

Backup & recovery

A practical checklist for planning, protecting and testing recovery.

Set recovery objectives

RPO describes the point in time to which data must be recovered; it expresses the tolerable data-loss window.

RTO is the target time to restore the required service after disruption.

Agree both with the service owner and test whether the design can meet them.

Know what must be recoverable

Inventory data, application configuration, identity services, encryption keys, certificates, licences and dependencies. Document owners and restore order. Protect the recovery documentation so it remains available when production systems are down.

Choose and document retention

A full backup copies the selected data set. An incremental usually contains changes since a previous backup; a differential usually contains changes since the last full. Product behaviour varies. Keep every dependency required by retained restore points.

Capacity is more than source size

Allow for change rate, retained chains, archives, extra copies, metadata and free space. Compression and deduplication depend on the workload. Measure actual stored growth rather than assuming a reduction ratio.

Protect the recovery path

Keep a protected copy separate from the production environment, using offline or appropriately isolated/immutable storage where suitable. Restrict backup administration, protect recovery credentials and verify that encryption keys can be recovered independently. Encryption alone does not stop deletion.

Budget the complete window

Include scanning, snapshots, data transfer, verification and retries. Jobs can compete for network, source, repository and processing capacity. A network-only transfer estimate is a starting point, not a completion guarantee.

Test a real restoration

1. Select a representative restore point.
2. Restore in a safe, isolated environment.
3. Verify data and application function.
4. Check permissions and dependent services.
5. Record elapsed time, recovered point and issues.
6. Update the runbook and repeat on a planned schedule and after material changes.

Daily evidence to review

Failed or missing jobs, backup age, repository capacity, protected-copy status and unresolved restore-test findings. A green backup job does not by itself prove recoverability.

Simple Systems tools

Backup retention calculator, Backup window planner and Storage growth planner.
simplesys.dev/other-tools/