



Miria for Backup Documentation

Miria 4.0

Publication Number: MIRIA-BAC-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 Backup	1
CHAPTER 2 - Product Installation	3
Prerequisites	3
Port Number Matrix	3
Install	4
Install Additional Agents or Data Movers (Optional)	4
Manage the License	5
CHAPTER 3 - Connect to Miria Web Interface	7
CHAPTER 4 - Manage the Infrastructure	8
Add a Storage Manager and Container	8
File Storage Container	9
File Storage One to One	10
SnapStor	12
Virtual Storage	13
Media Storage	13
Easy move Amazon S3	15
Google Cloud Storage	17
Microsoft Azure Blob Block	18
Scality	20
Quantum Active Scale	22
Seagate Lyve Cloud	24
Cloudian HyperStore	25
Add Server and Agent(s)	27
Add a New NAS Platform	28
Add a Storage Platform	29
Add a Shared File System	29
Activate My File System	30
Available options	31
Edit a Platform	32
Platforms Permissions	32
Metadata	33
CHAPTER 5 - Configure Policies	35
Add a New Policy	35
Edit a Policy	36
CHAPTER 6 - Organize and Configure a Backup Project	38
Organize Projects	38

Project description	38
Task description	39
Configure the Backup	39
Create a New Project	39
Create a New Backup Task	39
Create a New Tiering Task	41
Edit a Project	42
Edit a Task	42
Start Task(s)	42
Duplicate a Task	43
Disable a Project or a Task	43
CHAPTER 7 - Move Data	44
Archive Data	44
Copy, Move, Synchronize Data	45
Retrieve Data	46
Relaunching an Easy Move Job	46
CHAPTER 8 - Organize Repositories	48
Repository Types	48
Repository Organization	48
Folders and Sub-Folders	48
Archived Directories and Files	48
Manage Repositories	48
Add Folder	49
Rename Object	49
Delete Object	49
Permissions on the Repositories	50
Manage Metadata	51
Applying Metadata to Repositories	52
Manage Instances	53
Retrieve Instance	54
Instance Details	56
Session Details	58
CHAPTER 9 - Manage Users	59
Add a User	59
Edit a User	60
Add a User Group	60
.....	62
Configure SAP	62
Set Password Policies	63
Add a LDAP Rule	64

Add a LDAPS Rule	64
Edit a Rule	64
Set the Two-Factor Authentication	64
Configuring a Two-Factor Authentication Set as Mandatory	65
Configuring a Two-Factor Authentication Set as Optional	66
CHAPTER 10 - Advanced Tasks	69
Task Types	69
Internal Management Tasks	69
Data Movement Tasks	70
Creating a Task	72
Creating a New Task from the Tasks Tab	72
Duplicating an Existing Task	72
Organizing tasks	72
Manage projects	73
Move a task	73
How Tasks Run	73
Testing a Task	75
Launching a Task Manually	75
Canceling a run	75
General Configuration Parameters for Tasks	76
General Parameters Common to All Tasks	76
Common Tabs	78
Task-specific Parameters	81
Automatic Catalog Ingest Task	81
Automatic Deletion Task	84
Automatic Retention Tasks	85
Automatic Storage Repack Task	86
Database Backup Task	87
Maintenance tasks	87
Archive Report Task	90
Volume Management on Storage Managers Task	92
XML Ingest Tasks	92
CHAPTER 11 - Monitoring	100
Generate an Environment Report	100
Explore a Platform	100
Test the API Connection of a Platform	100
View Project or Task Logs	101
APPENDIX Configure an Isilon Storage	102
Isilon NAS Platform Prerequisites	102
Stream Options	102

APPENDIX Recycling Triggered by Volume on Storage	104
APPENDIX Replications in between two S3 object storages	106

CHAPTER 1 - About Miria for Backup

Miria for Backup is a software appliance developed by Atempo that allows administrators to backup and restore large file storages, Object, Cloud and NAS.

This document instructs users on how to configure and manage data backup projects.



CHAPTER 2 - 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](#)
- Download the latest GA release from <https://support.atempo.com>.
- Gather Host MAC Address to generate the license.
- Prepare a desktop or X-term environment to install Miria agents on the servers and data movers. Installation binaries are GUI-based.

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
Web Interface							
Acces Server	Admin Console @IP	Server	Server @IP	HTTP TCP	80	IN	Port automatically opened by Setup
Acces Server SSL	Admin Console @IP	Server	server @IP	HTTPS TCP	443	IN	Port automatically opened by Setup
Data Mover							
Engine Port	Agent @IP	Server	Server @IP	TCP	2524	IN	Port automatically opened by Setup
Miria Server / DB							
PostgreSQL Server	Server @IP		Server @IP	TCP	5433		PostgreSQL Server / No need to open
Other							

Table 1: Port numbers per component

From Component	From @IP	Destination Component	To @IP	Protocol	Port	FWRule	Comment
Server	Server @IP	Mail Server	SMTP Server @IP	TCP	25 / 2525	OUT	Port needed for mail notification
External storage	Server @IP	Cloud/S3 like storage	Provider @IP	TCP	Provider dependant	OUT	Port needed in function of target cloud/S3 storage
NFS	Server @IP	NFS Storage	Storage @IP	TCP/UDP	111	OUT	
				TCP/UDP	2049	OUT	
CIFS	Server @IP	CIFS Storage	Storage @IP	UDP	137-138	OUT	
				TCP	139 / 445	OUT	

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.

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 1](#)).

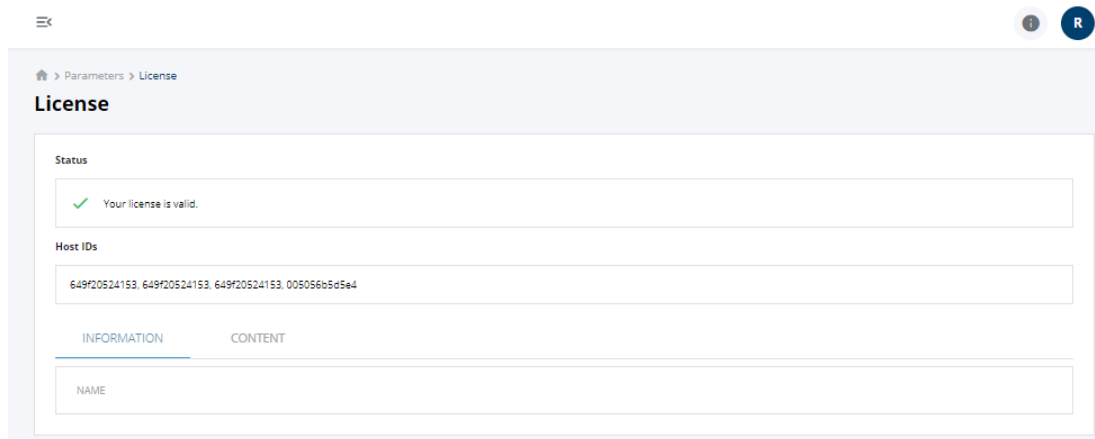


Figure 1: A valid product license in the Web Interface

CHAPTER 3 - Connect to Miria Web Interface

1. Open a web navigator.
2. Type the server URL: <Miria server IP Address>/webapp-en. If you want to display the interface in French or Chinese you can enter webapp-fr or webapp-zh. The login window is displayed.
3. Enter your authentication information:
 - **Username** Name of the user as defined in Miria Administration Console.
 - **Password** Password associated with the specified username.
 - **Database** The database instance that you want to use. This field only displays in case of multiple databases.
4. Click **Login**.

CHAPTER 4 - Manage the 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 2](#)).

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

The following tiles are available:

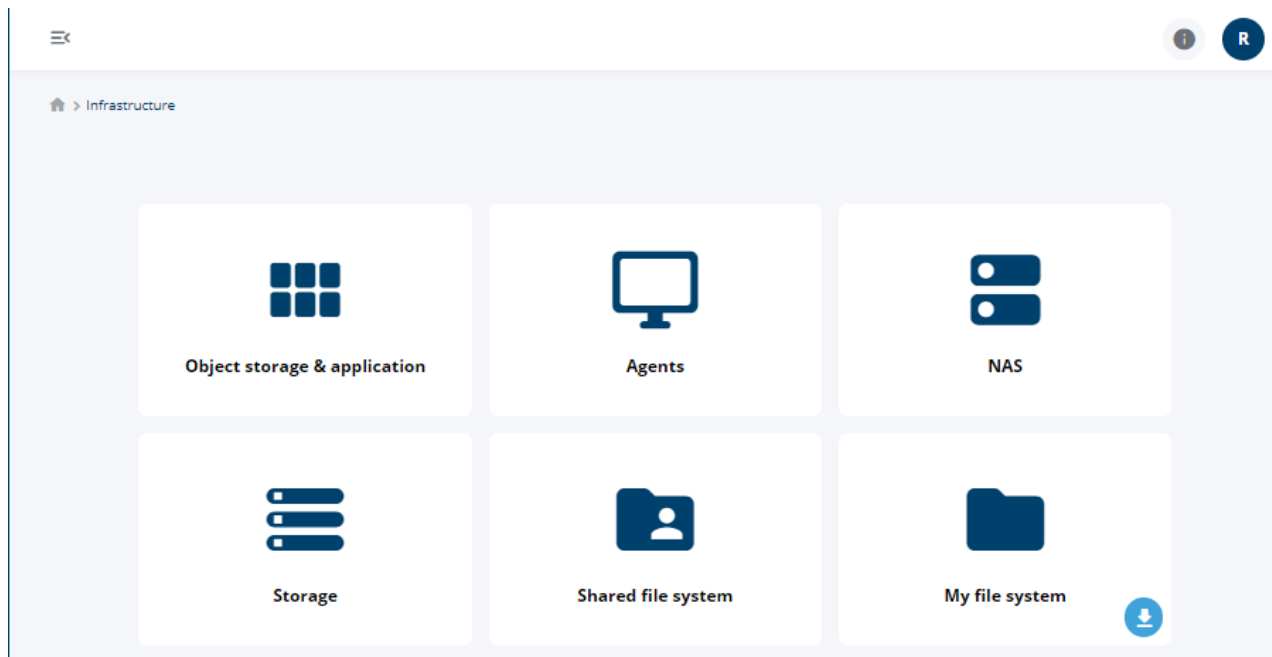


Figure 2: Storage types sorted by list in the **Infrastructure** interface

- **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.
- **My file system** Activate and access My file system to perform data-move operation from and to the local 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).

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

Virtual Storage

Step 1: Add a storage manager

1. Click the **Infrastructure** tab, then **Object Storage & Application**.
2. Click **New storage manager**.
3. Select **Virtual 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. 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.
7. 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.
3. Click **Add container** to select a storage manager container from the list. Then click **Add**.
4. 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

1. Click the **Infrastructure** tab, then **Object Storage & Application**.
2. Click **New storage manager**.
3. 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 .
 - c. **Archiving run lock.** A new one can be created, by clicking the .
 - 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 .
 - 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 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.sca11;s3.sca12:s;s3.sca13:1523s`




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 Scality 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 Scality 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 Scality storage. Refer to your Scality 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.

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 3](#)).

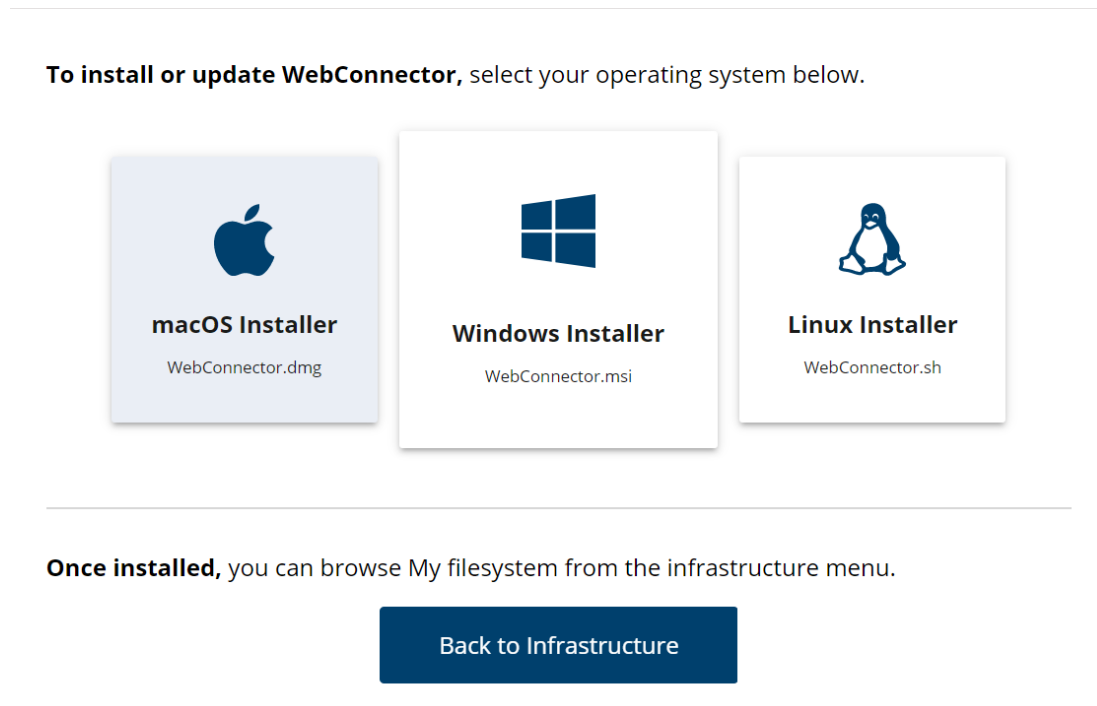


Figure 3: Installer selection

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 4](#)).

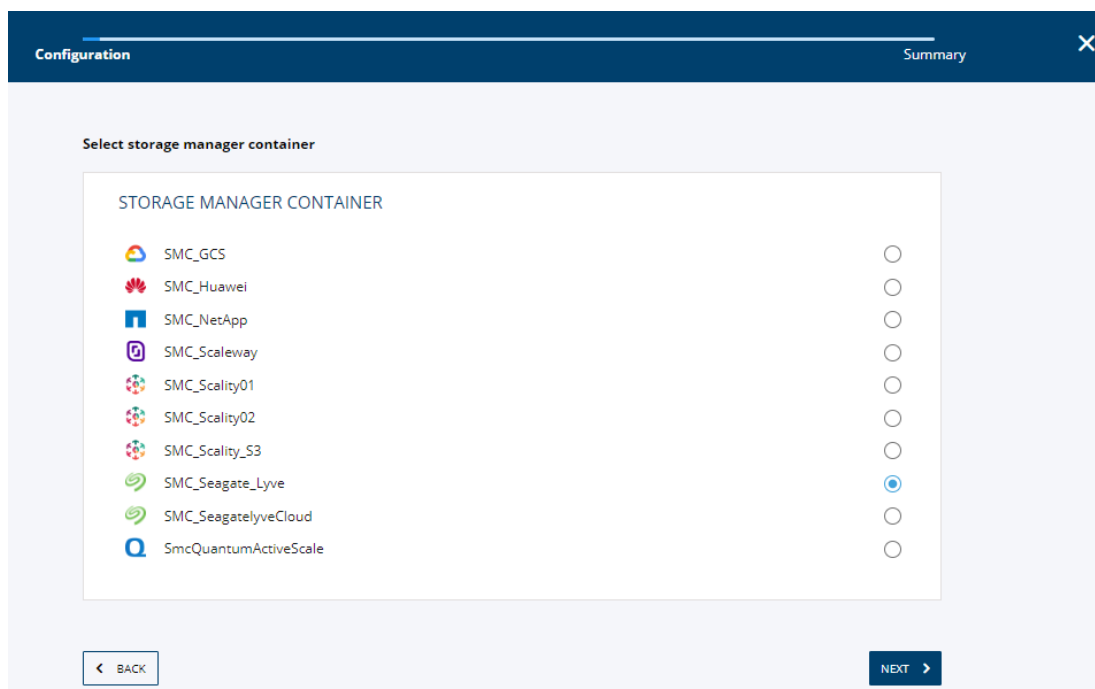


Figure 4: Example displaying a Nutanix NAS configuration that can be edited in the wizard

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

CHAPTER 5 - Configure Policies

The policy associates the storage manager container(s) with a retention. It enables you to define which storage manager container(s) to use and how long each container retains the data.

Before configuring a policy, you must create at least one storage manager container and one retention period. See [Add a Storage Manager and Container](#).

Add a New Policy

Step 1: Connection

1. Connect to the Web Interface.
2. Click the **Policies** tab, then the **Add new policy** button at the top right. The policy configuration window is displayed (see Figure).

Figure 5: The policy configuration window

Step 2: Configuration

Enter the configuration parameters:

- **Name** Name that identifies this policy within Miria.
- **Global retention** Period of time for which backed up files are preserved:
 - Choose the retention period from the list.
- **Or**
 - Click the + icon to add a new retention to the list.
- **Deduplication reference** Select the name of the reference storage manager container from the list.
- **Reduce IO impact on source platform** If this option is set, data are transferred from the platform to only the first storage manager container in the list. Subsequent writings use the



first storage manager container as the source, transferring data from there without reconnecting to the source platform. This reduces network traffic and IO impact on the source platform.

Step 3: Association


Associate the policy with at least one of the storage manager containers that have been configured:

1. Click **+ New target** to open the **Target** pop-up window (see Figure).

Figure 6: The target configuration window

2. In the **Target** list, select the storage manager container you want to use.
3. If needed, select the **Custom retention** option and define a retention period in the list.
4. Click **Add**.
5. If needed, repeat the previous steps and reorder the list:
 - You can drag and drop the rows to raise or lower a container in the order in which it is searched when a retrieval is requested.
 - You can click the  and  icons under the **Actions** column to respectively edit or remove a container from this list.
6. Click **Create**.

Edit a Policy

1. Click the **Policies** tab.
2. From the list of policies, click the  button. The current policy configuration is displayed (Figure 7).

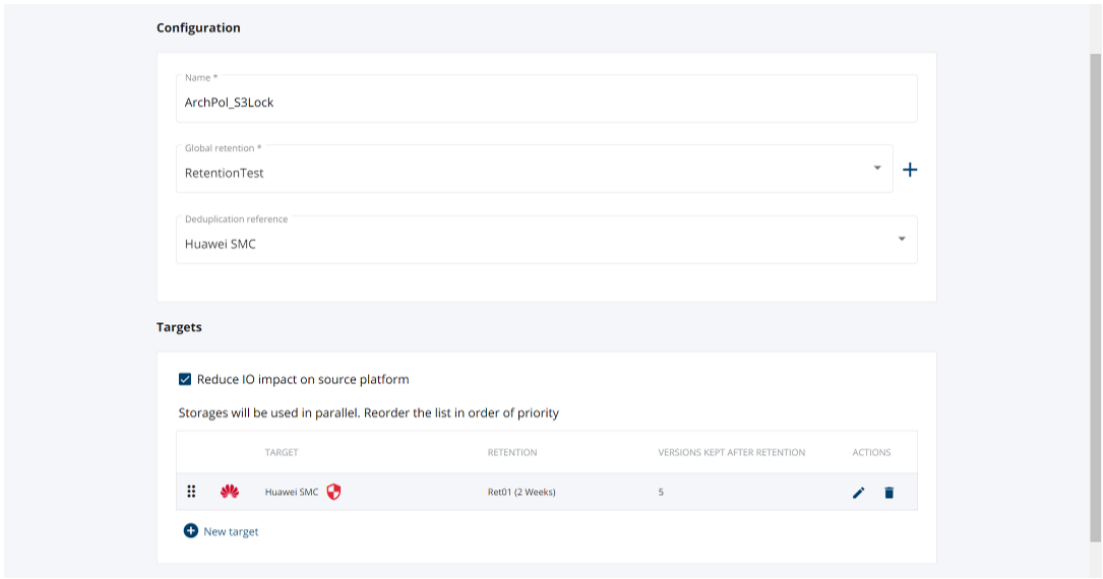


Figure 7: Example displaying a policy configuration that can be edited

- 3. Update the policy configuration and click **Update** to save modifications.

CHAPTER 6 - Organize and Configure a Backup Project

The **Backup** entry in the Web Interface is used to create and manage backup projects and tasks.

> Click the **Backup** tab.

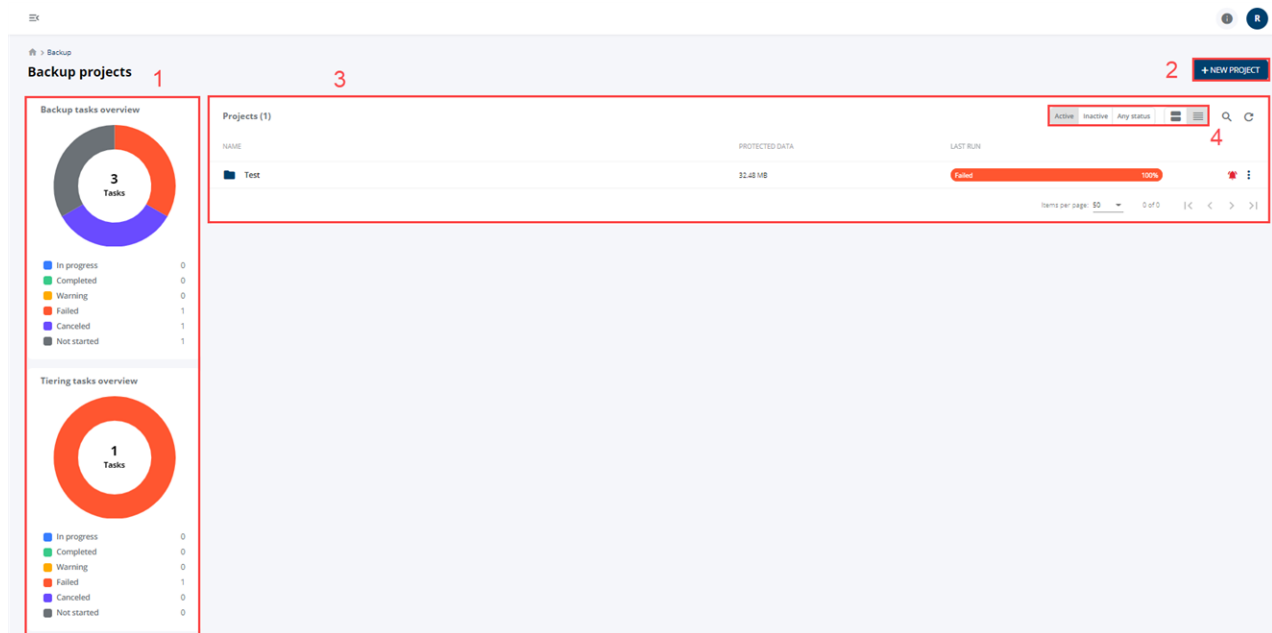


Figure 8: 1. Backup and tiering tasks; 2. Add new project; 3. Current projects; 4. Project representation

The following information can be displayed on backup projects and tasks (Figure 8):

- Status of backup and tiering tasks.
- Backup projects, the volume of protected data and the number of tasks created within a project.
- Projects can appear as individual tiles or in a list.

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 backup.

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

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

- See an overview of configured backup tasks and tiering tasks within a 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. 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 Backup

This section outlines how to create a backup project and add tasks within it.

Create a New Project

1. Click the **Backup** tab, then the **New project** button.
2. Enter the desired name and click **Create**.

Your project is created.

Create a New Backup Task

The automatic backup task is aimed at automating the backup of specified directories and files. This task enables you to schedule both full and incremental backups into a single task.

The DDN IntelliFlash FastScan NAS helps you to reduce the time needed for an incremental backup.

Note: Before creating a backup task, you must have configured a policy.

Step 1: Create a new task

1. In the **Backup** tab, select the project to create a task within it.
2. In the upper right corner, select **Add > New backup task**. The task configuration wizard is displayed ([Figure 9](#)).

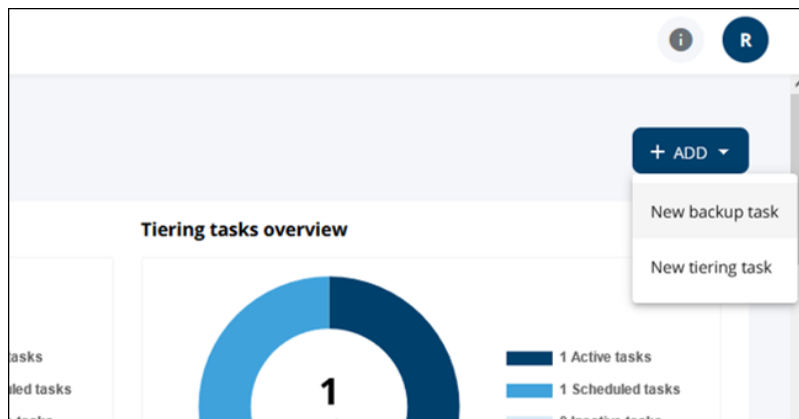


Figure 9: Add a new backup task

Step 2: Select a source and a target

1. Enter the name of the backup task.
2. Select a source platform. This is the root of the path from which the backup job is to search for files and directories on the platform.
3. Select a target and set the following options:
 - a. Select a repository name or create a new one in which the data will be backed up.
 - b. Activate **Full path auto-generated** if the data must be backed up at the root of the selected repository. Miria controls the path. The task replicates the file tree of the source directory in the target repository.
 - c. Activate **Backup repository** if the data must be backed up in the repository of your choice.
4. Select a policy to apply.
5. Click **Next**.

Step 3: Back up objects

1. Explore the source platform and add objects to backup.
2. Repeat step 1 for each object to backup. Added objects can easily be removed from **Your selection** by clicking the button.
3. Include or exclude objects if the backup selection needs to be refined.
4. Click **Next**.

Step 4: Schedule full and incremental backups

1. Enable a backup schedule (full and/or incremental).
2. Set following options for tasks to be launched:
 - Day(s) of the week.
 - Intervals at which the task is launched in the month (e.g., the first Sunday or third Friday).
 - Time(s) of the day.

Example 1: A task must be launched at 04:45: Choose 4 Hours and 45 Minutes. If you select Every 5 minutes, the task runs every five minutes during the hours that you specify under Hours.

Example 2: A task must be run between 03:00 and 05:00 and relaunched every five minutes: Select 3 and 4 Hours and Every 5 minutes. This option is useful when you have source material that is constantly changing.

3. Click **Next**.

Step 5: Set additional options

1. If needed and if snapshot management is available on the source, activate snapshots.
2. Enable **Jobs Parallelization** to accelerate data movements. This feature is particularly useful for large volumes of data as it enables you, for instance, to back up to multiple tape drives simultaneously. If enabled, set following options:
 - a. Maximum number of jobs that can run in parallel.
 - b. Create a job after:
 - Period of time assigned to the task to browse the file system and build up a file selection.
 - Maximum size that the file selection can reach. The default value is 1,024 GB.
 - Maximum number of files that the file selection can reach. The default value is 250,000 files.

If only one of the limits (time, size, or number of files) is set, enter 0 in the field that the task must ignore. You can set to 0 only one of these fields. The limit(s) that you set to the file selection should be enough for the task to select a sufficient number of files to feed a job, but not too much as to leave drives idle if writing to tape. See also Parallel Jobs - Use Case in Miria Administration documentation.

3. Enable **Commands** to be able to enter the full path of any scripts you want to launch before or after the task is run.
4. Enable **Retention of deleted objects** to be able to define an additional retention for backed up objects which were deleted at the source.
5. Click **Next**.

Step 6: Summary

1. Read the summary of the task.
2. Click **Create** to add the backup task.

Create a New Tiering Task

The automatic tiering task allows you to replicate data backed up on one storage to another storage. For tiering to work, the storage for the filter and the storage for the policy must point to the same agent.

Step 1: Create a new task

1. In the **Backup** tab, select the project to create a task within it.
2. In the upper right corner, select **Add > New tiering task**. The task configuration wizard is displayed.

Step 2: Select a source and a target

1. Enter the name of the tiering task.
2. Select a repository.

3. Select the data you want to replicate. This can be a complete repository, a directory or a folder.
4. In the **Filter** section, click the **New filter** button.
5. Select the storage manager containers where the data are located. This can be a File Storage One to One or a File Storage Container.
6. Select a policy to apply.
7. Click **Next**.


Step 3: Set task options

1. Select the task mode:
 - Full**Or**
 - Incremental
2. Enable **Scheduling** to specify the days of the week, hours and recurrence of tiering tasks to be run.
3. Enable **Jobs Parallelization** to accelerate data movements.


Step 4: Summary

1. Read the summary of the task.
2. Click **Create** to add the tiering task.

Edit a Project

1. Click the **Backup** 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 **Backup** 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 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.

To start a backup task

1. Select the project.
2. In the **Tasks** section, click the button of a task.
3. Choose one of the following options:
 - Start task in full mode.
 - Start task in incremental mode.

- Start task in test full mode.
- Start task in test incremental mode.

To start all backup tasks

1. Click the button of a project.
2. Choose one of the following options:
 - Start all tasks in full mode.
 - Start all tasks in incremental mode.
 - Start all tasks in test full mode.
 - Start all tasks in test incremental mode.

Only backup tasks can be launched in full or incremental mode.


To start a tiering task

1. Select the project.
2. In the **Tasks** section, click the button of a task.
3. Choose one of the following options:
 - Start task.


Or

 - Start task in test mode.


Duplicate a Task

1. Click the **Backup** 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 **Backup** 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 7 - Move Data

The **Easy Move** interface is divided into a source area and a target area (Figure 10).

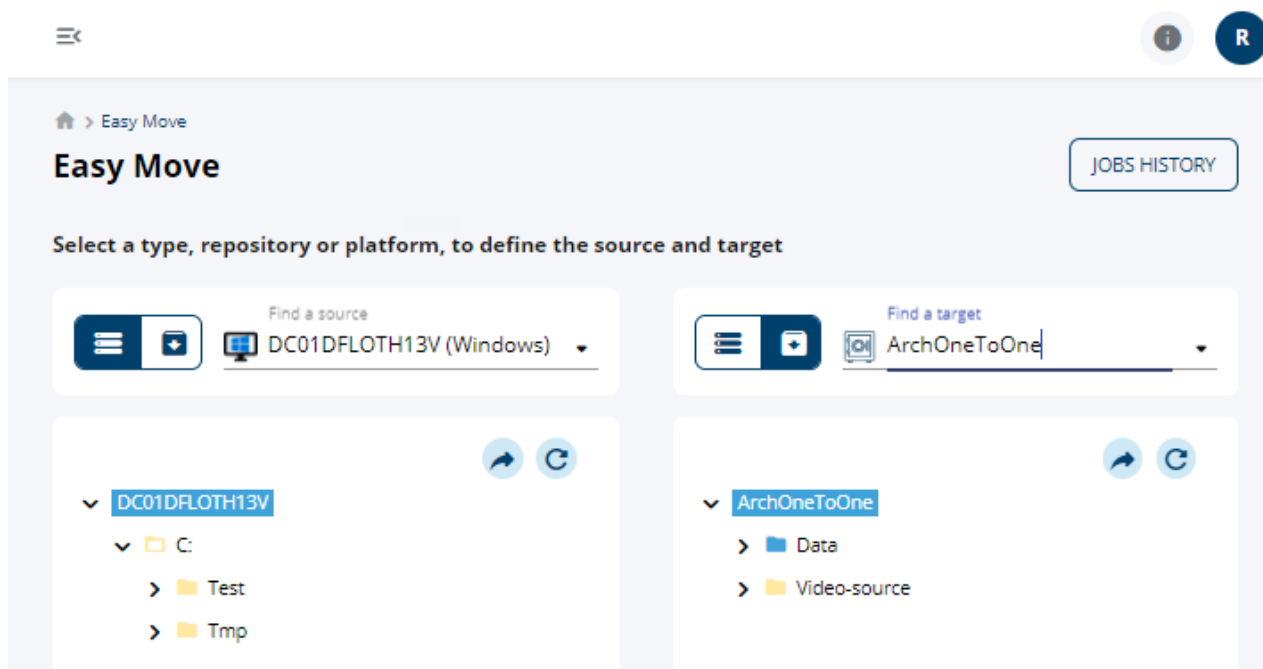


Figure 10: Easy Move interface with a source and target selection

Move operations always go from a source on the left to a target on the right. You can perform the following actions:

- **Archiving** Moving data to a storage location where it remains available for future retrieval.
- **Retrieval** Transfer data from the storage location to your workstation or any other computer where you can view or edit it.
- **Copying** Copy data from one platform to another. The data will be present on both the source and target platforms.
- **Moving** Move data from one platform to another platform. The data will no longer be present on the source platform and is available on the target platform.
- **Synchronizing** Compare a source data directory with a target data directory. An object present on the source but missing from the target is copied into the target.
- **Relaunching a job** Through the **Jobs history** button, you can access **Easy Move** jobs history and relaunch a job, without having to reconfigure it.

This chapter explains how to perform each one of these tasks with Easy Move.

Archive Data

1. In the Web Interface, click the **Easy Move** tab.
2. In the left field, select the source type as **Platform** and find your source (Figure 11).

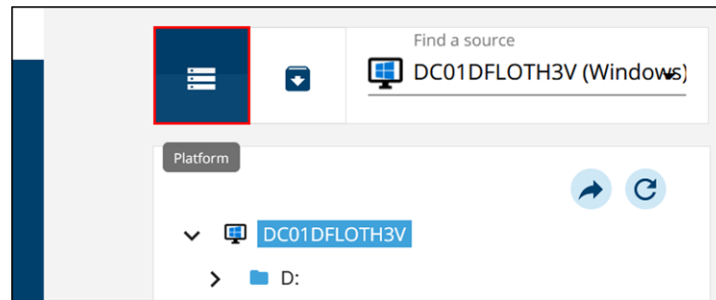


Figure 11: Platform selected as source

3. In the right field, select the target type as **Repository** and find your target.
4. Explore the file tree of the platform and select the object you want to move.
5. Explore the file tree of the repository and select the destination folder or directory. You can also add a new folder.
6. Move the object:
 - Click **Add**.
- Or
- Drag the object from the source to the desired location in the target.
7. Repeat steps 3, 4 and 5 for each move you want to perform.
8. Validate the basket.
9. If the administrator has configured metadata, enter a value for the metadata of your choice and click **Continue**. The archiving job is launched.
10. Click the **Jobs** tab to verify the job progress.

Copy, Move, Synchronize Data

1. In the Web Interface, click the **Easy Move** tab.
2. Select the source and target types as **Platform** and find your source and target (Figure 12).

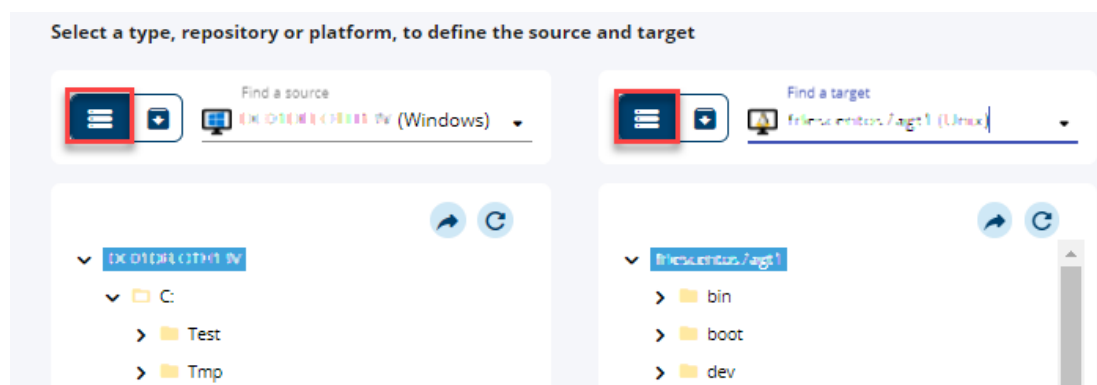


Figure 12: Platform selection

3. Explore the file tree of the source platform and select the object you want to move.
4. Explore the file tree of the target platform and select the destination directory.
5. Move the object:
 - Click **Add**.

Or

- Drag the object from the source to the desired location in the target.
- Repeat steps 3, 4 and 5 for each move you want to perform.
 - Choose the task to perform: **Copy**, **Move** or **Synchro**.
 - Validate the basket.
 - Click the **Jobs** tab to verify the job progress.

Retrieve Data

- In the Web Interface, click the **Easy Move** tab.
- In the left field, select the source type as **Repository** and find your source ([Figure 13](#)).

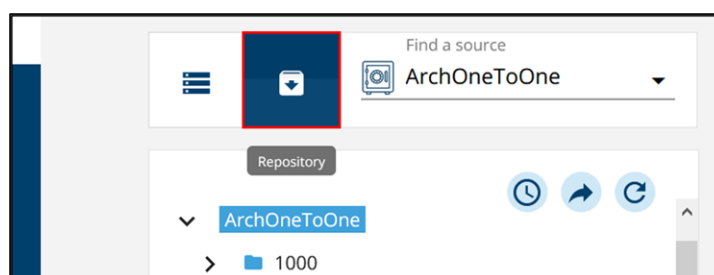
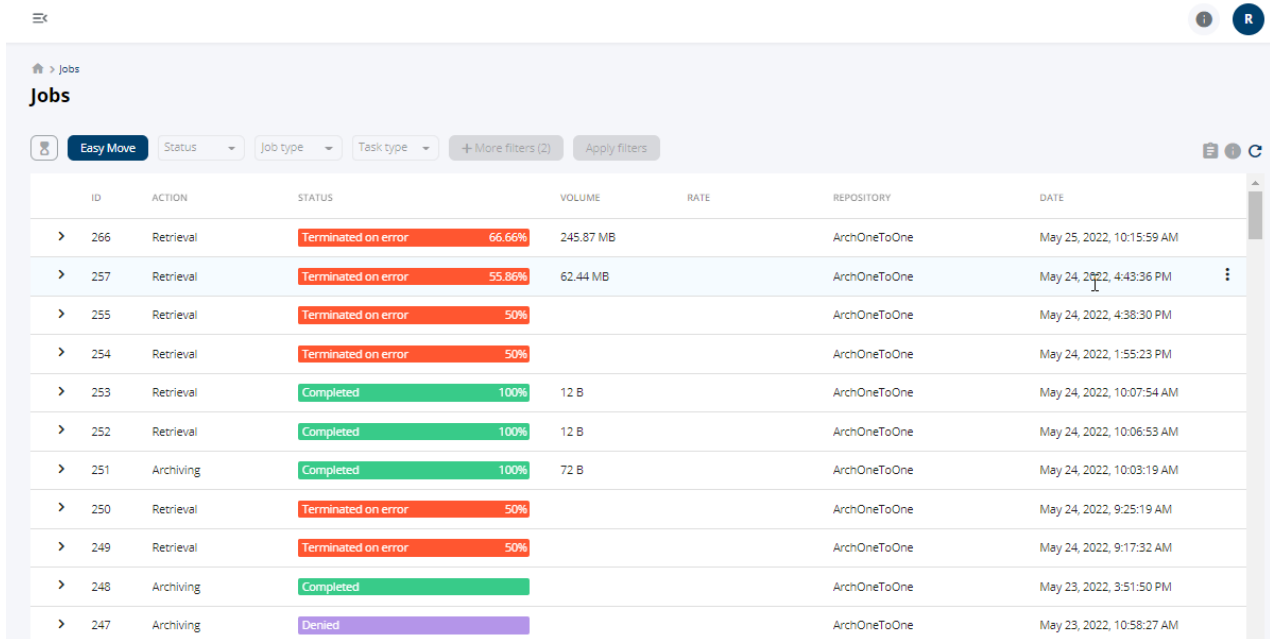


Figure 13: Repository selection

- In the right field, select the target type as **Platform** and find your target.
 - Explore the file tree of the repository and select the object you want to retrieve.
 - If needed, click the **Time line** ⌚ button to use time navigation and retrieve data at a specific date and time.
 - Explore the file tree of the platform and select the destination directory. You can also add a new directory.
 - Move the object:
 - Click **Add**.
- Or**
- Drag the object from the source to the desired location in the target.
- Repeat steps 3, 4 and 5 for each move you want to perform.
 - Validate the basket. The retrieval job is launched.
 - Click the **Jobs** tab to verify the job progress.

Relaunching an Easy Move Job

- In the Web Interface, click the **Easy Move** tab.
- Click the **Jobs history** button. The **Jobs** pane opens ([Figure 14](#)). The **Easy Move** filter is selected.



ID	ACTION	STATUS	VOLUME	RATE	REPOSITORY	DATE
266	Retrieval	Terminated on error 66.66%	245.87 MB		ArchOneToOne	May 25, 2022, 10:15:59 AM
257	Retrieval	Terminated on error 55.86%	62.44 MB		ArchOneToOne	May 24, 2022, 4:43:36 PM
255	Retrieval	Terminated on error 50%			ArchOneToOne	May 24, 2022, 4:38:30 PM
254	Retrieval	Terminated on error 50%			ArchOneToOne	May 24, 2022, 1:55:23 PM
253	Retrieval	Completed 100%	12 B		ArchOneToOne	May 24, 2022, 10:07:54 AM
252	Retrieval	Completed 100%	12 B		ArchOneToOne	May 24, 2022, 10:06:53 AM
251	Archiving	Completed 100%	72 B		ArchOneToOne	May 24, 2022, 10:03:19 AM
250	Retrieval	Terminated on error 50%			ArchOneToOne	May 24, 2022, 9:25:19 AM
249	Retrieval	Terminated on error 50%			ArchOneToOne	May 24, 2022, 9:17:32 AM
248	Archiving	Completed			ArchOneToOne	May 23, 2022, 3:51:50 PM
247	Archiving	Denied			ArchOneToOne	May 23, 2022, 10:58:27 AM

Figure 14: Easy move jobs history

3. Select one of the row. A menu appears.
4. Click on **Relaunch**. This window opens (Figure 15):

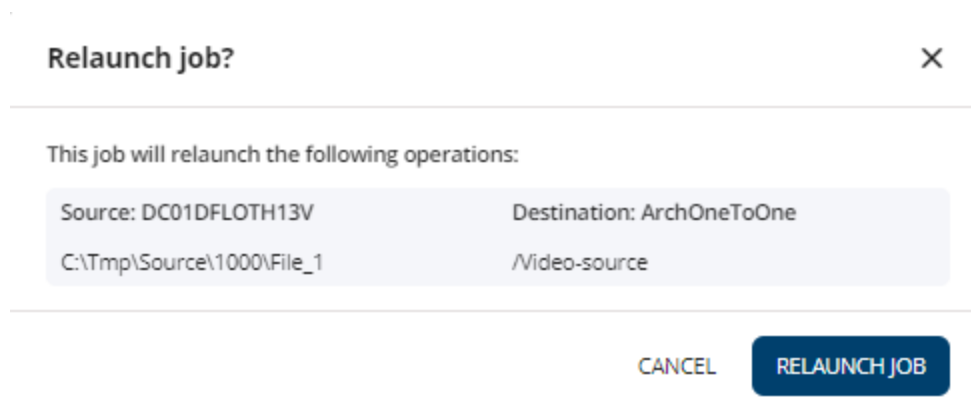


Figure 15: Relaunch a job

5. Click **Relaunch job**. The job is relaunched.

CHAPTER 8 - Organize Repositories

A repository is a centralized storage location to preserve and manage data for long-term retention. This chapter explains how to structure data within repositories.

Repository Types

There are two types of repositories:


- **Archive.** The process of archiving involves moving data from one location to another location for long-term retention. Data archives are classified in folders and sub-folders that you can organize at your convenience.
- **Backup.** A backup consists of copying data to a repository with the intent to keep the original data in its current location. Backups are useful if the original data are lost or corrupted and you want to restore it to a certain point in time.

Repository Organization

When you log in to the Web Interface, it displays the projects and repositories that are shared with you and other users.


- **Projects** Miria provides an organization tool to group repositories into projects. They can be accessed by multiple users.
- **Repositories** A repository contains folders and sub-folders, in which directories and files are archived. The administrator may define one or multiple repositories that belong to a user and can only be accessed and managed by its owner.

Folders and Sub-Folders

Folders and sub-folders are used to organize archived data in a file tree structure. When you explore a repository, they are represented by a folder icon: .

You can both manually create and organize folders to classify your archived data. Folders can also be generated by automatic archiving tasks set up by the Administrator, or by external tools.


Archived Directories and Files

Archived directories and files are located in repository folders. When you explore a repository, the archived files are represented by an icon indicating their application. You recognize directories by the directory icon: .

Manage Repositories

When exploring the repositories, various object options are accessible.

When holding the mouse pointer over an object, you can perform multiple operations using the

More actions  button (Figure 16):

- Archive data directly in the **Easy Move** interface.
- View and retrieve the instance of a file.
- View and manage metadata on an object.
- Perform a search by criteria on an object.
- Retrieve data at a specific date by using the time navigation.

Alternatively, you can select and drag folders and directories to change their location in the repository.

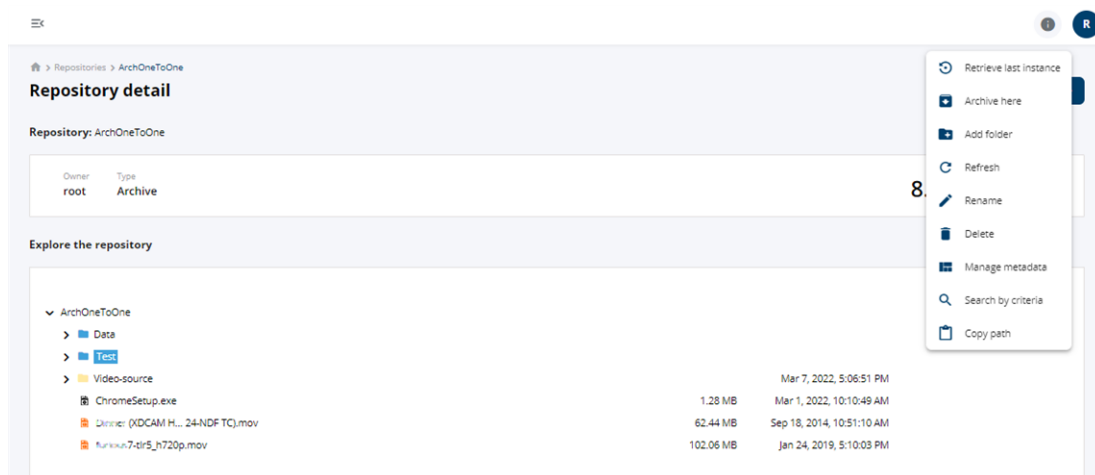




Figure 16: Repository operations

The number of options depends on the selected object (file, directory, or folder) and the permissions you have on that object.

Add Folder


1. In the Web Interface, click the **Repositories** tab.
2. Click on a repository.
3. Explore the repository to highlight the object and click the **Add folder**  button.
4. Type a folder name.
5. Confirm with **Enter**.

Rename Object

1. In the Web Interface, click the **Repositories** tab.
2. Select a repository.
3. Explore the repository to highlight the object and click the **Rename**  button.
4. Type a new name for the object.
5. Confirm with **Enter**.

Delete Object

1. In the Web Interface, click the **Repositories** tab.

2. Select a repository.
3. Explore the repository to highlight the object and click the **Delete**  button.
4. Confirm to delete the object.

Permissions on the Repositories

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

To access to the permissions, click the **Repositories** tab, in the repositories list, 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 repository

1. Click the button **+ NEW PERMISSION**. A pop-up 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
- Archive
- Retrieve
- Add a folder
- Rename a folder
- Delete a folder
- Move a folder
- Rename an object
- Delete an object
- Move an object
- Modify file extension
- Manage metadata
- Move a folder to another repository
- Administration
- Validate retention jobs

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.

Manage Metadata

Metadata are information about data that is applied to objects during the archiving process or that has been added manually. You can directly view and manage associated metadata from the contextual menu of your repository.

To view and manage metadata

1. In the Web Interface, click the **Repositories** tab.
2. Select a repository.
3. Explore the repository to highlight an object and select **⋮** > **Manage metadata**. The associated metadata are displayed ([Figure 17](#)).

Manage metadata

Metadata on archive@ArchVideo:/Dinner (XDCAM HD422, 1080p24, 8x1 Audio, 24-NDF TC).mov ⓘ

> Metadata

Add

test
Value
Yes

date
Date
12/8/2020

string
Value
toto

Validate

Figure 17: In this example, 3 metadata types are associated to the object

4. If needed, modify or remove the associated metadata.
5. If needed, select other metadata ([Figure 18](#)):
 - a. Expand the tree and select a metadata.
 - b. Click **Add**. Repeat this for each metadata you want to include.

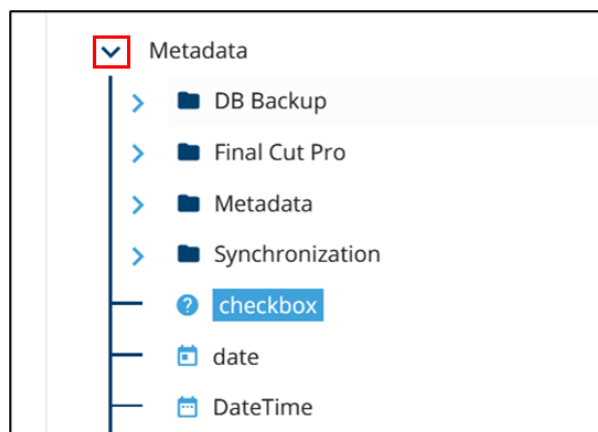


Figure 18: Metadata types

6. Click **Validate** to save the modifications.

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

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.

Manage Instances

Objects can be archived several times under the same name and the same location. These versions are called instances. You can view details about each instance archived in the Miria Web Interface.

To obtain information on archived objects and storage details

1. In the Web Interface, click the **Repositories** tab.
2. Select a repository.
3. Explore the repositories to highlight an object and select **:** > **Instance**. The following information is displayed:
 - **Archiving date/Name** Specifies the instance archiving date and time and the storage manager associated with the instance.
 - **Type** Identifies the archived object.
 - **Date of deletion** Indicates the deletion date from the file system.
 - The **Instance Details** are displayed on the right.
4. Expand the archiving instance to see the storage that hosts the archived files and directories. You can click the storage to access the **Session Details** (Figure 19).














Instances: archive@ArchOneToOne_FL:/Binary.zip					
ARCHIVING DATE / NAME	TYPE	DATE OF DELETION		Session details	
▼ May 2, 2022, 10:24:30 AM	File		 	Storage manager type	File Storage One To One
Sm_OneToOne				Storage manager	Sm_OneToOne
▶ Apr 15, 2022, 11:10:07 AM	File		 	Storage manager container	Smc_OneToOne
▶ Apr 15, 2022, 10:52:17 AM	File		 	Compression format	None
▶ Apr 15, 2022, 10:14:58 AM	File		 	Relative file path	/Project/5/Binary (5).zip
▶ Apr 15, 2022, 8:41:38 AM	File		 	Retention information	
▶ Apr 15, 2022, 8:39:21 AM	File		 	Retention	Ret01
				Retention date	Jan 1, 1970, 1:00:00 AM
				Deduplication information	
				Deduplication domain	Deduplication is not enabled for this session
				Digest type	
				Digest	
				Reference count	1

Figure 19: The storage manager is listed below the instance



The **Instances** interface lets you:

- Perform a retrieve in the **Easy Move** interface by clicking the **Retrieve**  button.
- Preview an archived video asset file and perform a partial retrieve.
- Manage and view metadata.
- Return to the repositories by clicking the arrow in the top right corner.

Retrieve Instance

The easiest way to retrieve an archived file is to retrieve its latest instance. However, you can also retrieve any file instance by selecting it from a list of instances.

To retrieve an instance

1. In the Web Interface, click the **Repositories** tab.
2. Select a repository.
3. Explore the repository, choose the object you want to retrieve and:
 - Select **> Retrieve last instance**. The **Easy Move** interface is displayed and indicates the path to retrieve the last instance. Continue with step 7 of this procedure.
- Or
- Select **> Instance**. The **Instances** interface is displayed. You can expand an instance to see more details.
4. Select the archiving instance to retrieve. The corresponding instance details are displayed to the right of the instance.
5. If needed, click the **Manage metadata**  button to view or modify metadata.
6. Click the **Retrieve**  button.
7. Select whether you want to retrieve at new, original, or default location on the window that just opened (Figure 20).

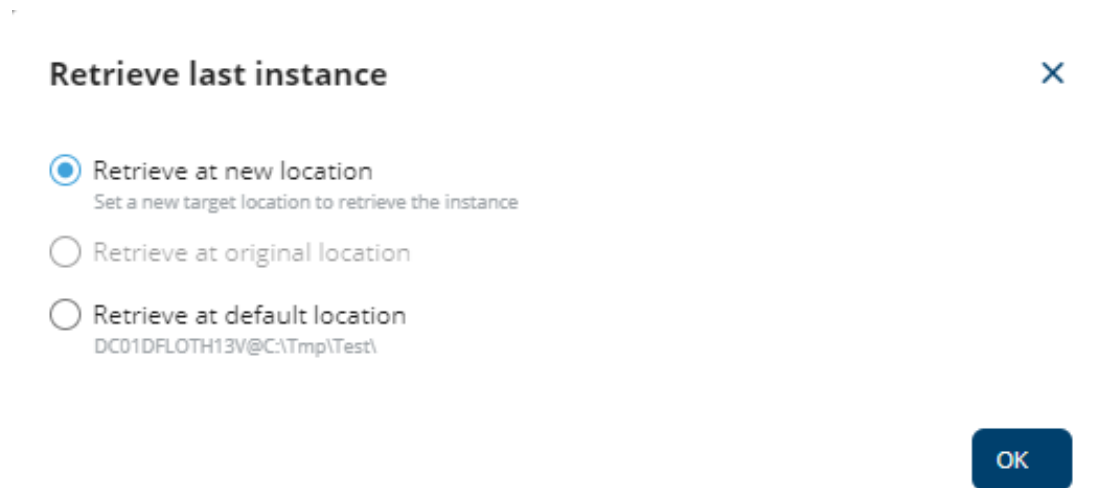


Figure 20: Retrieve last instance

8. Select **Retrieve at date** to get to choose a new location.
The **Easy Move** interface is displayed and indicates the path to retrieve the instance (Figure 21).

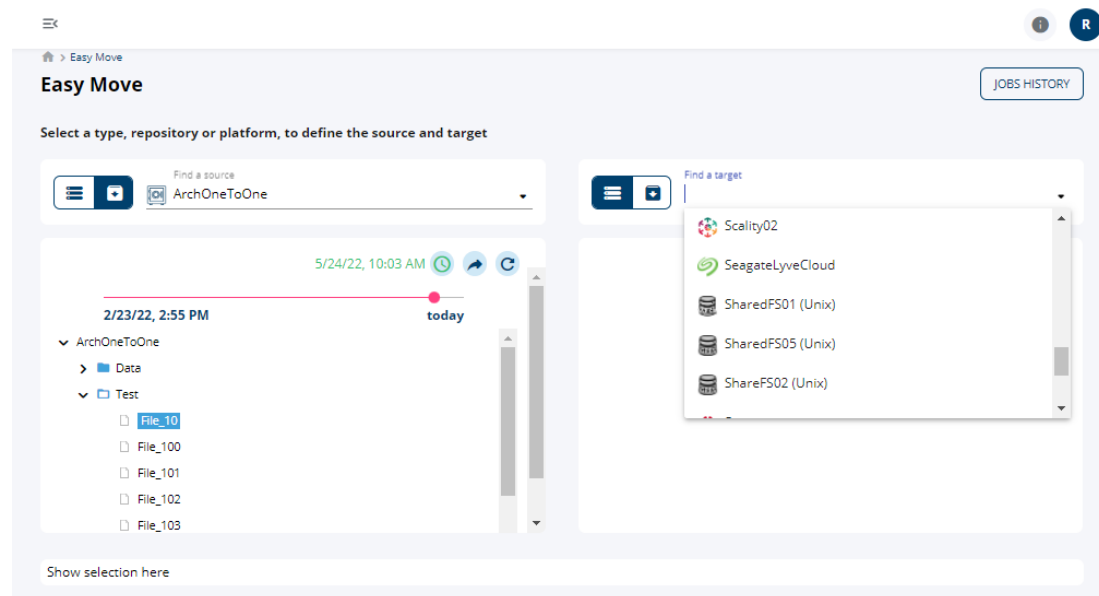


Figure 21: The selected path is directly indicated in the source repository

9. In the right field, select the target type as **Platform** to choose your target.
10. Move the object:
 - Click **Add**.
 Or
 - Drag the object from the source to the desired location in the target.
11. Validate the basket. The retrieval job is launched.
12. Click the **Jobs** tab to verify the job progress.

Instance Details

Check the following overview ([Table 3](#)) for information about the instance details.

Table 3: Instance details properties

Property	Description
Archiving date	Date and time the file or directory was sent to the archive
MIME type	<p>Specifies the MIME type of the archived file which is a two-part identifier of file formats, for example: audio/mpeg, video/quicktime, or text/plain.</p> <p>It is a more reliable indicator of file format than the file extension. This property displays only if the administrator has configured Miria to recover it.</p>
File size	Size of the file or directory.
Creation date	Date the file or directory was created, independent of the archive.
Last update	Last time the file or directory was modified, independent of the archive.
Last access	Last time the file or directory was consulted without modification, independent of the archive.
Owner user	User who owns the file or directory.
Owner group	Group of the user who owns the file or directory.
Original location	Original location of the file on the user's machine. If the file was archived from a network drive, this displays the path from the network drive (e.g., X:\Data\MyData).
Global path	Global path of the file original location.
File path on source	File original location on the primary storage.
Digest type during archiving	Type of digest that is calculated on the file at the moment of archiving on the storage when performing multiple writing. It verifies whether the file content is the same on all storage (i.e., [None], MD5, SHA-1, SHA-256, SHA-384, or SHA-512).
Digest during archiving	Value of the above digest, if this was used.
Link target	Path of the target file/directory to which the link points on the source disk. Displays only if the archived object is a symbolic link.

Table 3: Instance details properties

Property	Description
Alternate stream	Indicates whether the alternate streams (i.e., file attributes, rights, etc.) are archived in this instance. Possible values are Yes or No .

Session Details

Check the following overview ([Table 4](#)) for information about the session details.

Table 4: Session details properties

Property	Description
Storage manager type	Type of storage manager used (e.g., Miria File Storage One To One etc.).
Storage manager	Name of the storage manager as configured in Miria.
Storage manager container	Name of the storage manager container as configured in Miria.
Compression format	See the Miria Administrator's Documentation for details on compression.
Relative file path	Defines the location that is relative to the current directory or folder.
Retention	Name of the retention period associated with the repository where the file is stored.
Retention date	Date and time of the end of retention period.
Deduplication domain	Name of the deduplication domain as configured in Miria.
Digest type	Type of the deduplication digest that is calculated at archiving time to verify that the new file to be archived is unique (SHA-1, SHA-256, SHA-384, SHA-512, or Filename/Size).
Digest	Value of the deduplication digest, if this was used.
Reference count	Number of times a file with the same digest has been archived.

CHAPTER 9 - 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 22).

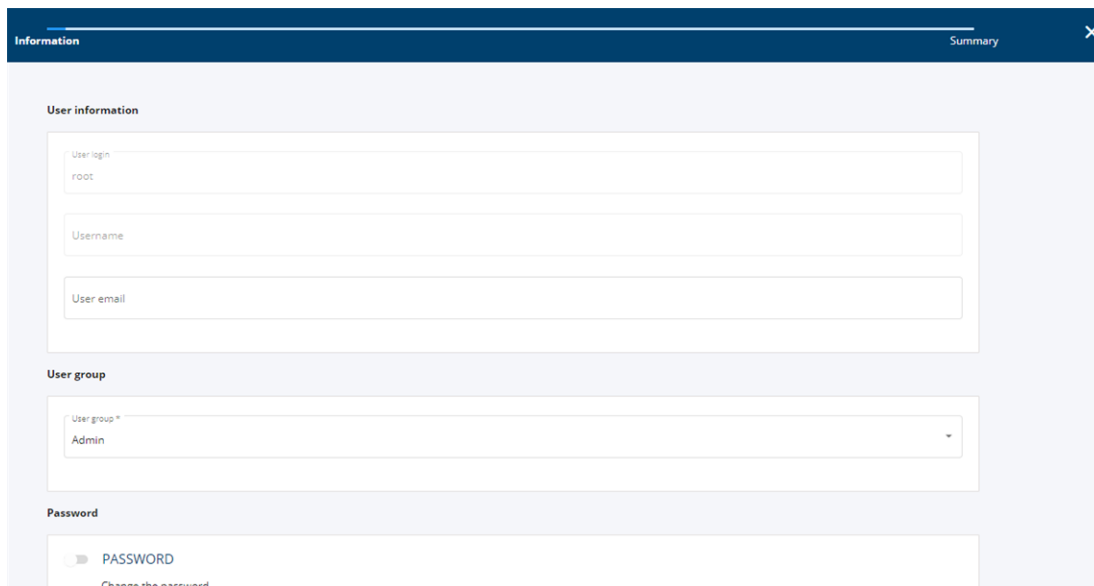
Figure 22: The user creation wizard

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 23](#)).



The screenshot shows a 'User configuration wizard' window with a dark blue header bar containing 'Information' and 'Summary' tabs, and a close button (X). 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 that says 'Change the password'.

Figure 23: 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 24](#)):

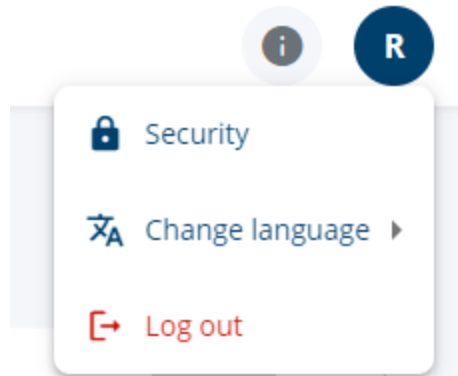


Figure 24: User profile menu

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 25):

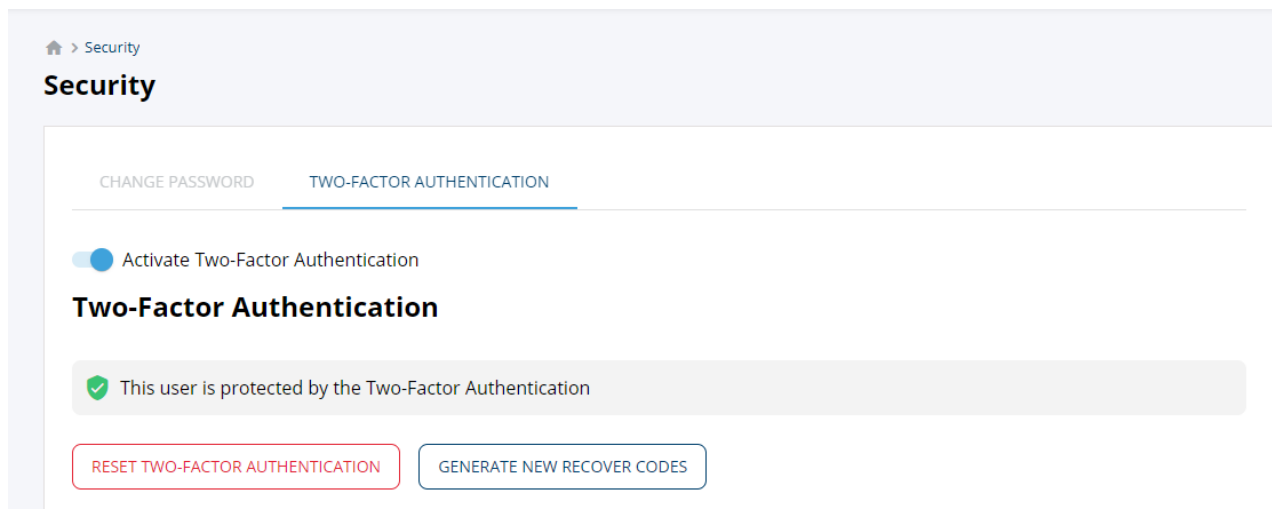


Figure 25: Mandatory Two-Factor Authentication

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 26](#)):

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 26: 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 27). 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.

[illegible]

Figure 27: 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 28):

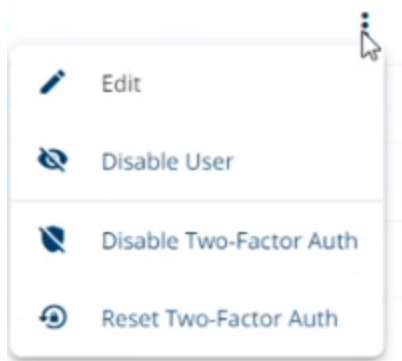


Figure 28: Rows menu

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

CHAPTER 10 - 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 5](#)) describes the template that you can use to create internal management tasks:

Table 5: Internal management task template

Task	Description
Automatic deletion	<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 Automatic Deletion Task for details.</p>
Automatic retention	<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 Automatic Retention Tasks for details.</p>

Table 5: Internal management task template

Task	Description
Maintenance	<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 Maintenance tasks for details.</p>
Retention	<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 Creating a Task for details.</p>
Storage proxy maintenance	<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>
Volume management on storage manager	<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 Recycling Triggered by Volume on Storage and Volume Management on Storage Managers Task for details.</p>
Miria Database backup for PostgreSQL	<p>Backs up the Miria database.</p> <p>See Database Backup Task for details.</p>
Archive Report	<p>Generates a report on the archive volume.</p> <p>See Archive Report Task 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 6](#)), 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 6: Data movement automatic tasks template

Task	Description
Automatic Archiving	Launches archiving jobs based on a schedule.
Automatic catalog ingest	Launches Catalog Ingest jobs to import external LTFS media into the Miria database.
XML Ingest	<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"> • Archiving of specific files rather than whole directories. • Attributing metadata to files and folders. • Archiving into different archives and folders with a single run of the task. <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 6: Data movement automatic tasks template

Task	Description
Interplay Dispatcher	<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 29](#)).

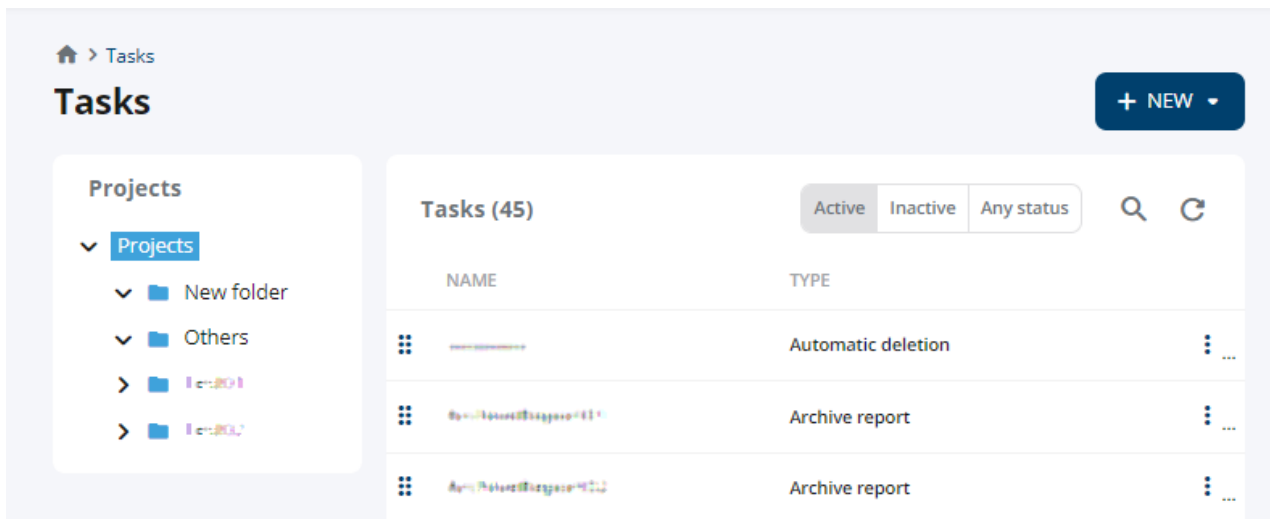


Figure 29: Tasks view

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 30](#)).

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 30: 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 topic 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 7: Tasks list menu

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

Table 7: Tasks list menu

Parameter	Description
Email	<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"> • Add + 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"> • None they won't receive any email. • Email they will receive an email every time the task runs. • On error only they will receive an email only if the task ends with errors. • • above the users list, there is a toggle Email only if an action was performed. 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. <p>See Task-specific Parameters 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>
Settings	<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 Default Settings and Settings Templates.</p> <p>Note: For tasks that do not require configuration, such as manual tasks, this tab is grayed out.</p>

Table 7: Tasks list menu

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

When Creating or Editing a Task

Table 8: General parameters common to all tasks

Parameter	Description
Task type	When creating a new task, you have first to select a task type. See Creating a Task
Task name	Name that identifies the task within Miria. <div> Important: 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"> - ARCHIVING - RETRIEVAL - COPY - MOVE - DELETE - SYNCHRO - RETENTION </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 9: General parameters common to all tasks

Parameter	Description
Commands	<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"> 1. Pre-processing: 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. 2. Post-processing: 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"> • {Job_Number}: Job ID associated to the task. • {Db_Name}: name of the environment on which you are working. • {Tpl_Status}: retcode of the job, if the retcode is different than 1, there is an error. They will be replaced automatically upon execution. It must always contain the full path of script to run and its interpreter. Example: D:\miria\Binary\Bin\ada_perl.exe D:\miria\Custom\custom_action.pl -job_id{Job_Number} -db_name {Db_Name} -retcode {Tpl_Status} <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
Run options.	

Table 9: General parameters common to all tasks

Parameter	Description
Run timeframe	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 Run Timeframes for details .
Run lock	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 Run Locks for details.
Next task	Select the next task among the drop-down list.
Maximum number of simultaneous runs	<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>
Wait when the maximum number of runs is reached	<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
Date	Time and hour at which the report was generated.
Name	Name of the report in the <code>Archive_date-time.ext</code> format.
Size	Size of the generated report that is in PDF format.
Download button	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.
Delete button	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
Source.	
Ingest Type	Select Media/LTFS from the list.
Storage Manager Container	<p>Only for Media Manager storage manager container.</p> <p>Select from the list, an ingest Storage Manager Container into which you want to ingest the media.</p>

Parameter	Description
Retention	<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>
Filters.	
Library	<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>
Media Type	<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., LT0-6 and LT0-7), 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
Define filters on barcodes	<p>Optional.</p> <p>Select Include from the list to ingest media with a specific barcode range.</p> <p>Select Exclude 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"> The * means any alphanumeric character any number of times. The ? means any alphanumeric character once. The separates several possible pattern options. <p>The expression must contain at least one * or ?.</p> <p>For example:</p> <ul style="list-style-type: none"> 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. *L4 includes/excludes any media with a barcode ending in L4. You might use this, for example, to select only media of LTO4 type. 162* WV* includes/excludes any media with either a barcode beginning with the string 162, or a barcode beginning with WV.

Target.

Existing repository	<p>Imports the media into a repository which already exists in Miria.</p> <p>Select Existing repository 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
New repository	Imports the media into a new repository. Project: 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.
Reference repository	Optional. 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
Source.	
Storage platform	Select the storage platform in which you want to delete data.
Location of data to delete	Enter the path of the data that Miria can delete.
Target.	
Repository name	Select the target repository
Full path auto-generated	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
Source.	
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.
Target.	
Repository name	Select the target repository

Parameter	Description
Full path auto-generated	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.
Archive repository	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
Retention	<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"> • Apply on Stub. When the stub is no longer present on the file system. • Apply on Object. When the object is no longer present on the file system.

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
Nb. Expected Objects	Total number of media present on the storage manager container.
Nb Objects	Number of media selected for repack.
Volume Expected	Total storage volume.
Volume	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
Maintenance.	

Parameter	Description
Check running jobs	Click this toggle to process the jobs that have been running for more than 24 hours: <ul style="list-style-type: none"> Jobs on creation or running switch to the Terminated on error status. Jobs on queue restart or switch to the Terminated on error status, if they do not start.
Delete sub-job metadata	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.
Delete in recycler	To delete permanently the repositories folders that you removed from a repository.
Check expired instances	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.
Check expired SML instances	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.
Delete temporary tables	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.
Delete archiving job details	To delete details, messages, or alarms that are past their retention period.
Delete copy / synchronization job details	To delete details, messages, or alarms that are past their retention period.
Delete repository tiering job details	To delete details, messages, or alarms that are past their retention period.
Delete statistics on jobs	To delete details, messages, or alarms that are past their retention period.

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

Parameter	Description
Delete events	<p>To delete events that are past their retention period:</p> <ol style="list-style-type: none"> 1. Click the toggles for the types of events (see the list below), that you want to delete. 2. Click the event retention toggle. 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. <p>Type of events that you can delete:</p> <ul style="list-style-type: none"> • AUDIT TRAIL • CRITICAL • DEBUG • DEBUG STACK • ERROR • FATAL • INFO • STACK • STOP/DIE • SUCCESS • WARNING


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
Source.	
Repository name	Select from the drop down list a name for the repository.
Repository path	Click the  button to select the absolute path of the selected repository for which the volume report is generated.
Layout. Enables you to modify the PDF file layout.	
Format	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"> • Leave the field empty. The PDF file does not display any image. • Enter the <code>{default}</code> keyword. The PDF file displays the default image included in the Miria distribution. <p>Or</p> <ul style="list-style-type: none"> • 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.
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"> • <code>{Job_Number}</code> • <code>{SubJob_Number}</code> • <code>{Archive_Name}</code> • <code>{Archive_Path}</code> • <code>{Archive_Global_Path}</code> • <code>{Archive_Comment}</code> <p>The PDF file displays the associated value for each keyword that you have defined.</p>
Report information. Enables you to modify the PDF file contents.	
Media details	<p>Details on the media. These are the valid values:</p> <ul style="list-style-type: none"> • None. Default value. The report does not display any media information. • Media By Job. The report displays the names of media, associated with the jobs that have put the objects in repositories. • Folders By Media. 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.

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

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
Configuration.	
Storage platform	<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>This must always be a path, never a file name.</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"> • 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. • 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>. • 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>. <p>The second set contains the original, untranslated XML files, named <code>originalFilename_jobNumber.xml</code> (without the <code>_ADA</code> suffix).</p> <p>Result Directory. 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
XML error report	<p>In some cases the XML ingest task does not complete correctly. This happens when:</p> <ul style="list-style-type: none"> • The XML ingest file is malformed. • The XML ingest file does not conform to the XSD file. • If you used the Translator, it could be incorrect in itself, or not translate correctly to a form that ada_ingest.xsd can read. • The files specified for repository do not exist. • Repositories requested in the XML files do not exist. • The metadata to be associated with the files put in repositories do not exist. • 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. <p>In these cases, the Event logs display error messages to help you analyze the error cause.</p> <p>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>Perform this modification in either of these two ways:</p> <ul style="list-style-type: none"> • 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. • If the Error Report check box is selected, the XML files are moved from

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>Reject Directory. 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.
StartComboAtIndex	<p>By default, the ComboBox in Miria goes from 1 to N, while in many client software combos start from 0 to N. The StartComboAtIndex parameter allows to automatically increment the index of a combo box.</p> <p>Example: 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 StartComboAtIndex 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
metadata_folder_action	<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 11 - Monitoring


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  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 31](#)).

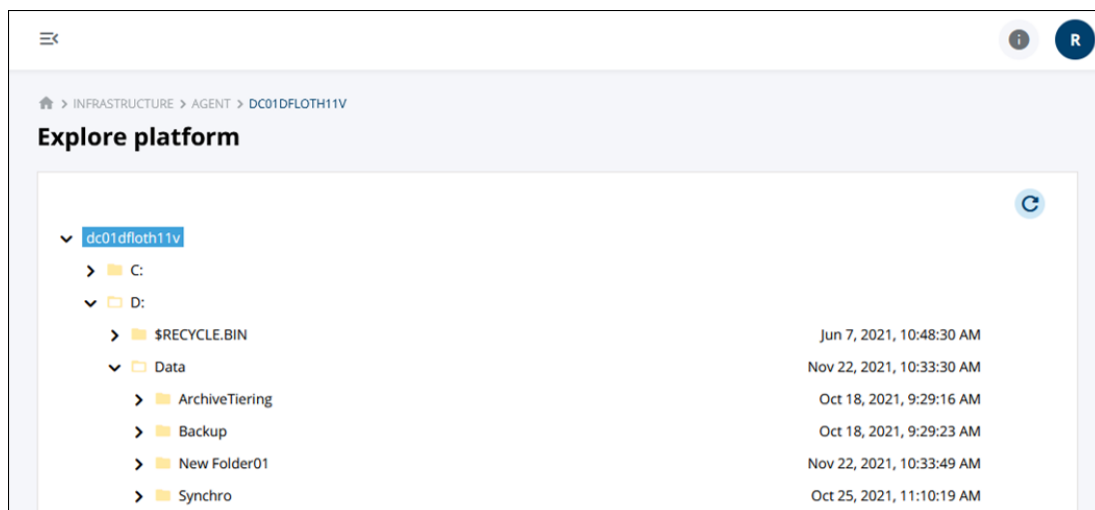



Figure 31: The arrow keys enable to navigate


Test the API Connection of a Platform

1. Click the **Infrastructure** tab.
2. Select a storage (e.g., Agent, NAS etc.).
3. From the list of platforms, click the **Connection** button.

View Project or Task Logs

1. Click the **Backup** 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**.
2. (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.

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 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 10](#)):

Table 10: Triggering methods

	On demand recycling	Scheduled monitoring
High Water Mark	<p>Required 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
Task High Water Mark	Ensure this option is not selected, unless you also want to activate scheduled monitoring.	Required 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.
Low Water Mark	<p>Required 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>Required 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.**