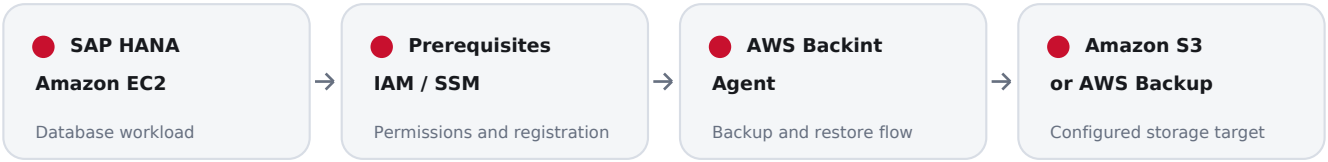
SAP HANA Backup on AWS

A structured setup sequence for AWS Backint Agent protection and backup assurance.

Backup architecture



Configuration sequence

1 PREPARE

Confirm supported HANA/EC2 scope, network path and recovery requirements.

2 AUTHORIZE

Set least-privilege IAM access, SSM readiness, instance role and KMS permissions if used.

3 CONFIGURE

Install and configure AWS Backint Agent; select S3 or AWS Backup as the target.

4 VALIDATE

Run a backup, check agent/HANA logs and verify backup catalog and storage evidence.

Technical coverage

AREA	CONFIGURATION / CHECK	EVIDENCE / VALIDATION
Access and scope	Confirm HANA/EC2 support, instance role, IAM permissions, SSM and target bucket or vault.	Registered database, agent status and access checks
Data and log policy	Define full/incremental/differential and log backup needs, schedules and retention.	HANA schedule, jobs and available recovery points
Backint operation	Review agent configuration, catalog handling, S3 paths or AWS Backup integration.	Agent logs, backup.log, backint.log and catalog
Monitoring	Check failed jobs, log chain gaps, permissions, network and KMS access symptoms.	Agent/HANA logs, S3 or AWS Backup job status
Optional EBS snapshots	Assess application-consistent EBS snapshots as a supplementary recovery layer.	Snapshot consistency, copy scope and restore procedure

Operational note: Coordinate HANA retention with S3 lifecycle rules, preserve the AWS Backint Agent folder structure, and verify current AWS support, IAM/KMS access and recovery requirements before production use.