launch of the task. See <a href="#">Launching a Task Manually</a> for details.  <b>Note:</b> For backup tasks, you can start them in full or incremental mode.
<b>Start the task in test mode</b>	Creates a task job for preview, but does not archive or delete any data. See <a href="#">Testing a Task</a> for details.
<b>Duplicate task</b>	Duplicates a task with the same configuration.
<b>Disable</b>	Lets you deactivate the task temporarily, without requering to delete it.



Table 5: Tasks list menu

Parameter	Description
<b>Email</b>	<p>Gives you access to the list of users that are notified by email when a scheduled task is run.</p> <ul style="list-style-type: none"> <li>• <b>Add +</b> click this button in the upper right corner of your screen. Select user(s) or groups, and click on one of those options to set on them: <ul style="list-style-type: none"> <li>• <b>None</b> they won't receive any email.</li> <li>• <b>Email</b> they will receive an email every time the task runs.</li> <li>• <b>On error only</b> they will receive an email only if the task ends with errors.</li> </ul> </li> <li>• </li> <li>• above the users list, there is a toggle <b>Email only if an action was performed</b>. A task can run without actually doing anything (e.g., a scheduled task on an empty directory). If this toggle is selected, and if you selected the email option in the creation or edition of the user(s)/group(s), the email is sent only if the task actually accomplished an action.</li> </ul> <p>See <a href="#">Task-specific Parameters</a> Receiving E-mail Notifications About an Automatic Archiving Task for details on obtaining an email notification on the status of an automatic archiving task.</p>
<b>Settings</b>	<p>Gives you access to the settings. You can change them directly here, or apply a template.</p> <p>Tasks inherit their settings only from the default settings. The only exception is the Archiving Policy setting which is inherited from the repository. If there is no archiving policy specified for the repository, then the task inherits its Archiving Policy setting from the default settings.</p> <p>If an setting is defined on a specific task through this tab, the value applies to the task on which you define it, overriding the inherited values.</p> <p>For the tasks, these are the available settings: Jobs, Email, and Security. Other types of settings are irrelevant.</p> <p>The Object Groups pop-up list enables you to select one of the object groups already existing in Miria. The task then inherits the subset of advanced settings that you have defined for the group and that are relevant to tasks.</p> <p>Modify the advanced settings for this task individually by clicking the Value field next to the setting that you want to modify and selecting a value from the list. See <a href="#">Default Settings</a> and <a href="#">Settings Templates</a>.</p> <p><b>Note:</b> For tasks that do not require configuration, such as manual tasks, this tab is grayed out.</p>

Table 5: Tasks list menu

Parameter	Description
<b>Report history</b>	You can display and download the volume reports from the Report History button.

## When Creating or Editing a Task

Table 6: General parameters common to all tasks

Parameter	Description
<b>Task type</b>	When creating a new task, you have first to select a task type. See <a href="#">Creating a Task</a>
<b>Task name</b>	Name that identifies the task within Miria.  <div> <b>Important:</b> When naming a new automatic task, do not use these terms (in either lowercase or uppercase) as they are reserved for the template name: <ul style="list-style-type: none"> <li>- ARCHIVING</li> <li>- RETRIEVAL</li> <li>- COPY</li> <li>- MOVE</li> <li>- DELETE</li> <li>- SYNCHRO</li> <li>- RETENTION</li> </ul> </div>

## Common Tabs

### The configuration tab

The Configuration tab enables you to set the configuration parameters for the individual Miria tasks, as described in Task-specific Parameters.

For tasks that do not require configuration, such as manual tasks, this tab is grayed out.

### The Scheduling tab

The schedule allows you to define the regular times at which the automatic tasks must be started.

The Scheduling tab enables you to define the regular times at which automatic tasks are to be launched. It is active for all tasks, except basic archiving, retrieval, copy tasks...

An error message displays if no occurrence in the month, days, and hours, minutes are set when the Scheduler is activated.

To set the scheduling:

1. Click the toggle **ENABLE SCHEDULING**.
2. Select a week day and an occurrence in the drop down menu. It specifies the day(s) of the week when automatic tasks must be started and at which frequency.

3. Select a time and check **Every 5 minutes**, or **Choose an interval**. It specifies the time when the automatic tasks must be started.

**Note:** For backup tasks, you can schedule both full, and incremental modes.

## Options Tab

The options tab enables you to associate run timeframes and run locks with the task, as well as any pre- or post-processing scripts.

The pre- and post-processing scripts must be located on the agent defined in the task.

This table describes the parameters of the Advanced tab:

**Table 7:** General parameters common to all tasks

Parameter	Description
<b>Commands</b>	<p>This option enables to enter commands manually to add custom settings to the archiving job. Click the toggle to enable it. Two fields appear:</p> <ol style="list-style-type: none"> <li>1. <b>Pre-processing:</b> Field to be filled in to enable you to launch a script before the launch of the associated job. It must always contain the full path of script to run and its interpreter.</li> <li>2. <b>Post-processing:</b> Field to be filled in to enable you to launch a script after the associated job finished, through the following keywords: <ul style="list-style-type: none"> <li>• {Job_Number}: Job ID associated to the task.</li> <li>• {Db_Name}: name of the environment on which you are working.</li> <li>• {Tpl_Status}: retcode of the job, if the retcode is different than 1, there is an error.</li> </ul> They will be replaced automatically upon execution. It must always contain the full path of script to run and its interpreter.  <b>Example:</b>  D:\miria\Binary\Bin\ada_perl.exe  D:\miria\Custom\custom_action.pl -job_id{Job_Number}  -db_name {Db_Name} -retcode {Tpl_Status} </li> </ol> <p>Will be replaced by:</p> D:\miria\Binary\Bin\ada_perl.exe D:\miria\Custom\custom_action.pl -job_id 12345 -db_name miria -retcode 1
<b>Run options.</b>	

**Table 7:** General parameters common to all tasks

Parameter	Description
<b>Run timeframe</b>	Period during which a task is permitted to run or prevented from running. This feature enables you to prevent tasks from running at times when you know there is heavy use of network resources for other operations. Click to select a run timeframe among those configured in Miria. To associate a task with a run timeframe, you must have configured it in the list of Run Timeframes interface. See <a href="#">Run Timeframes for details</a> .
<b>Run lock</b>	Limits the number of Miria tasks of any kind that can run simultaneously. Click to select a run lock among those configured in Miria. To associate a task with a run lock, you must have configured the Run Lock in the list of Run Locks interface. See <a href="#">Run Locks</a> for details.
<b>Next task</b>	Select the next task among the drop-down list.
<b>Maximum number of simultaneous runs</b>	<p>Number of times the current task can be run simultaneously. You can modify this field only for manual archiving and retrieval tasks. A user can launch one manual archiving and then launch a second before the first has completed. If you do not want to limit the number, leave this field at 0.</p> <p>For all types of tasks other than manual, this parameter is set to 1 and you cannot modify it.</p> <p>The Maximum number of simultaneous runs parameter differs from the Run Lock notion, in that it concerns only the task that is being configured. You can invoke a run lock on tasks of disparate types to prevent more than a specified number of tasks of any kind from running concurrently.</p>
<b>Wait when the maximum number of runs is reached</b>	<p>Select this box if you do not want additional tasks to be canceled (e.g., if the Maximum number of simultaneous runs is 3, the fourth task is not canceled.)</p> <p>If the box is selected, Miria waits for the first three tasks to complete before running the fourth task.</p>

## The Report History Tab

The Report History tab displays information on the generated reports (e.g., by the Archive Report task).

This table describes the columns of the List of available reports:

Parameter	Description
<b>Date</b>	Time and hour at which the report was generated.
<b>Name</b>	Name of the report in the <code>Archive_date-time.ext</code> format.
<b>Size</b>	Size of the generated report that is in PDF format.
<b>Download button</b>	Opens the report in the associated browser. Then, you can download the PDF file from the server to your local machine. For the Archive Report task, you can also obtain a volume report from the <code>ADA\Report</code> directory using the Windows Explorer.
<b>Delete button</b>	Click this button to delete the selected report from the server.

## Task-specific Parameters

Some tasks require particular configurations (e.g., it may be necessary to specify the platforms and directories that the task must scan for files to process, or you may want to set constraints on the files, such as age or size).

For all automatic tasks, see [General Configuration Parameters for Tasks](#) in the table General parameters common to all tasks, to know how you can name them.

Define these settings in the Configuration tab of the task Properties pane. Each task has its own requirements, so the tab displays different fields depending on the task that you are configuring.

See [General Configuration Parameters for Tasks](#) for details on the configuration parameters that apply to all tasks.

## Automatic Catalog Ingest Task

This table describes the fields that you can complete to configure the Automatic Catalog Ingest task:



Parameter	Description
<b>Source.</b>	
<b>Ingest Type</b>	Select Media/LTFS from the list.
<b>Storage Manager Container</b>	<p><b>Only for Media Manager storage manager container.</b></p> <p>Select from the list, an ingest Storage Manager Container into which you want to ingest the media.</p>

Parameter	Description
<b>Retention</b>	<p>Select from the list a retention that you want to apply to the data imported from the media.</p> <p>Click the + button to add a retention.</p>
<b>Filters.</b>	
<b>Library</b>	<p>Library in which Miria stores the archived data. The library alias (if any) displays between parenthesis.</p> <p>If you have completed the Barcode Selection filed, this field is ignored.</p> <p>This parameter is mandatory if you do not specify a Scratch Media Group or if you have not completed the Barcode Selection filed.</p> <p>Click the Browse button to select the library. Click the Minus (-) button to reset the field.</p>
<b>Media Type</b>	<p>Type of the media that you want to use for this storage manager container.</p> <p>Complete this field only if the library may contain media of several types (e.g., <b>LT0-6</b> and <b>LT0-7</b>), and that you want to use only one type.</p> <p>If you have completed the Barcode Selection filed, this field is ignored.</p> <p>If you have not completed the Barcode Selection filed, this field becomes optional as it defines the media type identifier.</p> <p>If this field remains undefined, all the orphan media belonging to the selected library are ingested into the selected archive.</p> <p>Click the Select button to display the list of compatible media types.</p> <p>You can select either a Media or a Class.</p>

Parameter	Description
<b>Define filters on barcodes</b>	<p>Optional.</p> <p>Select <b>Include</b> from the list to ingest media with a specific barcode range.</p> <p>Select <b>Exclude</b> to exclude a barcode range from ingestion.</p> <p>Enter the barcode range in the text field in the form of a pattern, using these wildcards:</p> <ul style="list-style-type: none"> <li>The * means any alphanumeric character any number of times.</li> <li>The ? means any alphanumeric character once.</li> <li>The   separates several possible pattern options.</li> </ul> <p>The expression must contain at least one * or ?.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>A005?? includes/excludes any media with a six character barcode beginning with the string A005. You might use this, for example, to select media from A00500 to A00599.</li> <li>*L4 includes/excludes any media with a barcode ending in L4. You might use this, for example, to select only media of LTO4 type.</li> <li>162* WV* includes/excludes any media with either a barcode beginning with the string 162, or a barcode beginning with WV.</li> </ul>

### Target.

<b>Existing repository</b>	<p>Imports the media into a repository which already exists in Miria.</p> <p>Select <b>Existing repository</b> and click the  button to choose a repository from the arborescence.</p> <p>The data will be imported at the repository root in a folder named after the media barcode.</p> <p>If the selected repository is not associated with a Media Manager storage manager container, you will have to complete the Storage Manager Container field.</p>
----------------------------	---

Parameter	Description
<b>New repository</b>	Imports the media into a new repository.  <b>Project:</b>  Enter a repository project name or click the  button to select one from an arborescence. Then, if you don't select a reference repository, the data will be imported at the organization root in a repository created automatically and named after the media barcode.
<b>Reference repository</b>	<b>Optional.</b> Click the  button to select from a list the repository that will be used as a template to create the new one.

## Automatic Deletion Task

These tasks delete the source data that matches a set of constraints once the source data has been put in repositories. Only the source data put in a repository through an automatic archiving task is deleted.

This table describes the parameters displayed in the Source & Target tab:

Parameter	Description
<b>Source.</b>	
<b>Storage platform</b>	Select the storage platform in which you want to delete data.
<b>Location of data to delete</b>	Enter the path of the data that Miria can delete.
<b>Target.</b>	
<b>Repository name</b>	Select the target repository
<b>Full path auto-generated</b>	Select the repository for which source data is deleted once it has been archived.



Parameter	Description
Archive repository	Possibility to store archived objects in archive repositories.

## Automatic Retention Tasks

If you delete a stub from a file system, and if there is no retention set on its corresponding instance(s) in the repository, these instances can remain in the database indefinitely. The automatic retention task provides a method to assign a retention period to these orphaned objects. Then, the first automatic maintenance task to run on the repository after the retention period has expired can delete them.

The automatic retention task works in this way:

- It first runs a check to ensure that all stubs in the file system correspond to object instances in the Miria database.
- If it finds an object in the database that no longer has a corresponding stub in the file system, and the object database instances have no defined retention period (the associated retention was set to Without), then the retention period defined in the automatic retention task is applied.  
If the automatic retention task does not have any retention periods defined, the retention is set to expire on the current date.
- Then, the next maintenance task to run after the expiration of the retention period eliminates the orphaned database instances.

**Important:** If a stub is renamed, it is considered as lost, and the retention task processes the corresponding instance in the database.

This table describes the Source & Target tab parameters for an automatic retention task:

Parameter	Description
<b>Source.</b>	
Storage platform	Displays the platforms configured in Miria. Select the platform that hosts the data to put in repositories.
Data for applying retention	Enter the root of the path from which the automatic retention task runs its check to see that all object instances in the database have corresponding stubs in the file system. You can enter multiple paths.
<b>Target.</b>	
Repository name	Select the target repository

Parameter	Description
<b>Full path auto-generated</b>	Opens a list of all repositories to which you have rights as a logged-in user. Select a repository to associate with the task and validate by clicking the check mark.
<b>Archive repository</b>	Absolute destination path. Select the destination location to associate with the automatic retention task.

This table describes the Options tab parameters for an automatic retention task:

Parameter	Description
<b>Retention</b>	<p>Opens the List of Retention Periods window that displays the retention periods configured in Miria. Select the appropriate retention period and select the check mark.</p> <p>If you select None, the next maintenance task deletes files.</p> <p>The Apply on Stub and Apply on Object options enables you to refine the retention by applying a retention period to a file from a repository in these circumstances (they can be activated individually or together):</p> <ul style="list-style-type: none"> <li>• <b>Apply on Stub.</b> When the stub is no longer present on the file system.</li> <li>• <b>Apply on Object.</b> When the object is no longer present on the file system.</li> </ul>

## Automatic Storage Repack Task

The repack task is used to defragment a media storage. When you launch an archiving job, Miria creates a .pax file containing all the files that will be put in repositories.

When a file from the repository is deleted, it is no longer referenced in Miria's database but still exists in the .pax file. The purpose of the repack task is to recover all the files that are still referenced in Miria. A new .pax file is then created which will contain all the files except those which have been deleted from the repository.

The volume of the repack task is defined by the following parameters:

Parameter	Description
<b>Nb. Expected Objects</b>	Total number of media present on the storage manager container.
<b>Nb Objects</b>	Number of media selected for repack.
<b>Volume Expected</b>	Total storage volume.
<b>Volume</b>	Actual volume of selected media.

**Note:** When you create an automatic storage repack task, there are a few specific actions that you need to do:

- Define the Source Storage Manager Container Name (Only a FileStorageContainer can be selected for a repack task. This container will be used to calculate the fill rate of each media).

- Enter the Data Fragmentation Ratio percentage. This threshold will be used to select the media to repack.

For example: A .pax file with a size of 150 MB contains File 1 (100 MB) and File 2 (50MB). When File 2 is deleted from the repository, there is  $(150-100) = 33\%$  of free space to recover on this media. This percentage is the data fragmentation ratio and allows you to select all the media that have 33% or higher of free space to recover inside the .pax file.

- (Optional) Activate Delete source media after repack. The media selected for the repack job will be deleted if the repack job is completed without errors.

- (Optional) Set the maximum number of jobs running in parallel. By default, the task creates one job per media.

## Database Backup Task

The Miria database backup task backs up the Miria database.

It is the PostgreSQL database backup task.

See Miria administration guide for more details.

## Maintenance tasks

The maintenance task enables you to delete both the repositories objects that have reached the end of their retention period and their associated jobs and events.

The preset Maintenance task performs all maintenance operations, except job and event deletion, on every first Sunday of the month at 12:00 P.M.; however, you can reconfigure it according to your needs or create new maintenance tasks with different parameters.

Parameter	Description
<b>Maintenance.</b>	

Parameter	Description
<b>Check running jobs</b>	Click this toggle to process the jobs that have been running for more than 24 hours: <ul style="list-style-type: none"> <li>Jobs on creation or running switch to the Terminated on error status.</li> <li>Jobs on queue restart or switch to the Terminated on error status, if they do not start.</li> </ul>
<b>Delete sub-job metadata</b>	To delete the metadata associated with a sub-job. As the data is , the metadata is linked to an instance and already present in the database. It is recommended that you delete job metadata regularly to optimize database space.
<b>Delete in recycler</b>	To delete permanently the repositories folders that you removed from a repository.
<b>Check expired instances</b>	To search the database for all expired instances, and create a retention job for each repository. A retention job deletes expired repository instances from the storage and the database.
<b>Check expired SML instances</b>	Click this toggle to delete the SML (Storage Manager Layer) archiving instances that are past their retention period.  This is only relevant when using the Miria (Messaging) software.
<b>Delete temporary tables</b>	To delete some temporary database tables that Miria may create while operating.  It is recommended that you delete such tables regularly to optimize database space.
<b>Delete archiving job details</b>	To delete details, messages, or alarms that are past their retention period.
<b>Delete copy / synchronization job details</b>	To delete details, messages, or alarms that are past their retention period.
<b>Delete repository tiering job details</b>	To delete details, messages, or alarms that are past their retention period.
<b>Delete statistics on jobs</b>	To delete details, messages, or alarms that are past their retention period.

Parameter	Description
<b>Delete jobs</b>	<p>To delete jobs that are past their retention period:</p> <ol style="list-style-type: none"> <li>1. Click the toggles for the types of jobs (see the list below), that you want to delete.</li> <li>2. Click the Job and Event retention toggle.</li> <li>3. Choose how long you want to keep the jobs In the Job retention fields. The default value is one month.</li> <li>4. Choose how long you want to keep the events related to the jobs in the Event retention field. This value must be less than or equal to the job retention. The default value is one month.</li> </ol> <p>Type of jobs that you can delete:</p> <ul style="list-style-type: none"> <li>• AER collection</li> <li>• Repository tiering</li> <li>• Archiving</li> <li>• Catalog ingest</li> <li>• Change LTFS volume lock</li> <li>• Change LTFS volume name</li> <li>• Copy</li> <li>• Create directory</li> <li>• Delete</li> <li>• Device scan</li> <li>• Drive diagnostic</li> <li>• Drive performance</li> <li>• Drive unmount</li> <li>• Ejection request</li> <li>• Library unknown media scan</li> <li>• Media deletion</li> <li>• Media duplication</li> <li>• Media mount</li> <li>• Media recycling</li> <li>• Media scratch</li> <li>• Media verify</li> <li>• Move</li> <li>• Rename</li> <li>• Retention</li> <li>• Retrieval</li> <li>• Storage manager integrity check</li> <li>• Synchronization</li> <li>• Synchro. digest</li> <li>• Task</li> </ul>

Parameter	Description
<b>Delete events</b>	<p>To delete events that are past their retention period:</p> <ol style="list-style-type: none"> <li>1. Click the toggles for the types of events (see the list below), that you want to delete.</li> <li>2. Click the event retention toggle.</li> <li>3. Choose how long you want to keep the events related to the jobs in the Event retention field. The default value is one month.</li> </ol> <p>Type of events that you can delete:</p> <ul style="list-style-type: none"> <li>• AUDIT TRAIL</li> <li>• CRITICAL</li> <li>• DEBUG</li> <li>• DEBUG STACK</li> <li>• ERROR</li> <li>• FATAL</li> <li>• INFO</li> <li>• STACK</li> <li>• STOP/DIE</li> <li>• SUCCESS</li> <li>• WARNING</li> </ul>


## Archive Report Task


The Archive Report task generates a volume report for a selected repository path.

### Volume Reports

Configuring the Archive Report Task

This table describes the Configuration tab fields that you must complete to configure an Archive report task:

Parameter	Description
<b>Source.</b>	
<b>Repository name</b>	Select from the drop down list a name for the repository.
<b>Repository path</b>	Click the  button to select the absolute path of the selected repository for which the volume report is generated.
<b>Layout. Enables you to modify the PDF file layout.</b>	
<b>Format</b>	Select the A4 or the US letter format.

Parameter	Description
Orientation	Select the portrait or landscape orientation.
Heading logo	<p>Image that displays as the output file header. You can either:</p> <ul style="list-style-type: none"> <li>• Leave the field empty. The PDF file does not display any image.</li> <li>• Enter the <code>{default}</code> keyword. The PDF file displays the default image included in the Miria distribution.</li> </ul> <p>Or</p> <ul style="list-style-type: none"> <li>• Click the  button to choose a heading logo in the arborescence. and browse for your own image. You can use any image that is in .jpg, .tif, .png, or .gif formats.</li> </ul>
Header title	<p>String that displays as the report title.</p> <p>You can enter a free text plus these keywords:</p> <ul style="list-style-type: none"> <li>• <code>{Job_Number}</code></li> <li>• <code>{SubJob_Number}</code></li> <li>• <code>{Archive_Name}</code></li> <li>• <code>{Archive_Path}</code></li> <li>• <code>{Archive_Global_Path}</code></li> <li>• <code>{Archive_Comment}</code></li> </ul> <p>The PDF file displays the associated value for each keyword that you have defined.</p>
<b>Report information. Enables you to modify the PDF file contents.</b>	
Media details	<p>Details on the media. These are the valid values:</p> <ul style="list-style-type: none"> <li>• <b>None.</b> Default value. The report does not display any media information.</li> <li>• <b>Media By Job.</b> The report displays the names of media, associated with the jobs that have put the objects in repositories.</li> <li>• <b>Folders By Media.</b> The report displays the associated folders for each media that you have defined in the source pane and that is involved in the archiving of objects.</li> </ul>

Parameter	Description
<b>Metadata</b>	<p>Archive metadata. These are the valid values:</p> <ul style="list-style-type: none"> <li>• <b>None.</b> Default value. The report does not display any metadata. The Metadata pane displays grayed out and you cannot access it.</li> <li>• <b>Job.</b> The report displays the metadata collected from the jobs that have put the objects in repositories.</li> <li>• <b>Object.</b> The report displays the metadata collected from the objects or instances.</li> <li>• <b>Object and Job.</b> The report displays the metadata collected from the objects or instances and the jobs.</li> </ul>
<b>Folder details</b>	<p>Details on the folder. These are the valid values:</p> <ul style="list-style-type: none"> <li>• <b>No.</b> Default value. The report displays only the source path and the cumulated Volume or number of files. The Directory Rules pane displays grayed out and you cannot access it.</li> <li>• <b>Yes.</b> The report displays: <ul style="list-style-type: none"> <li>– Recursively, all the folders that you have defined in the source pane.</li> <li>– For each folder, the volume and the number of files.</li> </ul> </li> </ul>

## Volume Management on Storage Managers Task

The Storage Manager Name field of the Volume management on storage managers task displays all the storage managers configured in Miria. You can select either all of them or only one at a time. To run the task on more than one, but not all the storage managers, configure a separate task for each.

The task scans the storage manager. If the *Use Volume Level to Trigger Retention Job* parameter is enabled on the storage manager, the task checks the *Task High Water Mark* value. If this value is attained or exceeded, the task deletes files on the storage manager until the *Low Water Mark* value is reached, or until there are no more eligible files to delete.

See [Recycling Triggered by Volume on Storage](#).

## XML Ingest Tasks

In contrast to basic automatic repository tasks, which do not permit association of metadata, the XML ingest task uses XML files to run enriched automatic archiving. It reads the XML files in a designated directory and parses them according to the rules set out in an XML schema definition (.xsd file) provided with Miria (`ada_ingest.xsd`). The `ada_ingest.xsd` file describes the structure to follow to create a valid XML file to be used by Miria.



During the installation of the Miria server, the setup installs the .xsd file and a sample XML ingest file in the Perl subdirectory (e.g., on Windows, they are located in `C:\Miria\Binary\Bin\Perl\Miria\XML`). The sample XML file is `ADA_Ingest_sample.xml`.

You can also get both these files from a browser on the Miria server using this syntax:

```
http://<Miria_server_name>:<port>/xml/ADA_Ingest.xsd
```

```
http:// <Miria_server_name>:<port>/xml/ADA_Ingest_sample.xml
```

For more information on the different parameters in the sample file, see the second table below.

In addition to the scheduling of repository tasks, the XML ingest task permits you:

- To put specific files in repositories rather than whole directories.
- To attribute metadata to files and folders.
- To put data into different repositories and folders with a single run of the task.

You are responsible for creating the XML files that launch the task. If they are not written directly with the Atempo format, you can translate them to the proper format using a stylesheet that you can request from Atempo Professional Services.

It is assumed that all repository objects invoked in the XML files have been created in Miria. Metadata and repositories must already exist within Miria. Source directories of files for repositories must exist within the file system.

This table describes the parameters displayed in the Configuration tab of a XML ingest task:

Parameter	Description
<b>Configuration.</b>	
<b>Storage platform</b>	<p>The list displays all storage platforms configured in Miria. Select the one to be used for the task. This is the machine hosting the XML files to be read.</p> <p>If the XML files must run archiving tasks on machines other than this one, the storage platform must have access rights to the other platforms.</p>

Parameter	Description
Directory	<p>Enter the root path which contains the XML file(s) that the XML ingest task must read and parse for the launching of the repository task.</p> <p><b>This must always be a path, never a file name.</b></p> <p>You can use the Select button to the right of the field to select the path, which is local to the machine that you specified in the platform.</p> <p>The XML ingest task processes all the files having the .xml extension.</p>
Recursive scan	<p>If you select this box, the XML ingest task also processes all the files having the .xml extension in the subdirectories of the directory entered in the previous field.</p>
Translator	<p>Absolute path and name of the translator .xslt file. Choose the file by clicking the Select button. If this field is populated, the XML files are not parsed according to the XML schema definition that Miria provides in the ada_ingest.xsd file.</p> <p>Instead, an .xslt file translates your XML files into XML files that conform to the ada.xsd.</p> <p>Like for the XML files themselves, it is your responsibility to create and supply the .xslt translator. On request, Atempo Professional Services can also create it.</p>

Parameter	Description
XML processing report	<p>Once the XML files have been correctly parsed and read, and the associated tasks have been launched without error, the used XML files in the XML file directory must be moved in a way that prevents rescanning the next time the task is launched.</p> <p>These are the ways in which you can perform this modification:</p> <ul style="list-style-type: none"> <li>• If the Processing Report field is not populated, the XML files are simply renamed in their original directory to prevent their rescanning. The file extension is changed from <code>.xml</code> to <code>.out</code>. The next scan ignores the files having the <code>.out</code> extension.</li> <li>• If the Processing Report field is populated, but the Translator field is not populated, then the XML files are moved from their original XML file directory to the Result Directory specified in the corresponding field. In the new directory, they are also renamed in this way: <code>originalFilename_jobNumber_ADA.xml</code>.</li> <li>• If both the XML Processing and the Translator fields are populated, then two file sets are moved into the Result Directory. The first set is as described above, and contains the translated files, named <code>originalFilename_jobNumber_ADA.xml</code>. The <code>_ADA</code> suffix indicates their conformity with the <code>ada_ingest.xsd</code>.</li> </ul> <p>The second set contains the original, untranslated XML files, named <code>originalFilename_jobNumber.xml</code> (without the <code>_ADA</code> suffix).</p> <p><b>Result Directory.</b> Path to which the XML files that have been used in an XML ingest task are to be moved after the task has</p>

Parameter	Description
	completed correctly.

Parameter	Description
<b>XML error report</b>	<p data-bbox="834 293 1417 371">In some cases the XML ingest task does not complete correctly. This happens when:</p> <ul data-bbox="847 376 1426 1099" style="list-style-type: none"> <li data-bbox="847 376 1353 409">• The XML ingest file is malformed.</li> <li data-bbox="847 414 1406 492">• The XML ingest file does not conform to the XSD file.</li> <li data-bbox="847 497 1422 651">• If you used the Translator, it could be incorrect in itself, or not translate correctly to a form that ada_ingest.xsd can read.</li> <li data-bbox="847 656 1426 734">• The files specified for repository do not exist.</li> <li data-bbox="847 739 1369 817">• Repositories requested in the XML files do not exist.</li> <li data-bbox="847 822 1382 900">• The metadata to be associated with the files put in repositories do not exist.</li> <li data-bbox="847 904 1394 1099">• The storage platform machine might not have access rights to all the machines that the XML ingest task must scan for files to put in repositories.</li> </ul> <p data-bbox="834 1122 1401 1234">In these cases, the Event logs display error messages to help you analyze the error cause.</p> <p data-bbox="834 1256 1414 1491">Additionally, if the XML ingest task rejects the XML files due to malformation or non-conformity, you must modify the rejected XML files in the XML file directory so as they are not rescanned the next time the XML ingest task runs.</p> <p data-bbox="834 1514 1390 1581">Perform this modification in either of these two ways:</p> <ul data-bbox="847 1592 1430 1951" style="list-style-type: none"> <li data-bbox="847 1592 1430 1872">• If the Error Report field is not populated, the XML files are simply renamed in the original ingest folder. The file extension is changed from .xml to .err. The next scan ignores the files having the .err extension.</li> <li data-bbox="847 1877 1430 1951">• If the Error Report check box is selected, the XML files are moved from</li> </ul>

Parameter	Description
	<p>their original directory in the XML file directory path to the Reject Directory specified in the corresponding field. In the new directory they are also renamed in this way:</p> <p><code>originalFilename_jobNumber.xml</code> (without the <code>_ADA</code> suffix).</p> <p>Thus, you can easily rename or return the files to the ingest directory after you have corrected them.</p> <p><b>Reject Directory.</b> Path to which the XML files that have been used in an XML ingest task are to be moved after the files have been rejected.</p>

This table describes the parameters displayed in the sample XML ingest file:

Parameter	Description
<code>ada_ingest_v1</code>	Allows you to configure the ingest.
<code>StartComboAtIndex</code>	<p>By default, the ComboBox in Miria goes from 1 to N, while in many client software combos start from 0 to N. The <code>StartComboAtIndex</code> parameter allows to automatically increment the index of a combo box.</p> <p><b>Example:</b> If you generate an xml by programming from a third party application, you will put index 1 for Value 2 in the metadata associated to the <code>ada_file_ingest</code> or <code>ada_folder_ingest</code> file. Miria <code>StartComboAtIndex</code> parameter will automatically replace "Value 2" by "Value 1".</p>
<code>ada_file_ingest</code>	Allows you to create and configure files.
<code>ada_folder_ingest</code>	<p>Allows you to create folders and add metadata.</p> <p>It is not possible to browse directories in the XML ingest, in this case you must have an <code>ada_file_ingest</code> tag for each file in the directory.</p>

Parameter	Description
<b>metadata_folder_action</b>	<p>Allows you to add, merge or delete metadatas on the existing folder.</p> <p>To have the exact values of this parameter, see the DTD in Binary/Bin/Perl/ADA/XML/ingest.xsd.</p>

---

## CHAPTER 14 - Monitoring

Several features are available to monitor the configuration of your migration. This chapter outlines the tools that Miria provides for monitoring jobs and events, tracking job details and histories, filtering, validating, and exporting them in a variety of formats.

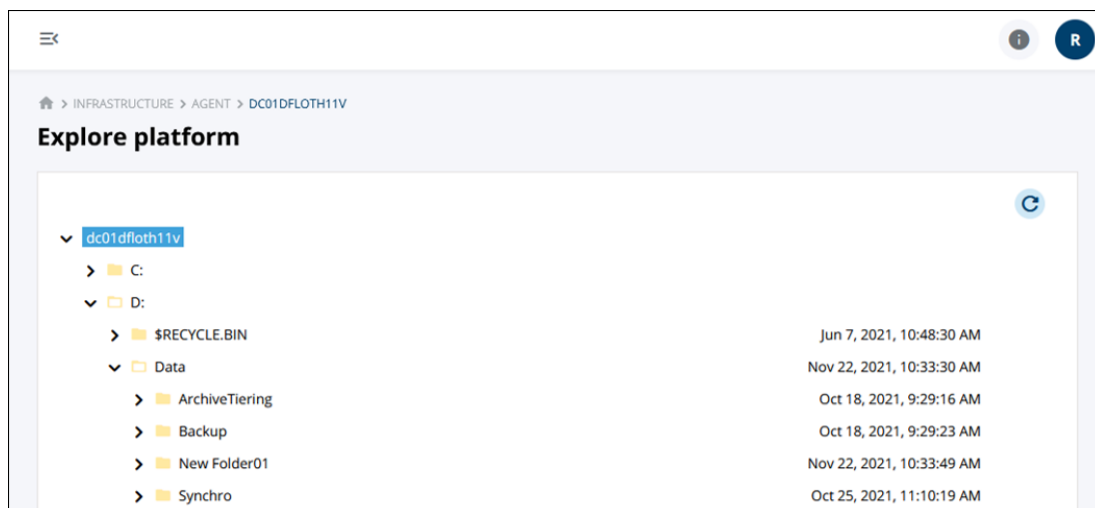
### Generate an Environment Report

1. Click the **Infrastructure** tab, then the **Agent** tile.
  2. From the list of platforms, click the **A** button.
  3. In the **Environment Report** view:
    - Click the **+** button to generate a new report.
- Or**
- Download a previous report from the list.

### Explore a Platform

The Web Interface is equipped with a check option to make sure a connection with a source or target storage is established.

1. Click the **Infrastructure** tab, then the **Agent** tile.
2. From the list of platforms, click on **👁** button. You can browse the storage to verify each element ([Figure 24](#)).



**Figure 24:** The arrow keys enable to navigate

### Test the API Connection of a Platform

1. Click the **Infrastructure** tab.
2. Select a storage (e.g., Agent, NAS etc.).



- From the list of platforms, click the **Connection** button.

## Monitor the Task Progress

- Click the **Migration** tab, then select a project.
- In the **Project overview**, select a task. When a task is started you can monitor its progress in the **Task overview** (Figure 25).

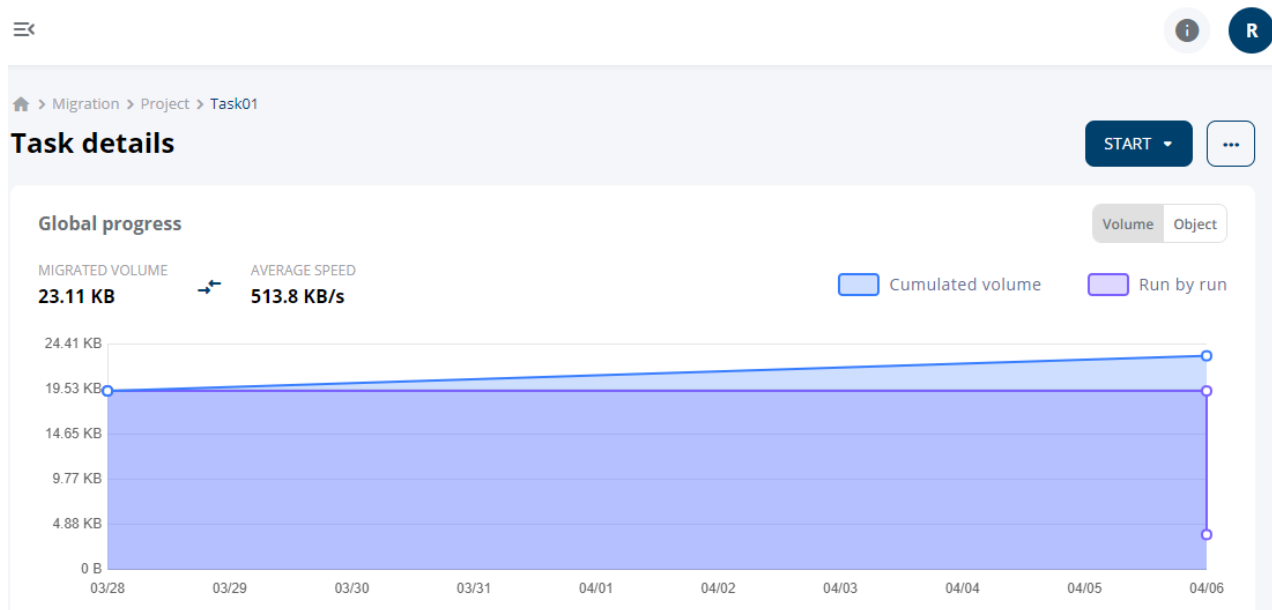


Figure 25: Global task process

## View Project or Task Logs

- Click the **Migration** tab:
  - Click the **⋮** button in a project and select **Show logs**.

**Or**


  - Select a project, then click the **⋮** button in a task and select **Show logs**.
- (Optional) In the **Logs** view, use the buttons in the upper right corner to:
  - filter the logs results.
  - refresh the list.
  - export all the logs as a CSV file.

## Perform Integrity Check

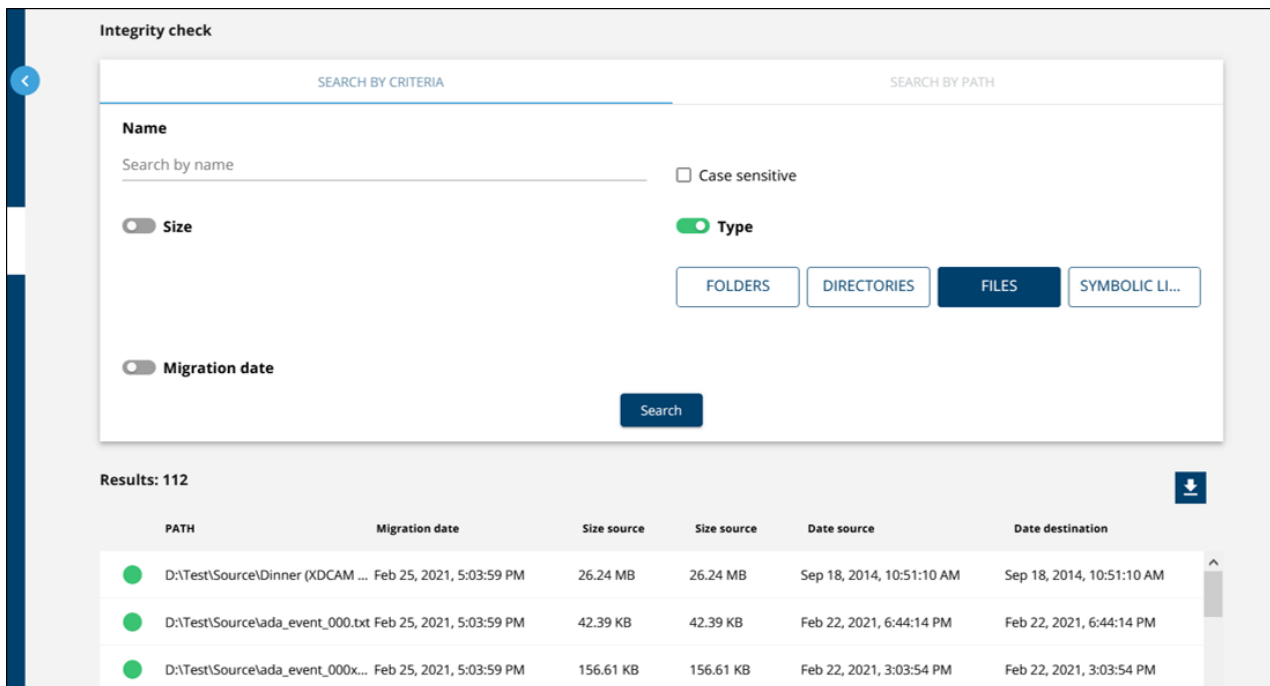
Miria lets you monitor file integrity and produce reports on migration tasks. This is useful in order to ensure that your data are correctly migrated.

If you have large data volumes, you can also choose to display and export the results in CLI mode. The command to generate the integrity results is `miria_migration_report`.

The following procedure explains how to perform an integrity check in the Web Interface.

1. Click on the **Migration** tab.
2. Select a project.
3. In the **Project overview**, select a task and click the configuration  button.
4. Click **Integrity check**. The search options are displayed.
5. Select of the following tabs to start your search:
  - **Search by criteria**. Continue with step 6 to specify all or certain criteria.
- Or
- **Search by path** to enter a specific path. Continue with step 10.
6. Enter the object name.
7. Choose the size of the object.
8. Select object types.
9. Set the start and end date within which the migration took place.
10. Click on **Search**. If too many results show up, you can stop the search.

The results are displayed below the search criteria ([Figure 26](#)).




The screenshot shows the 'Integrity check' window with two tabs: 'SEARCH BY CRITERIA' (active) and 'SEARCH BY PATH'. Under 'SEARCH BY CRITERIA', there are input fields for 'Name' (with a 'Search by name' placeholder), 'Size' (disabled), 'Migration date' (disabled), and 'Type' (enabled). There are also checkboxes for 'Case sensitive' and buttons for 'FOLDERS', 'DIRECTORIES', 'FILES' (selected), and 'SYMBOLIC LI...'. A 'Search' button is at the bottom right of the criteria section. Below the search section, it says 'Results: 112' with a download icon. A table displays the results with columns: PATH, Migration date, Size source, Size source, Date source, and Date destination. The first three rows are visible, each starting with a green circle icon.

PATH	Migration date	Size source	Size source	Date source	Date destination
D:\TestSource\Dinner (XDCAM ...	Feb 25, 2021, 5:03:59 PM	26.24 MB	26.24 MB	Sep 18, 2014, 10:51:10 AM	Sep 18, 2014, 10:51:10 AM
D:\TestSource\lada_event_000.txt	Feb 25, 2021, 5:03:59 PM	42.39 KB	42.39 KB	Feb 22, 2021, 6:44:14 PM	Feb 22, 2021, 6:44:14 PM
D:\TestSource\lada_event_000x...	Feb 25, 2021, 5:03:59 PM	156.61 KB	156.61 KB	Feb 22, 2021, 3:03:54 PM	Feb 22, 2021, 3:03:54 PM

**Figure 26:** Integrity check results

You can perform the following actions:

- See information about the object, source and destination size and digest, and the reference date.
- Click the **Export**  button to export results in a CSV file with the last iteration of the object.

## APPENDIX Configure an Isilon Storage

Isilon OneFS provides an API to manage volumes and snapshots. When running a Synchronization task in incremental mode, Miria uses Isilon FastScan to generate reports on the differences between two snapshots. The Isilon API also lets you manage:

- Clusters.
- Monitoring functionalities.
- Files and directories on the cluster.

Requests are sent to the API through a REST (Representational State Transfer) interface, by calling HTTP methods to dedicated URLs.

### Isilon NAS Platform Prerequisites

For Miria to support the Isilon NAS platform and the FastScan functionality, you must:

- Allow the agent to access the Isilon file system. To do so, the Isilon cluster must have:
  - A NFS export mount point on the Unix/macOS agent.
  - Access to the share via a login and password.

When configuring Isilon for NFS export, it is recommended to add the Unix/macOS agent to the *Root Client* list. This allows the agent to write files on the Isilon cluster as the `root` user. For details, see Isilon Web Administration Interface.

- Assure that the agent for Isilon 7.2 can run SSH (Secure Shell) commands on the Isilon cluster. The user must be defined in the **Connector** tab. For Isilon 8.x, all necessary actions are supported by the REST API.
- Ensure that Miria agents supporting the Isilon API are Windows and Unix-64 bits.
- Verify that Miria supports the Isilon OneFS versions 7.2, 8.0 and 8.1. For details, see the Isilon OneFS Web Administration Interface.
- Set cluster Encoding to `UTF-8`.
- Have a valid licensed SnapshotIQ module for the Isilon OneFS Cluster. For details, see the Isilon OneFS Web Administration Interface.
- Have a valid Miria license for the FastScan functionality.
- **Isilon OneFS 8.0 and higher.** Ensure that the `ChangelistCreate` job is enabled on the Isilon configuration.

#### *To check that the `ChangelistCreate` job is enabled*

1. From the Isilon Web Administration Console, select **Job Operations > Job Types**.
2. Edit the `ChangelistCreate` job details.
3. In the **Edit Job Type Details** window, ensure that **Enable this Job Type** check box is selected.

### Stream Options

String representing the stream behavior.

For an Isilon NAS, you can define the stream options in the **Properties** pane, **NAS** tabs, **Windows (CIFS)** and/or **Unix/MacOS (NFS)** tabs.

**Examples of Options:**

- `host=` This option is mandatory if several data movers must migrate the data. The value is the name of the directory to be migrated. It must be specified identically on each data mover.
- `source_roaming=` On a clustered Isilon architecture, you may collect the data to migrate from several Isilon nodes instead of only one. This enables you to optimize the bandwidth, particularly when migrating a large number of files.

Use the Isilon syntax to complete the **Stream Options** field. For instance, to specify that the data located in `/mnt/isilon1` can also be accessed from `/mnt/isilon2` and `/mnt/isilon3`, enter this command:

```
source_roaming=/mnt/isilon1,/mnt/isilon1-/mnt/isilon2-/mnt/isilon3
```

## APPENDIX Create a Nutanix User Account

Nutanix enables you to create a user account in the Nutanix command-line interface (nCLI). To proceed, you first need to download and install the nCLI on any server in your infrastructure.

1. Start the utility and establish a nCLI session launching the following command: `ncli -s management_ip_addr -u 'username' -p 'user_password'`
  - `management_ip_addr` IP address of any Nutanix Controller VM in the cluster.
  - `username` Username to access the Controller VM. If not specified, admin will be used as a default name.
  - `user_password` Password to access the Controller VM.
2. Run the `fs list` command to obtain the list of Nutanix File Servers.
3. Locate the name of the Nutanix File Server you want to audit.
4. Save the Uuid (Nutanix Files server ID) parameter to a text file.
5. To create a new user and specify credentials that will be used to access this Nutanix Files server, run the following command:

```
fs add-user uuid=<fs_uuid> user=<username> password=<password>
```

**Example:** `D:\Docs\Nutanix\ncli>ncli -s 172.20.30.58 -u admin -p password`

## APPENDIX Recycling Triggered by Volume on Storage

Recycling can also be triggered when a level of volume occupancy is exceeded on the storage. Volume-triggered recycling is used with multiple storage managers. It is non-destructive in that it only deletes data for which Miria has another copy. The purpose of such recycling is to free up space on more expensive, near-line storage by deleting files which also exist on a more economical, deeper storage.

These are the two methods:

- **On demand recycling** Job launches the On demand recycling based on the High Water Mark parameter. When the high water mark in the storage manager is reached, the archiving job stops and a retention job starts running. The retention job deletes files until the data volume reaches the low water mark. The advantage of this approach is that it is on demand. The storage manager is emptied in direct response to your need for space. The disadvantage is that this approach interrupts the archiving job until the retention job completes.
- **Scheduled control of storage occupancy** Volume management on storage managers task performs a monitoring of storage occupancy. At regularly scheduled intervals, this task monitors Miria storage managers. On each storage manager where volume management is enabled, it determines whether the task High Water Mark value is set. If so, it analyzes whether the volume of archived data on the storage manager has attained or exceeded the water mark. If it has, the task triggers a retention job that deletes files until the volume of archived data reaches the Low Water Mark parameter, or until there are no more files eligible for deletion. The advantage of this approach is that it anticipates storage needs and does not interrupt archiving jobs.

These are the options when Volume management is enabled ([Table 8](#)):

**Table 8:** Triggering methods

	On demand recycling	Scheduled monitoring
<b>High Water Mark</b>	<p><b>Required</b> Select the box and set a value in GB.</p> <p>When this value is attained, a retention job is triggered.</p>	<p>Used for jobs and is not needed to launch the Volume management on storage managers task.</p> <p>Do not use this setting as it takes precedence over the Task High Water Mark option if set to a lower value.</p>

	On demand recycling	Scheduled monitoring
<b>Task High Water Mark</b>	Ensure this option is not selected, unless you also want to activate scheduled monitoring.	<b>Required</b> Select the box to activate the Volume management on storage managers task on this storage manager. For coherent use of on demand and scheduled monitoring recycling, set the GB value to be between high and low water marks.
<b>Low Water Mark</b>	<p><b>Required</b> Select the box and set a value in GB.</p> <p>The retention job attempts to delete files until the data volume reaches this value. If there are no more eligible files (e.g., it has deleted all files having a second copy and all the files still in the storage manager are single copies), it stops before this water mark is reached.</p>	<p><b>Required</b> Select the box and set a value in GB.</p> <p>The retention job attempts to delete files until the data volume reaches this value. If there are no more eligible files (e.g., it has deleted all files having a second copy and all the files still in the storage manager are single copies), it stops before this water mark is reached.</p>





# APPENDIX Replications in between two S3 object storages

## ***What is replicated:***

- Filename
- Data
- All user defined metadata (wide open area in S3)
- Only one system defined metadata: content type
- Access Control List (ACL)
- Object Lock values

## ***What is not replicated:***

- Last modification time (mtime). It is not possible to re-apply it, but Miria stores the original value coming from source in an user defined metadata at target.
- VersionID: it is not possible to re-apply it, because VersionID is defined on the server side.
- **Everything else that is not listed in the first list above is not replicated.**