Dynatrace AWS Integration – Detailed Guide

# Overview: Dynatrace-AWS Integration

Dynatrace integrates with AWS to ingest metrics from:  
- CloudWatch (EC2, RDS, S3, Lambda, etc.)  
- AWS Tags  
- Auto-scaling groups, ELBs  
- Billing/usage metrics  
  
It uses a cross-account IAM role and CloudWatch APIs.

# Pre-requisites

- AWS account with admin access  
- Dynatrace SaaS or Managed account  
- Dynatrace Environment ID and API Token

# Step 1: Login to Dynatrace

1. Go to Settings → Cloud and Virtualization → AWS  
2. Click on "Connect new AWS account"

# Step 2: Generate External ID and Role Name

1. Dynatrace provides:  
 - Role Name (e.g., Dynatrace\_monitoring\_role)  
 - External ID (for trust policy)  
2. Copy both values for use in IAM setup

# Step 3: Create IAM Role in AWS

1. IAM → Roles → Create Role  
2. Choose "Another AWS account"  
3. Enter Dynatrace account ID: 018094539430  
4. Enable "Require external ID" and paste from Dynatrace

# Step 4: Attach Custom Policy

Sample policy:  
  
{  
 "Version": "2012-10-17",  
 "Statement": [{  
 "Sid": "AllowCloudWatchAndServiceReadAccess",  
 "Effect": "Allow",  
 "Action": [  
 "cloudwatch:GetMetricData",  
 "cloudwatch:GetMetricStatistics",  
 "cloudwatch:ListMetrics",  
 "ec2:DescribeInstances",  
 "ec2:DescribeRegions",  
 "ec2:DescribeTags",  
 "rds:DescribeDBInstances",  
 "lambda:ListFunctions",  
 "lambda:ListTags",  
 "s3:ListAllMyBuckets",  
 "autoscaling:DescribeAutoScalingGroups",  
 "tag:GetResources",  
 "elasticloadbalancing:Describe\*",  
 "pricing:GetProducts"  
 ],  
 "Resource": "\*"  
 }]  
}

# Step 5: Trust Policy Example

{  
 "Version": "2012-10-17",  
 "Statement": [{  
 "Effect": "Allow",  
 "Principal": {  
 "AWS": "arn:aws:iam::018094539430:root"  
 },  
 "Action": "sts:AssumeRole",  
 "Condition": {  
 "StringEquals": {  
 "sts:ExternalId": "your-dynatrace-external-id"  
 }  
 }  
 }]  
}

# Step 6: Finalize in Dynatrace

1. Paste the Role ARN into Dynatrace (from AWS console)  
2. Choose services/regions to monitor  
3. Save and finish setup

# Monitored Services

- EC2, S3, RDS, Lambda  
- ELB/ALB  
- CloudWatch metrics and tags

# Best Practices

- Use least-privilege policies  
- Rotate external ID if needed  
- Use AWS tags for grouping  
- Enable Davis AI anomaly detection  
- Build AWS-specific dashboards in Dynatrace

# Troubleshooting Tips

Issue: Role creation fails → Check trust policy (no 'Resource' field)  
Issue: No data → Confirm metrics exist in CloudWatch  
Issue: Access denied → Check IAM permissions  
Issue: Metrics delayed → CloudWatch delay ~5 minutes

# Optional: CloudFormation

Use Dynatrace-provided CloudFormation script for auto-role creation.  
Available in Dynatrace integration screen.