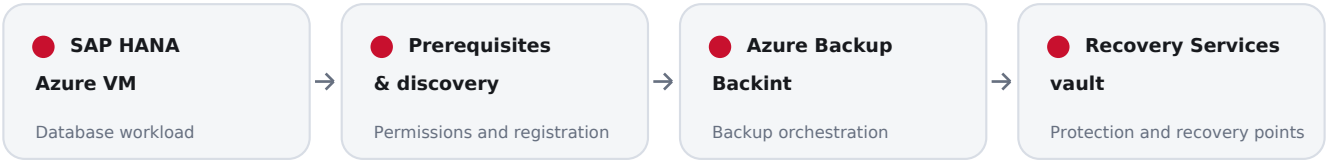
SAP HANA Backup to Microsoft Azure

A structured setup sequence for vault-based protection and operational backup assurance.

Backup architecture



Configuration sequence

1 PREPARE

Confirm HANA/Azure VM scope, network access, permissions and supported prerequisites.

2 PROTECT

Select the Recovery Services vault and establish the protection boundary.

3 CONFIGURE

Run registration and discovery; assign a policy for data and log protection.

4 VALIDATE

Run an on-demand backup, check job status and verify HANA backup/catalog evidence.

Technical coverage

AREA	CONFIGURATION / CHECK	EVIDENCE / VALIDATION
Protection scope	Confirm supported SAP HANA database and Azure VM topology; decide protection mode.	Vault registration and protected item status
Data and log policy	Define data backup schedule, log backup frequency, retention and on-demand needs.	Policy assignment, jobs and available recovery points
Backint operation	Review Azure Backup integration, HANA backup catalog and Backint communication.	Azure job details, backup.log, backint.log and catalog
Monitoring	Check failed or delayed jobs, log chain gaps, connectivity and capacity symptoms.	Vault job history, alerts, HANA traces and operational trend
Optional snapshots	Assess snapshot protection for faster operational recovery where supported.	Snapshot state and relationship to the Backint baseline

Operational note: Verify the current Azure Backup support matrix, region availability, network requirements and retention rules before implementing in a production landscape.