Cloud Approver AWS Read-Only Access Security Review

Updated June 28, 2026

Cloud Approver connects to AWS accounts through a customer-created IAM role. The role is intended for read-only cloud review: inventory, configuration evidence, approval status, recommendations, scan history, and reporting.

What the AWS setup creates

- An IAM role in the customer's AWS account. The default role name is CloudApprover-Audit-Role, but the name can be changed before setup.
- A trust relationship allowing the Cloud Approver scanner execution role to call sts:AssumeRole.
- A required sts:ExternalId condition. Cloud Approver generates this value per connected account to reduce confused-deputy risk.
- AWS managed SecurityAudit and ReadOnlyAccess policies attached to the customer audit role.
- An inline CloudApproverDataPerimeterDeny policy that blocks high-risk payload-reading APIs while leaving inventory and billing metadata available.
- Role tags including ManagedBy=CloudApprover and CloudApproverAccount so the role can be identified during verification.

What this access is used for

- Listing cloud resources and configuration metadata.
- Reviewing security posture signals such as public exposure, encryption settings, stale access indicators, and audit logging state.
- Estimating cost or waste opportunities from observable resource configuration and aggregate metrics.
- Checking approval tags and whether approved resources have changed from the configuration that was approved.
- Recording scanner API call metadata so customers can see which read-only provider calls supported a scan.

What Cloud Approver does not request by default

- No administrator, power-user, or remediation role.
- No default permission to change infrastructure, delete resources, rotate secrets, modify billing, or write application data.
- No agents installed in customer accounts or workloads.
- No need for customer AWS access keys to be entered into Cloud Approver.
- No default reading of S3 object bodies, table or database rows, queue messages, log events, query results, code artifacts, model outputs, secret values, private keys, or parameter values.

Read-only permissions Cloud Approver explicitly denies

- S3 object and object-lambda reads, S3 Tables table data, and S3 Vectors vector data/query reads.
- DynamoDB item reads, queries, scans, and PartiQL selects; Keyspaces, SimpleDB, QLDB, Aurora/RDS Data API, and Redshift Data API data reads.
- Secrets Manager secret values, SSM Parameter Store values, AppConfig configuration

payloads, KMS decrypt, and KMS data-key generation.
- SQS message receives, CloudWatch Logs event/query reads, Athena query results, Step Functions execution history, and X-Ray trace retrieval.
- EC2 user data, console output, password data, Auto Scaling launch configurations, ECS task definitions, API Gateway broad GET access, CloudFormation template bodies, EKS Kubernetes API access, and RDS log downloads.
- CodeArtifact package assets, CodeCommit file/blob/Git pulls, ECR image/layer downloads, Lambda function/layer downloads, CloudShell file downloads, Elastic Beanstalk retrieved environment info, and TNB package content.
- Kinesis records, Kinesis Video media/session reads, Bedrock retrieval/model invocation APIs, OpenSearch HTTP document reads, WorkDocs document/folder reads, and AWS Support attachments.

Data handling

- Cloud Approver stores account metadata, role connection status, inventory records, recommendations, approval records, reports, and assistance request content.
- Temporary AWS STS credentials are used for scanner jobs and are not stored as permanent customer credentials.
- Scanner evidence is designed around metadata and configuration, not customer payload data.
- Demo mode masks customer names, identifiers, inventory values, request details, account IDs, resource IDs, and ARNs where they can appear.
- Support or assistance requests should not include passwords, private keys, regulated health information, or other highly sensitive material unless a separate written handling agreement is in place.

Auditability and removal

- The CloudFormation template is visible before launch and can be reviewed by a customer’s AWS/security team.
- AWS CloudTrail can record API calls made by the assumed audit role when CloudTrail is enabled in the customer account.
- Cloud Approver records scanner API call metadata such as service, action, region, scanner, timing, status, error code, and AWS request ID.
- The customer can remove access by deleting the CloudFormation stack or the IAM role from the AWS account.
- If the role name or policies change, Cloud Approver marks the connection for review and may fail closed until the setup is corrected.

Important limitation

- Read-only scanner access helps Cloud Approver identify evidence and recommendations, but it does not guarantee every cost issue, security exposure, compliance concern, or configuration drift event will be detected.
- Approval codes are governance markers and drift indicators. They are not an AWS security boundary, and customers remain responsible for who can edit tags in their own cloud accounts.