Getting started with Backup & Recovery in mCloud

Micron21 Support - 2026-08-31 - mCloud Backup (mBackup)

Getting started with Backup & Recovery in mCloud

Overview

mCloud includes an integrated **Backup & Recovery** service, powered by Storware, that lets you protect your virtual machines with scheduled full and incremental backups. The service is built into your mCloud dashboard, so there is no separate console to log into.

This article covers three things:

1. Finding your way around the Backup & Recovery dashboard
2. Creating a backup policy (which VMs to protect and how long to keep their backups)
3. Creating a backup schedule (when those backups run)

Restoring from a backup is covered in a separate article.

> **How backups work in mCloud:** A **policy** defines *what* is protected and *how long* backups are kept. A **schedule** defines *when* backups run and links back to a policy. You will normally create one policy, then attach a full schedule and an incremental schedule to it.

Prerequisites

- **Before backups can run, the Backup & Recovery service must be activated for your project by our Support Team. The dashboard is visible by default, but backup jobs will fail until access has been granted. To request activation, send an email to sales@micron21.com**
- Access to the mCloud dashboard at https://mcloud.micron21.com
- One or more virtual machines running in your project that you want to back up

---

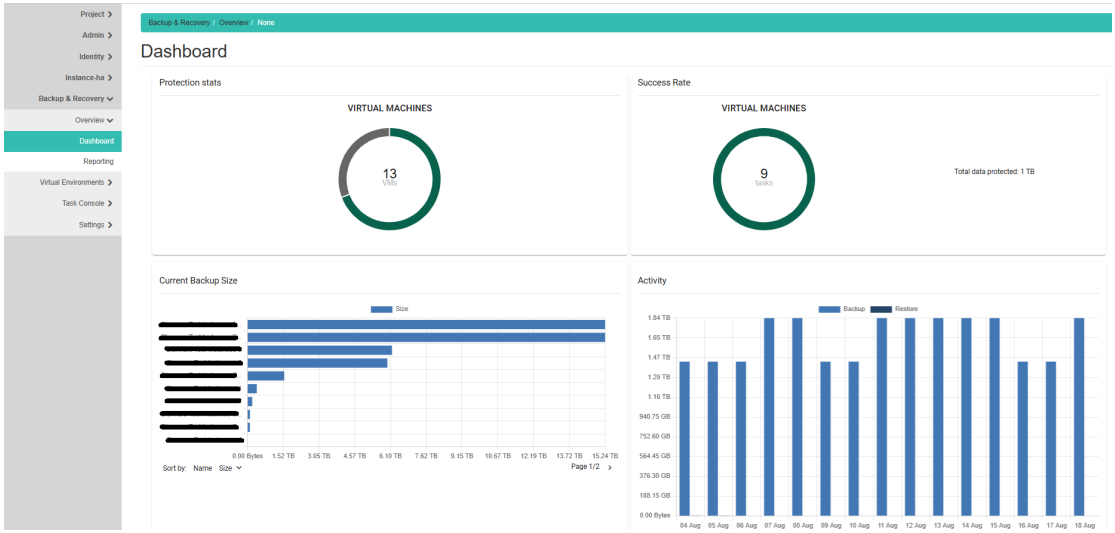
1. The Backup & Recovery dashboard

The Backup & Recovery tools appear as a plugin inside your mCloud (OpenStack Horizon) dashboard.

1. Log into mCloud at https://mcloud.micron21.com and select your project.
2. On the left menu, expand **Backup & Recovery**. You will see the following sections:

- **Overview** – dashboards and reporting
- **Virtual Environments** – your instances, backup policies (Backup SLAs), and mounted backups
- **Task Console** – live and historical backup/restore tasks
- **Settings**

3. Go to **Overview > Dashboard** to see the status of your protected environment.



The Dashboard is made up of four panels:

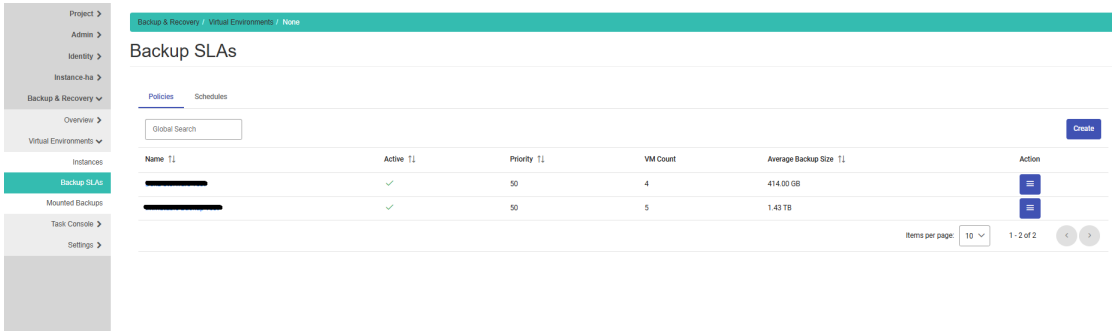
- **Protection stats** – the number of virtual machines currently covered by a backup policy.
- **Success Rate** – the proportion of backup tasks that completed successfully, along with the total amount of data protected.
- **Current Backup Size** – how much backup data you currently hold.
- **Activity** – a chart of backup and restore data over recent days.

  A newly configured project will show low or zero values here until your first backup has run.

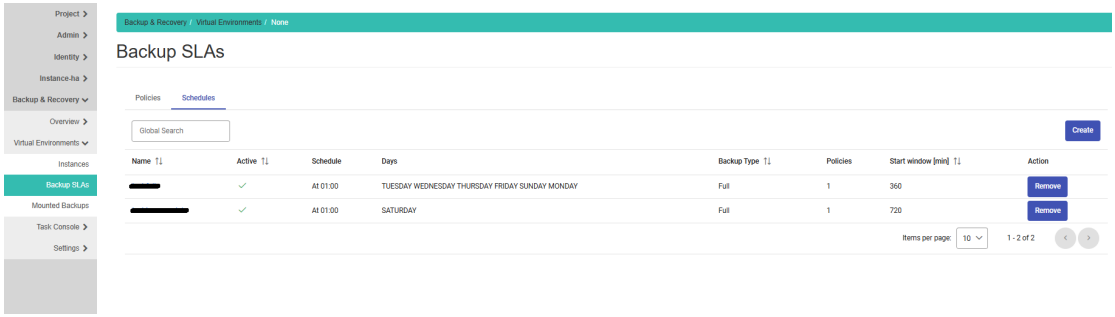
Other useful areas

- **Virtual Environments > Instances** – lists the VMs in your project and their protection status.
- **Virtual Environments > Backup SLAs** – where you create and manage **Policies** and **Schedules** (covered below).

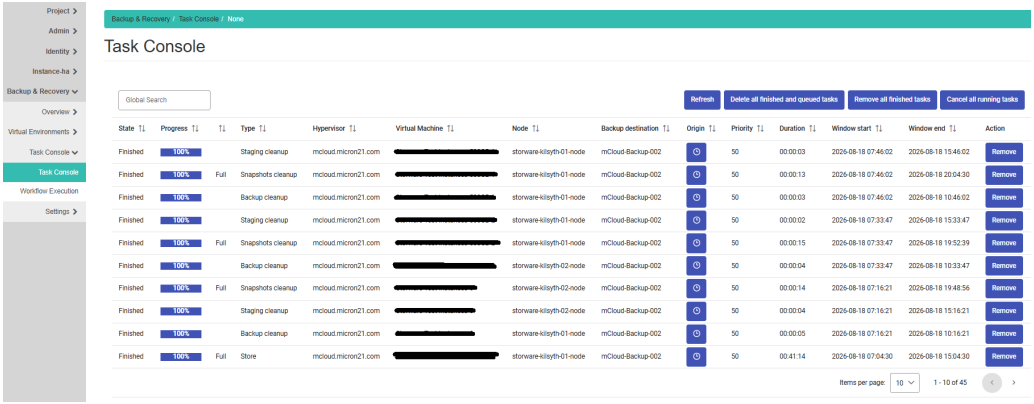
Policies



Schedules



- **Task Console** – shows every backup and restore task, with its state, progress, node, destination and duration. Use this to confirm that a job you started is running or has completed.



---

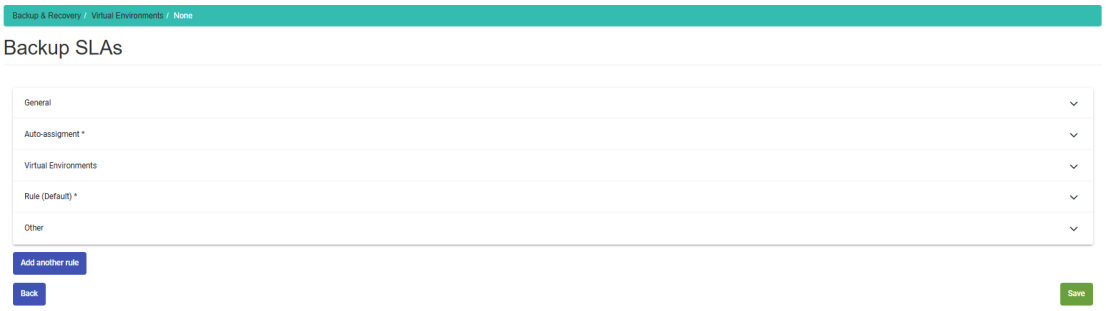
2. Create a backup policy

A backup policy defines which VMs to protect and how long to keep their backups.

1. Go to **Backup & Recovery > Virtual Environments > Backup SLAs**.

2. Make sure the **Policies** tab is selected, then click **Create**.

3. The policy form is divided into collapsible sections. Expand each one and complete it as below.



General

Field	Recommended setting
Name	A name of your choice that identifies the policy (for example, the VM or workload it protects).
Scheduled backups enabled	**Yes**
Auto remove non-present Virtual Environments	**Yes** – automatically cleans up policy entries for VMs that no longer exist.
Send daily backup/restore report for VMs assigned to this policy	Set to **Yes** if you want a daily email report; otherwise leave as **No**.
Retry Count	The number of times a failed backup is retried before it is reported as failed. A value of **1–2** is a sensible starting point.
Priority	Leave at the default unless you have a specific reason to change it.

Virtual Environments

Under **Choose Virtual Environments**, select the VM or VMs you want this policy to protect.

Rule (Default)

This section controls the backup destination and how long backups are retained.

1. **Active** – leave set to **Yes**.

2. **Name** – leave as **Default**.

3. **Select Backup Destination** – choose the backup destination provided for your project (for example, `mCloud-Backup-002`).

4. Set the retention values. The following are recommended starting points and can be adjusted to suit your requirements:

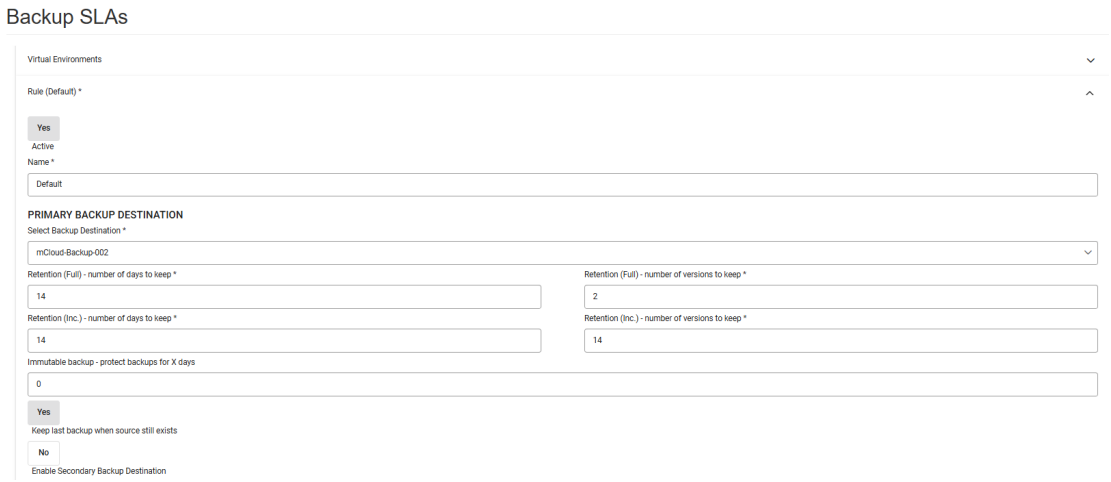
Field	Recommended value
Retention (Full) – number of days to keep	14
Retention (Full) – number of versions to keep	2
Retention (Inc.) – number of days to keep	14
Retention (Inc.) – number of versions to keep	14

5. **Keep last backup when source still exists** – set to **Yes**. This ensures you always retain at least one recovery point while the VM exists.

6. Leave **Immutable backup** and **Enable Secondary Backup Destination** at their defaults unless these have been arranged for your project.

7. When all sections are complete, click **Save**.

Example below for the Rule



> The retention values above are recommendations. Longer retention keeps more recovery points but uses more backup storage.

---

3. Create a backup schedule

A schedule defines *when* your backups run and links to the policy you created above. We recommend creating **two schedules per policy**: one **Full** backup that runs once a week, and one **Incremental** backup that runs on the remaining days.

Pick a time that suits your workload, ideally early morning or late at night when the VM is least busy. The examples below use a full backup one day a week and incrementals on the other days.

Recommended naming

Using a consistent name makes schedules easy to identify. We recommend:

- **Full:** `Full - <Day> - <time>` – for example, `Full - Sunday - 4am`
- **Incremental:** `Incremental - Daily - <time>` – for example, `Incremental - Daily - 4am`

Steps

1. Go to **Backup & Recovery > Virtual Environments > Backup SLAs** and select the **Schedules** tab.
2. Click **Create**.
3. Complete the form for your **Full** backup:

Field	Setting
Name	`Full - <Day> - <time>` (e.g. `Full - Sunday - 4am`)
Status	Active
Backup type	Full backup
Schedule execution type	Time

Start Window Length [min]	720 (recommended)
Choose time of day for backup	Your chosen time (e.g. `04:00`)
Choose days (required)	The single day of the week for the full backup (e.g. Sunday)
Choose Virtual Environment policies	Select the policy you created in step 2

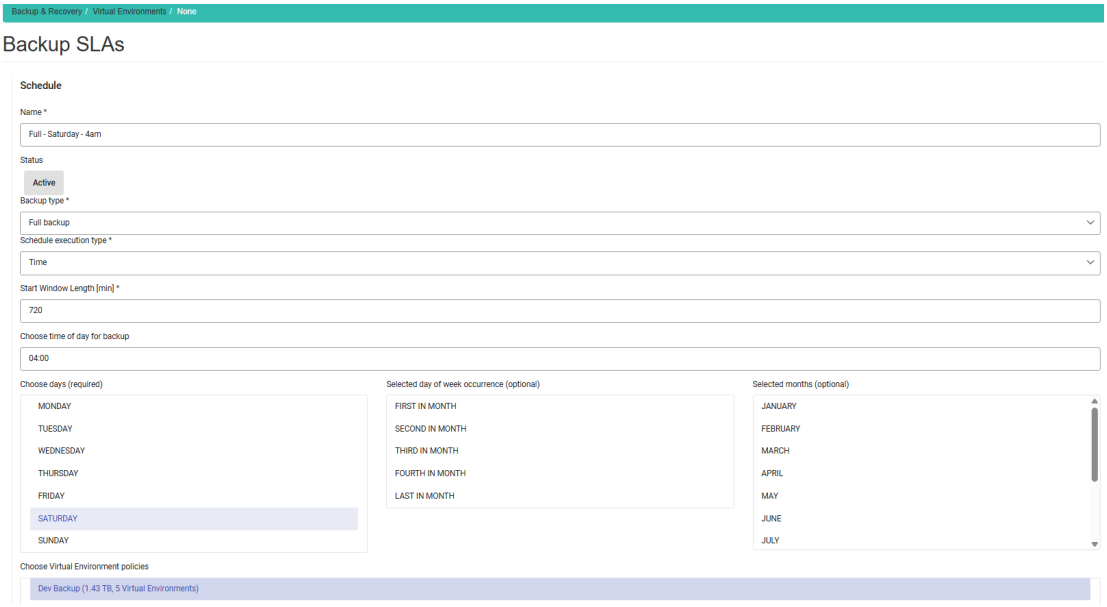
4. Click **Save**.

5. Click **Create** again and complete the form for your **Incremental** backup:

Field	Setting
Name	`Incremental - Daily - <time>` (e.g. `Incremental - Daily - 4am`)
Status	Active
Backup type	Incremental backup
Schedule execution type	Time
Start Window Length [min]	720 (recommended)
Choose time of day for backup	Your chosen time (e.g. `04:00`)
Choose days (required)	Every day *except* the full backup day (e.g. Monday–Saturday if the full runs on Sunday)
Choose Virtual Environment policies	Select the policy you created in step 2

6. Click **Save**.

Example below for a full backup schedule



> **Selected day of week occurrence** and **Selected months** are optional and can be left blank for a standard weekly/daily schedule.

Once both schedules are saved, your VMs will be backed up automatically. You can confirm jobs are running under **Backup & Recovery > Task Console**.

Next steps

- Check **Task Console** after your first scheduled run to confirm the backup completed successfully.
- To recover data from a backup, see the separate Restoring from a backup article.

Related Content

- Restoring a virtual machine from a backup in mCloud