Linux Academy | Cloud Assessments

THE DEVOPS DOCTRINE

Choose a Topic

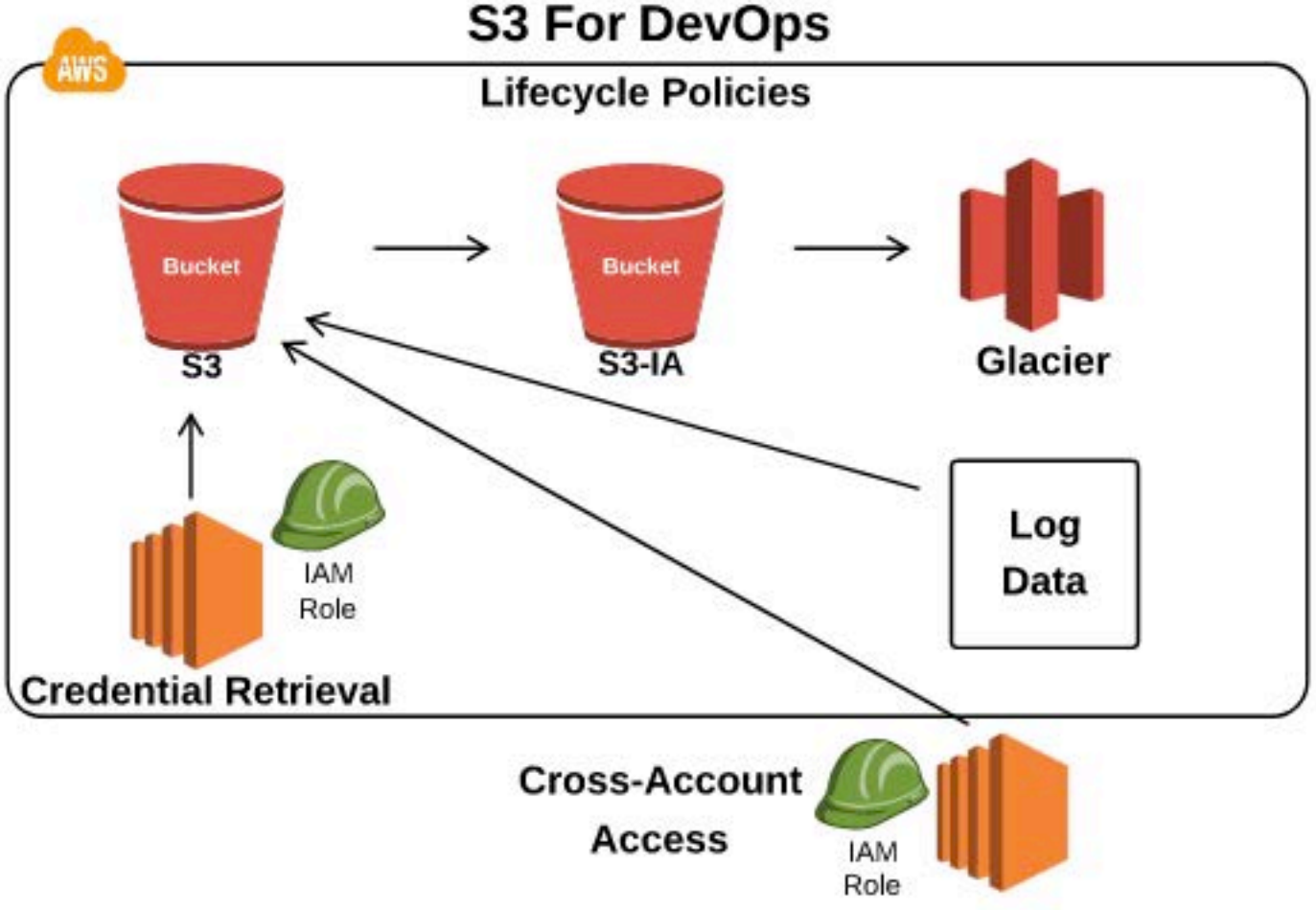
- Introduction
- Auto Scaling Deployment Concepts
- Deployment Concepts With EC2
- CloudWatch For DevOps
- CloudFormation For DevOps
- Elastic Beanstalk For DevOps
- Application Deployments With OpsWorks
- DynamoDB Concepts
- S3 Concepts For DevOps
- Blue/Green Deployments
- Scenario Solver
- Deployment Pipelines
- API Gateway
- Lambda

Deployment Concepts With S3

Scenario: Amazon S3 is used extensively in AWS DevOps operations. Its low cost and high durability dictates that it should always be considered as a storage option. Additionally, S3 provides comprehensive security and compliance capabilities that meet even the most stringent regulatory requirements. Devops specific uses for S3 include Log Data storage, secure storage to only be accessed via IAM Roles, and configuring cross-account access for S3 access from other AWS accounts.

- Lifecycle Management
- Exporting Log Data
- S3 Intelligent Tiering
- S3 Endpoints
- Cross-Account Access

S3 For DevOps

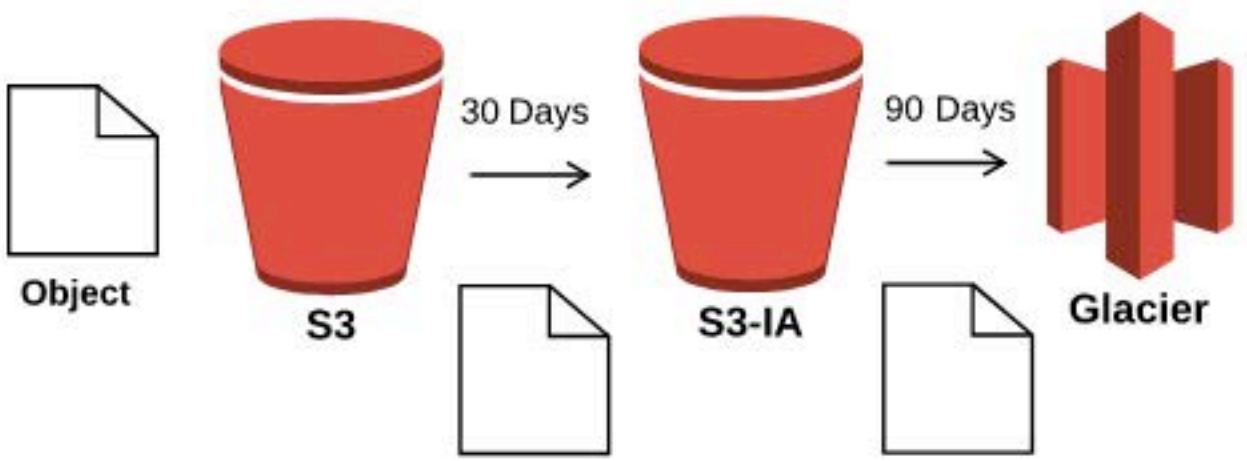


Deployment Concepts With S3

X

AWS

S3 Object Lifecycle Management



Object Lifecycle Management

- S3 Pricing Model - Charges depend on the amount of data being stored, how many requests are performed, and how much data is transferred out.
- S3 Storage Classes:
  - **Standard** - Pros: 99.999999999 % durability, high availability. Cons: Not the cheapest
  - **S3 Infrequent Access** - Pros: 99.999999999% durability, lower request costs, great for data that needs to be readily available but not frequently accessed. Cons: Higher request costs, lower availability.
  - **Amazon Glacier** - Used for rarely accessed data. Pros: Low storage cost per GB, highly durable. Cons: Very slow data retrieval, requests are expensive.
- We can manage an object's lifecycle by using lifecycle configurations which tell S3 how to manage objects during their lifecycle. Lifecycle actions:
  - Transition actions - define when to move objects to another storage class.
  - Expiration actions - specify when an object expires and should be deleted.
- Lifecycle Management Limitations:
  - Objects must be stored at least 30 days before they can transition to S3 IA.
  - You can not transition backwards (S3-IA to S3, or Glacier to any other class).

Deployment Concepts With S3

Back

AWS

S3 Intelligent Tiering

S3 Storage Classes - Focus on Intelligent Tiering

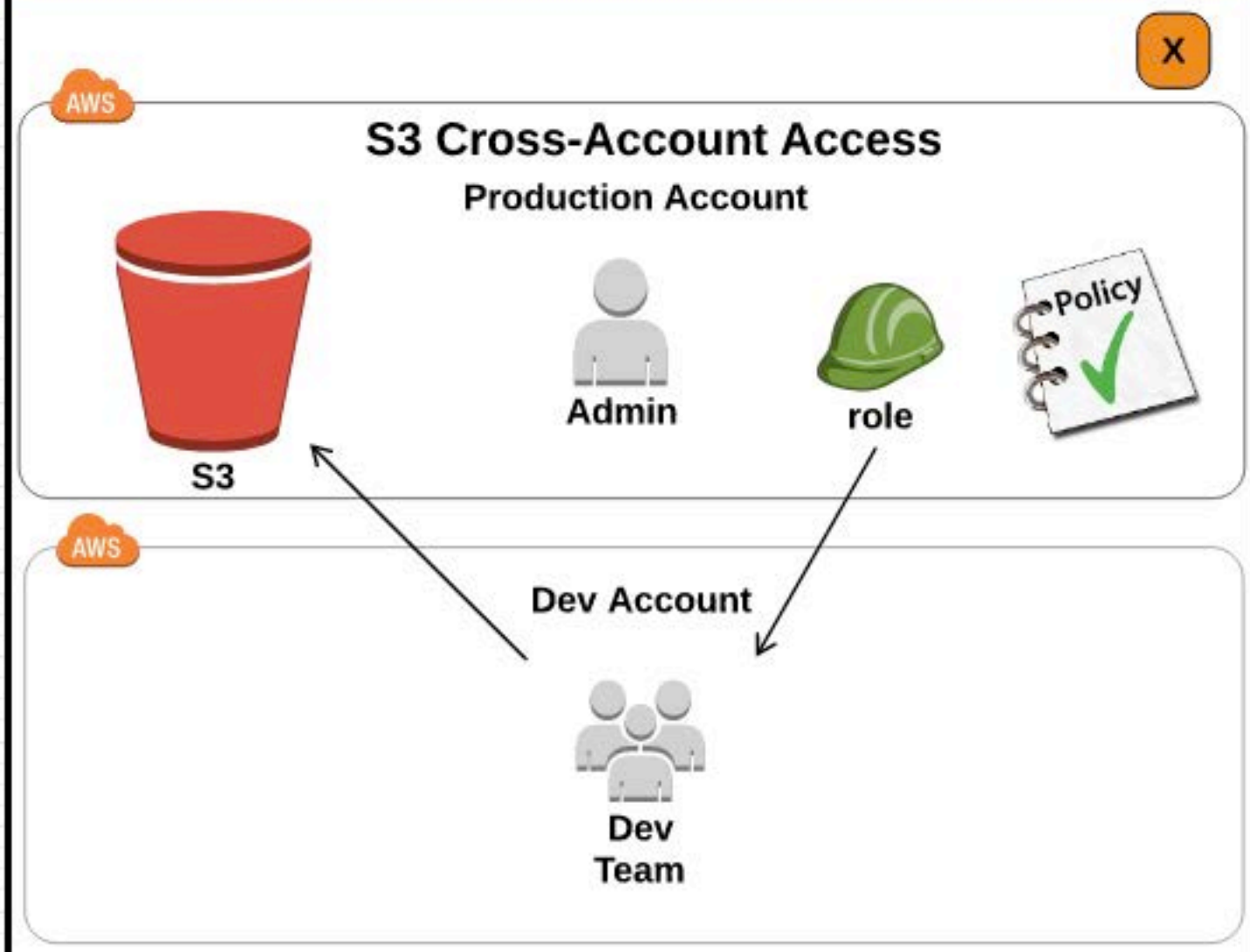
- S3 Standard - Frequently accessed data. High durability, availability, and performance.
- S3 Intelligent Tiering - Designed to optimize costs by automatically moving data to the most cost-effective access tier, without performance impact or operational overhead.
- S3 Standard IA - For data that is accessed less frequently, but requires rapid access when needed.
- S3 One Zone IA - Data that is accessed less frequently, but requires rapid access when needed. Because S3 One Zone-IA stores data in a single AWS Availability Zone, data stored in this storage class will be lost in the event of Availability Zone destruction.
- Galcier - Secure, durable, and low-cost storage class for data archiving.

Intelligent Tiering Details

- The first cloud object storage class that delivers automatic cost savings by moving data between two access tiers — frequent access and infrequent access — when access patterns change, and is ideal for data with unknown or changing access patterns.
- Uses Machine Learning to move objects that have not been accessed for 30 days.
- If infrequent accessed data is then accessed, it is then moved back to frequent access tier.
- Allows you to bypass Lifecycle Rules. The data lifecycle is handled by intelligent tiering.

Choose a Topic

Deployment Concepts With S3



Cross-Account Access

Step 1 - Create an Access Policy to be attached to a role
Step 2 - Create a Role in the Prod account to be used by Dev
Step 3 - Associate the role with the Dev account
Step 4 - Attach the access policy to the role
Step 5 - Record the Role ARN
Step 6 - Modify the Dev user account to enable switching to the role
Step 7 - Test access by switching to the new role

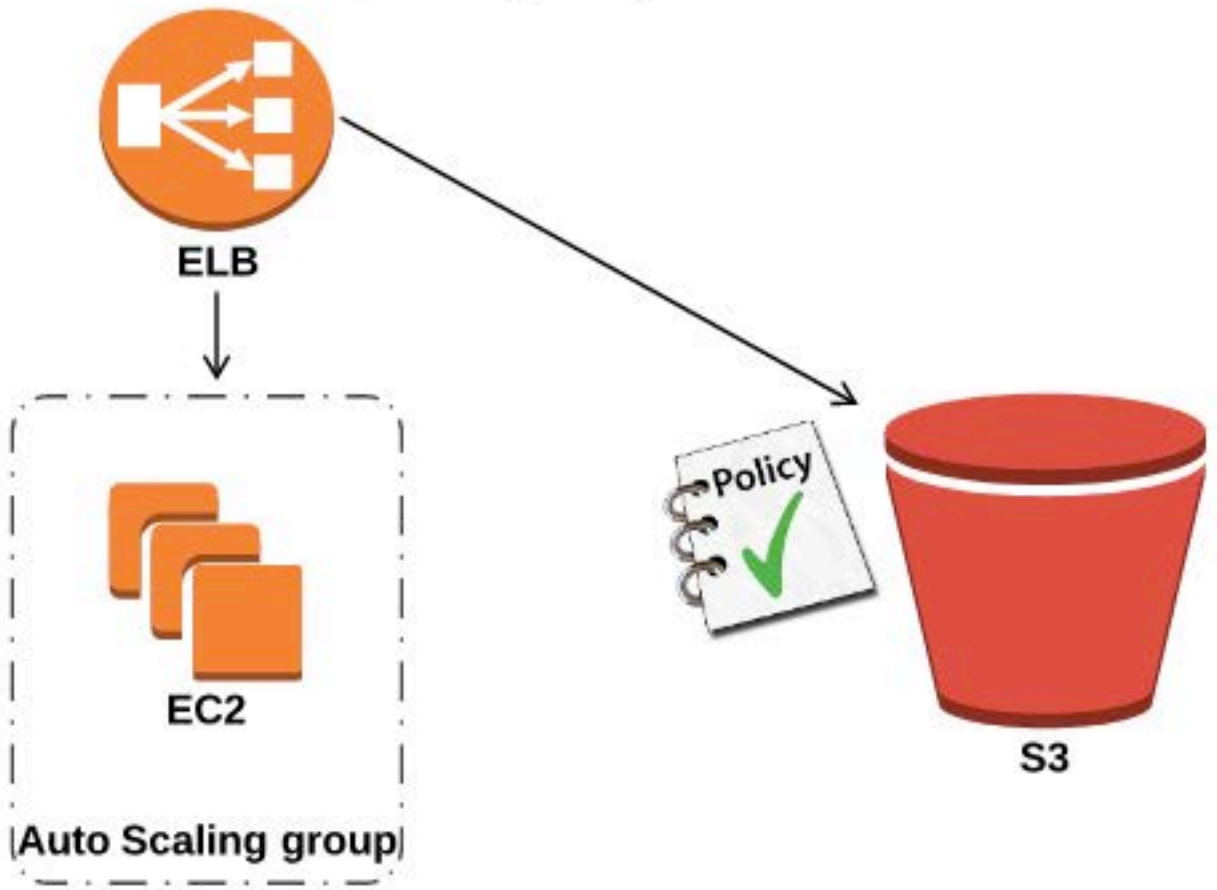
Choose a Topic

Deployment Concepts With S3

X

AWS

Exporting Log Data To S3



Exporting Log Data To S3

Step 1 - Create an Amazon S3 Bucket
Step 2 - Set permissions on the S3 Bucket
Step 3 - In S3, go to Policy Generator
Step 4 - Generate a Policy for S3 granting permission to the Load Balancer to store Access Logs in the S3 Bucket.
Step 5 - Copy and paste the policy generated into the S3 Bucket Policy area and click 'Save'.
Step 6 - Go to EC2, select 'Load Balancers, select your Load Balancer.
Step 7 - On the 'Description' tab, choose 'Configure Access Log', enable access logs, and specify your S3 location to store the logs.
Step 8 - Go to S3 and verify receipt of the test log file.