Monitor Automatic Backups and Retention

Monitor Automatic Backups and Retention

Overview

This guide will help you confirm backups run on schedule, retained files are healthy, and pruning does not remove required recovery points.

Backup health and recovery readiness are evidenced rather than inferred from settings.

Who can do this

You need access to Backup settings/status and authorized filesystem.

Before you start

Know expected interval, location, retention count, last successful run, database size, storage alert threshold, and off-host copy policy.

> Before saving, check that the correct company is open and that you have permission to complete this task.

Where to find it

Automatic Backup settings, set up backup folder, notifications/logs, and instance status.

Monitor Automatic Backups and Retention

Step 1: Confirm automatic backup remains enabled

Step 2: Compare last backup timestamp to the expected schedule

Step 3: Check newest file name, size, and database identity

Step 4: Confirm file count follows retention without removing protected recovery points

Step 5: Review errors and disk space

Step 6: Periodically restore a selected file in isolation

Check your work

Scheduled files appear, retention matches policy, off-host copies exist, and restore tests succeed.

> Take a moment to check your work before closing the window. This small check can save time later.

If something goes wrong

- A set up path with no recent file is a failed control.
- Stop pruning/cleanup investigation before manually deleting backup evidence.

Related guides

- Configure Automatic Database Backups
- Restore a Database Backup Safely
- Diagnose an External Integration Failure

What to do next

Configure Automatic Database Backups.

Revision #0
Created 2026-09-04 09:20:16 UTC by Shah Rukh Saeed
Updated 2026-09-07 10:14:00 UTC by Shah Rukh Saeed