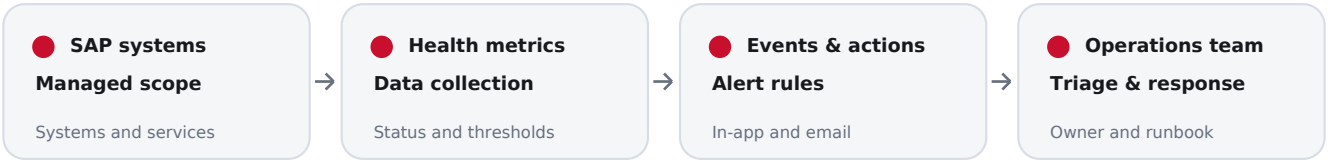
Cloud ALM Monitoring Setup

A clear path from system scope and metric collection to useful, actionable alerts.

Monitoring and alert path



Configuration sequence

1 SCOPE

Select managed systems and confirm Health Monitoring data and metrics are available.

2 CONFIGURE

Review metric thresholds, ratings and event conditions for agreed operational needs.

3 NOTIFY

Enable alert and email actions; select verified recipients and define escalation ownership.

4 VALIDATE

Trigger a controlled test and verify alert display, recipient delivery and response steps.

Technical coverage

AREA	CONFIGURATION / CHECK	EVIDENCE / VALIDATION
Managed scope	Confirm target systems, services, landscape tiers and required monitoring application.	Scope selection and managed component status
Metric collection	Check metric availability, last data time, health status and component setup.	Metric view, collection status and system scope
Thresholds & events	Agree warning/critical levels and event conditions; record why changes are needed.	Saved configuration and expected event rating
Alert actions	Enable alert creation and email actions; use verified recipients and agreed ownership.	Alert in Cloud ALM and delivery evidence
Operations	Define review cadence, triage, escalation and evidence retention for handover.	Runbook, named owners and test record

Operational note: Health metrics and event actions must be configured for the managed component. Email delivery can also depend on tenant email setup and verified recipients.