AiVRIC

Getting Started: Configuring the AWS Cloud Provider

Overview

This guide provides step-by-step instructions for configuring Amazon Web Services (AWS) as a cloud provider within AiVRIC to enable automated scans and resource analysis. Proper configuration ensures secure access, accurate data collection, and compliance with organizational policies.

Prerequisites

Before beginning the configuration, ensure the following:

- An active AWS account with administrative privileges or equivalent IAM permissions.
- Access to the AiVRIC platform with administrator rights.
- AWS CLI installed and configured (optional but recommended).
- Network access to AWS APIs from the AiVRIC environment.

Step 1: Create an IAM Role for AiVRIC

1. Log in to the **AWS Management Console**.
2. Navigate to **IAM** → **Roles** → **Create Role**.
3. Select **Another AWS Account** as the trusted entity type.
4. Enter the **AiVRIC Account ID** provided in the platform setup instructions.
5. Enable **Require external ID** and enter the external ID generated by AiVRIC.
6. Click **Next** to attach permissions.

Recommended Policies

Attach the following AWS managed policies:

- AmazonEC2ReadOnlyAccess
- AmazonS3ReadOnlyAccess
- AWSLambdaReadOnlyAccess
- AmazonVPCReadOnlyAccess
- AWSConfigUserAccess

Optionally, create a custom policy for more granular control.

1. Name the role AiVRICScanRole and complete the creation process.
2. Copy the **Role ARN** for later use.

Step 2: Configure the Role in AiVRIC

1. Log in to the **AiVRIC Dashboard**.
2. Navigate to **Settings → Cloud Providers → Add Provider**.
3. Select **AWS** from the list of supported providers.
4. Enter the following details:
   - **Provider Name:** AWS
   - **Role ARN:** Paste the ARN copied from AWS.
   - **External ID:** Use the same external ID configured in AWS.
5. Click **Validate Connection** to test access.
6. Once validated, click **Save Configuration**.

Step 3: Verify Connection and Permissions

1. In AiVRIC, open the **Cloud Providers** list.
2. Confirm that the AWS provider status shows **Connected**.
3. Run a **Test Scan** to verify that AiVRIC can access AWS resources.
4. Review the scan logs for any permission or connectivity issues.

Step 4: Configure Scan Settings

1. Navigate to **Scans → Configuration**.
2. Select **AWS** as the target provider.
3. Choose the desired **Regions** and **Resource Types** (e.g., EC2, S3, Lambda).
4. Set the **Scan Frequency** (manual, scheduled, or continuous).
5. Save the configuration.

Step 5: Enable Continuous Monitoring (Optional)

1. Go to **Monitoring → Cloud Events**.
2. Enable **AWS EventBridge Integration** for real-time updates.
3. Provide the EventBridge rule ARN if required.
4. Save and activate the integration.

Step 6: Review Security and Compliance Settings

- Ensure that the IAM role follows the principle of least privilege.
- Rotate credentials periodically.
- Enable AWS CloudTrail for audit logging.
- Review AiVRIC’s compliance dashboard for AWS-specific findings.

Troubleshooting

Issue	Possible Cause	Resolution
Connection failed	Incorrect Role ARN or External ID	Verify both values and revalidate
Access denied errors	Insufficient IAM permissions	Attach required read-only policies
Scan incomplete	Region not selected	Add missing regions in scan configuration
Validation timeout	Network or firewall restrictions	Allow outbound access to AWS APIs

Next Steps

- Configure additional cloud providers if applicable.
- Set up notification channels for scan results.
- Review the AiVRIC documentation for advanced automation and reporting features.

Support

For assistance, contact the AiVRIC support team or visit the documentation portal at **aivric.com/support**