

Set Up IAM Role Permissions for an AWS EC2 AIQ Controller

Set Up IAM Role Permissions for an AWS EC2 AIQ Controller

Use an IAM role for an EC2-hosted AIQ Controller when the controller must access AWS services without long-lived access keys. Scope permissions to the exact services and resources required by the integration.

Security checklist

- Prefer an EC2 instance profile over static IAM user keys.
- Create a least-privilege policy for the required AWS services, actions, and resources.
- Attach the role only to the AIQ Controller instances that need the access.
- Use tags, account boundaries, and environment separation to avoid cross-environment access.
- Review CloudTrail or equivalent logs after the first validation run.

Validation workflow

1. Attach the IAM role or instance profile to the EC2 Controller.

2. Restart or refresh the integration if required by the workflow.
3. Run a small AIQ operation that uses the AWS permission.
4. Confirm access succeeds and no broader permissions are required.
5. Document role name, policy owner, AWS account, and review date.

Last updated: October 8, 2026

Revision #3

Created 2026-07-31 16:29:38 UTC by Admin

Updated 2026-10-09 05:28:47 UTC by mmora