

# S3 Security Best Practices

John Mallory, Storage BDM

July 2018

# Least Privilege



- Security best practice:
  - Start with a minimum set of permissions
  - Grant additional permissions as *necessary*
- Defining the right set of permissions requires some research
  - What actions a particular service supports
  - What is required for the specific task
  - What permissions are required in order to perform those actions

# Let's Start with IAM

- Create and manage AWS users, groups, and permissions to control access to AWS resources
- Integrates with Microsoft Active Directory using SAML identity federation and AWS Directory Service
- Roles can be created and assumed to control what operations can be performed by an entity or AWS service (e.g. EC2 instance)

# Amazon S3 IAM Policies

- *“What can this user do in AWS?”*
- Directly grants access to Amazon S3 service actions
- Access control policy managed within the IAM environment and set by IAM administrators
- Attached to IAM users or roles—including EC2 Instance profiles
- Optional: can specify buckets and prefixes

```
{  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets"
      ],
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:DeleteObject"
      ],
      "Resource": "arn:aws:s3:::reinventbucket/*"
    }
  ]
}
```

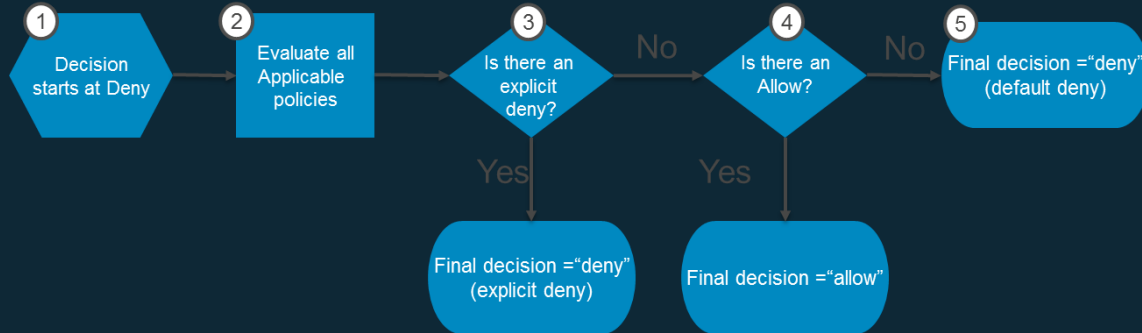
# Amazon S3 Bucket Policies

- *“Who can access this S3 bucket?”*
- Further defines bucket access
- Policies are attached directly to the Amazon S3 bucket itself
- Control belongs to the Amazon S3 bucket owner
- A simple way to grant cross-account access to your Amazon S3 environment, without using IAM roles
- Keeps access control policies in the Amazon S3 environment

```
{
  "Version": "2012-10-17",
  "Id": "123",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3::reinventbucket/taxdocuments/*",
      "Condition": {"Null": {"aws:MultiFactorAuthAge": true }}
    }
  ]
}
```

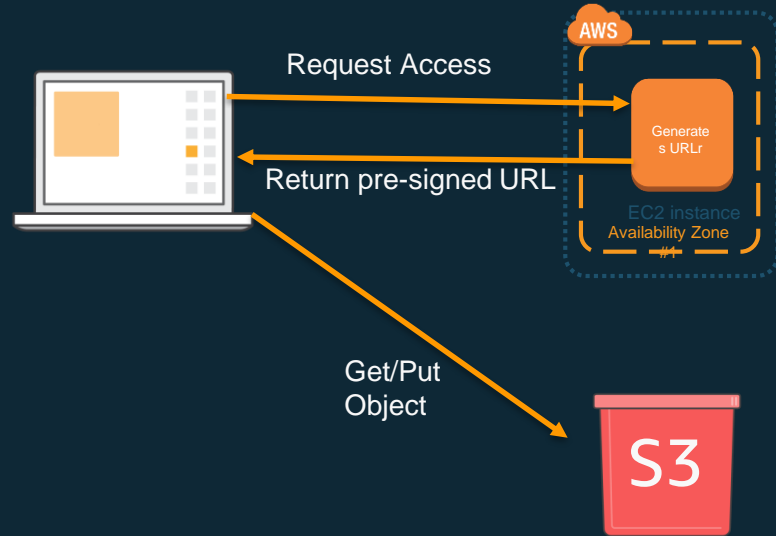
# Amazon S3 Access Control Lists (ACLs)

- Amazon S3 ACLs manage permissions on individual objects
- Bucket policies are only applied at the bucket or prefix level
- ACLs grant access (cannot explicitly deny)
- Only apply to principals outside the AWS account
- Allow predefined groups like “Everyone”
- Authorization is always a **union** of IAM policies, bucket policies, and ACLs:



# Pre-signed URLs

- Provide access to PUT/GET objects without opening permissions to do anything else
- Uses permissions of the user who creates the URL
- To generate URL, provide your security credentials, a bucket name, an object key, HTTP method (GET or PUT) and expiration date and time
- Only valid until expiration time



# Why encrypt in the cloud?

## What everyone says:

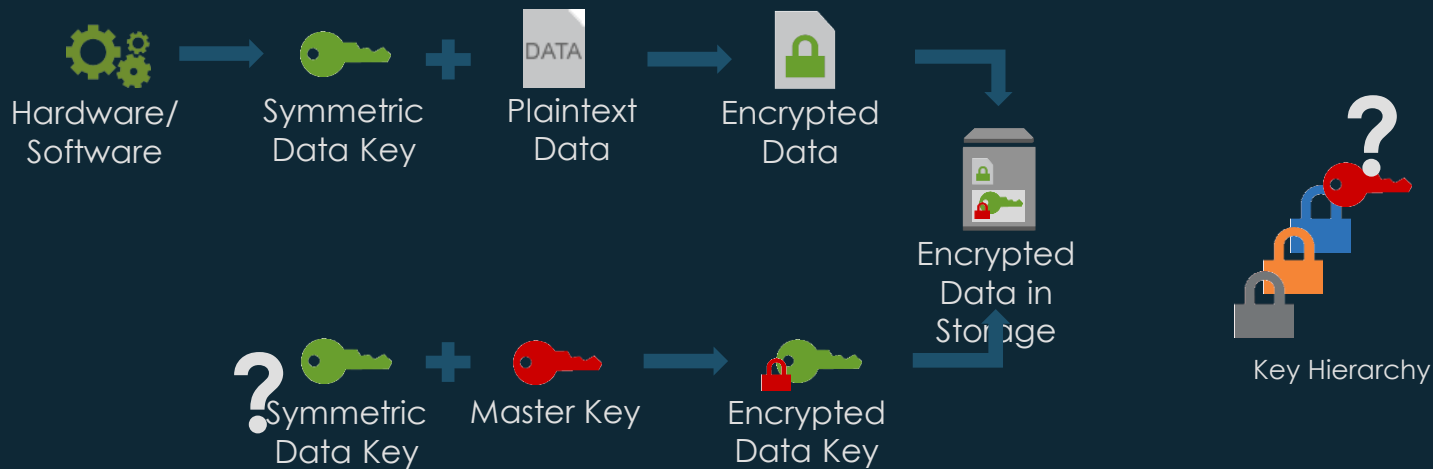
- Compliance
- Best practice in security
- Protect myself from my cloud provider's other customers
- Protect myself from my cloud provider

## What everyone means:

- Minimizing unauthorized physical access to data
- Minimizing unauthorized logical access to data
- **Confidentiality, Integrity, Availability**



# Encryption Primer



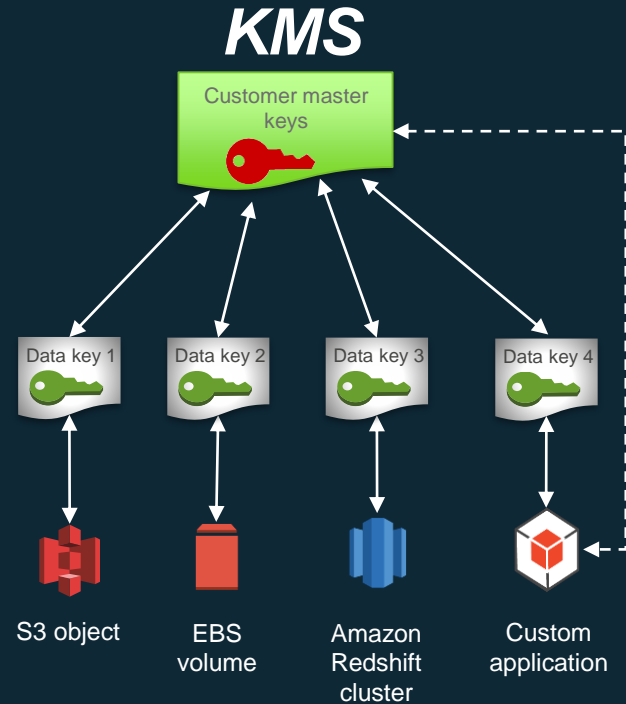
# Server-Side Encryption in AWS

Two-tiered key hierarchy using envelope encryption

- Unique data key encrypts customer data
- Customer Master Keys encrypt data keys

## Benefits

- Limits risk of compromised data key
- Better performance for encrypting large data
- Easier to manage small number of master keys than billions of data keys
- Centralized access and audit of key activity



# Encryption support in Amazon S3

- Encryption in motion—HTTPS/TLS
- Encryption at rest
  - Client-side encryption—encrypt before upload
  - Server-side encryption
    - SSE-S3—Amazon S3 manages the data and master encryption keys
    - SSE-C—you manage the encryption key
    - SSE-KMS—Amazon S3 manages the data key, you manage the master key in the AWS Key Management Service (AWS KMS)



# What's new for S3 Security

## S3 Inventory

- Encryption Status
- encrypt output using SSE-S3 or SSE-KMS

## Cross-Region Replication (CRR)

- CRR for KMS-encrypted objects
- CRR-Ownership Override

## Security Management

- Default Encryption  **wow**
- Bucket Permissions Check in S3 Console



# S3 Inventory



Object level  
Encryption Status



Encrypt inventory  
with SSE or KMS



ORC output format



Query with Athena

# How to Encrypt Inventory Report using KMS?

*You must grant Amazon S3 permission to encrypt using your AWS KMS key with a key policy.*

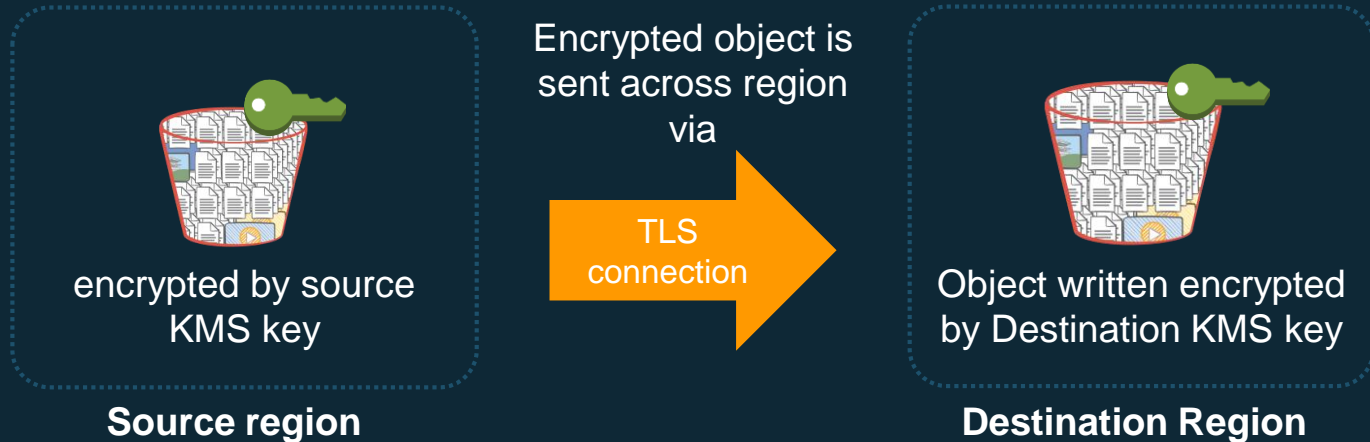
- ❏ Sign in to the AWS Management Console using the AWS account that owns the AWS KMS CMK and open the AWS Identity and Access Management (IAM) console
- ❏ In the left navigation pane, choose **Encryption keys**
- ❏ For **Region**, choose the appropriate AWS Region. Do not use the region selector in the navigation bar (top right corner) – KMS keys are region specific
- ❏ Choose the alias of the CMK that you want to encrypt inventory with
- ❏ In the **Key Policy** section of the page, choose **Switch to policy view**

- ❏ Copy the following key policy into the Key Policy editor and then choose Save Changes. You might want to copy the policy to the end of the existing policy

```
{
  "Sid": "Allow Amazon S3 use of the key",
  "Effect": "Allow",
  "Principal": {
    "Service": "s3.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey*"
  ],
  "Resource": "*"
}
```

# Cross-Region Replication – Support for KMS

Introducing CRR support for objects created with SSE using AWS KMS-Managed Keys



# Cross-Region Replication – Ownership Override

## Introducing Ownership Override

*In a cross account scenario, you can now direct S3 to change replica ownership to the destination bucket owner* **New**



*For business continuity, you can use the Object Ownership Override to separate the access control of source objects and replicated objects, so the **source object owners cannot read, update, or delete the replicated objects in the destination.***



# Cross-Region Replication – Ownership Override

## How it works:

- Add the <Account> and <AccessControlTranslation> elements as the child element of the <Destination> element
- Add permissions to the IAM role to allow Amazon S3 to change replica ownership
- Add permissions for the s3:ObjectOwnerOverrideToBucketOwner action to allow AWS account that owns the source bucket permission to change replica ownership

# Cross-Region Replication – Support for KMS

## How it works:

- ❏ KMS keys are region specific
- ❏ Specify Destination KMS Master key in replication configuration
- ❏ You can specify different KMS master key by prefix
- ❏ Objects remain encrypted throughout the replication process
- ❏ Provide the AWS KMS-managed key for the destination bucket region, that you want S3 to use to encrypt object replicas.
- ❏ Grant additional permissions to the IAM role so that Amazon S3 can access the objects using the KMS key.

## Best practices:

- ❏ Request an increase in KMS API rate limit by creating a case at AWS Support Center.
- ❏ We recommend confirming the rate limit increase before enabling CRR-KMS.
- ❏ There is no additional cost for KMS API rate increase.

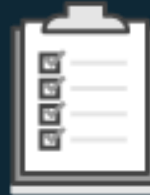
# Encryption by Default for S3 Buckets *New*



One time bucket level set up



Automatically encrypt all new objects



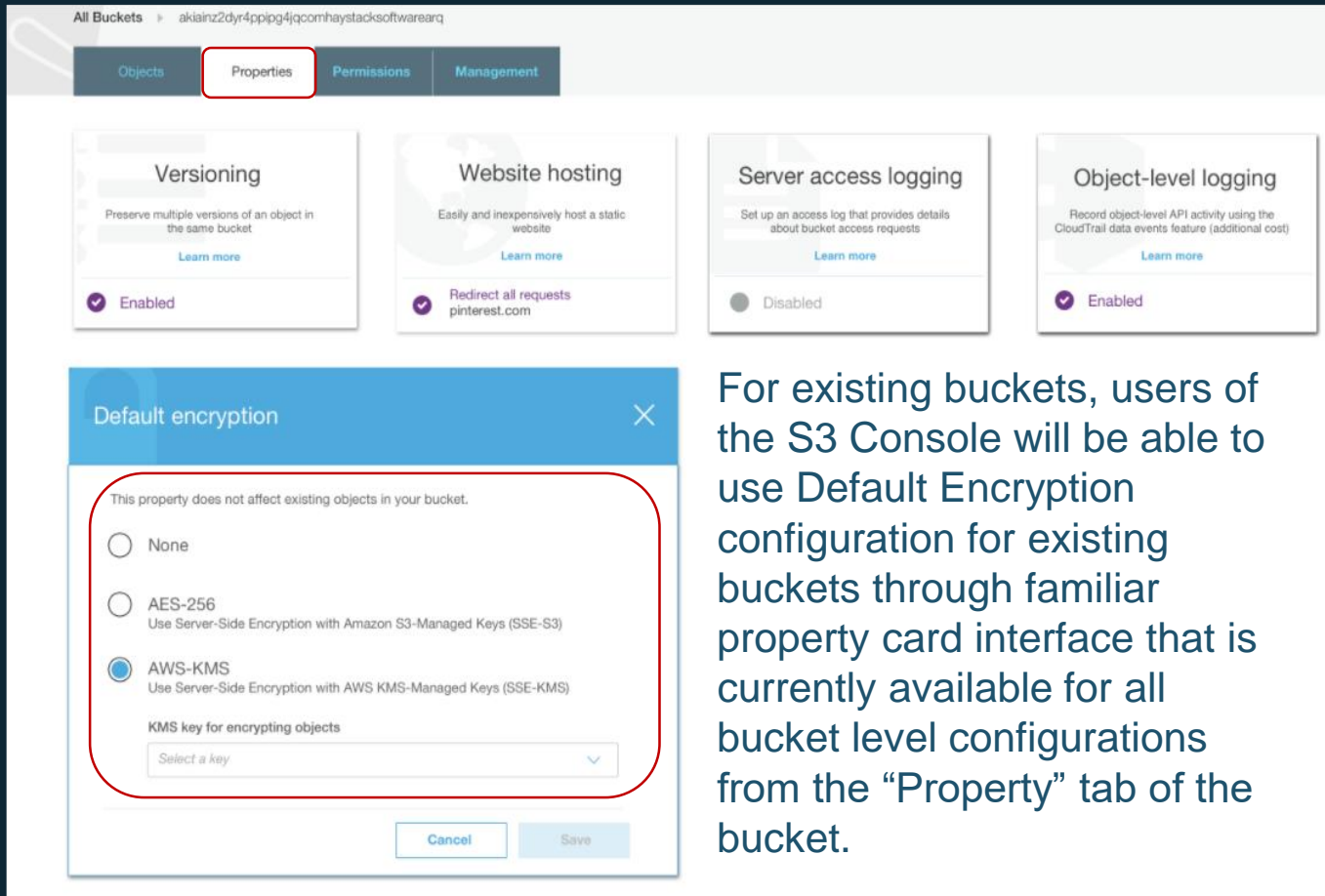
Simplified compliance



Supports SSE-S3 and SSE-KMS

Provides S3 encryption-at-rest support for applications that do not otherwise support encrypting data in S3

# Encryption by Default for S3 Buckets – What it Looks Like



The screenshot displays the AWS S3 console interface for a bucket named 'akiainz2dyr4ppipg4jqcomhaystacksoftwareaq'. The 'Properties' tab is selected and highlighted with a red box. Below the navigation tabs, there are four property cards: 'Versioning' (Enabled), 'Website hosting' (Redirect all requests to pinterest.com), 'Server access logging' (Disabled), and 'Object-level logging' (Enabled). A 'Default encryption' dialog box is open in the foreground, also with a red border. It contains the following options:

- None
- AES-256  
Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)
- AWS-KMS  
Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Below these options is a dropdown menu labeled 'KMS key for encrypting objects' with the text 'Select a key' and a downward arrow. At the bottom of the dialog are 'Cancel' and 'Save' buttons.

For existing buckets, users of the S3 Console will be able to use Default Encryption configuration for existing buckets through familiar property card interface that is currently available for all bucket level configurations from the “Property” tab of the bucket.

# Encryption by Default for S3 Buckets – How Does it Work?

- Ensure all PUT requests include encryption information
- Set bucket policy to reject all unencrypted PUT requests

B  
E  
F  
O  
R  
E



A  
F  
T  
E  
R

- Setup S3 bucket to automatically encrypt objects irrespective of PUT request having encryption information

## API Requests -

- PUT Bucket Encryption
- DELETE Bucket Encryption
- GET Bucket Encryption

Permission –  
S3:GetEncryptionConfiguration,  
S3:PutEncryptionConfiguration

## Remember..

- Only **NEW** objects will be encrypted as per settings
- PUT Bucket encryption requires SigV4
- SSE-KMS:
  - Incoming PUT and GET have to be sent over SSL connection
  - Signed with SigV4
  - KMS RPS Limits

## Target Customer Segments:

- Certification requirements such as PCI or SOC2.
- Regulatory requirements such as HIPAA.
- Business requirements due to a business policy or a customer commitment.

# Security Inspection



**Trusted Advisor**



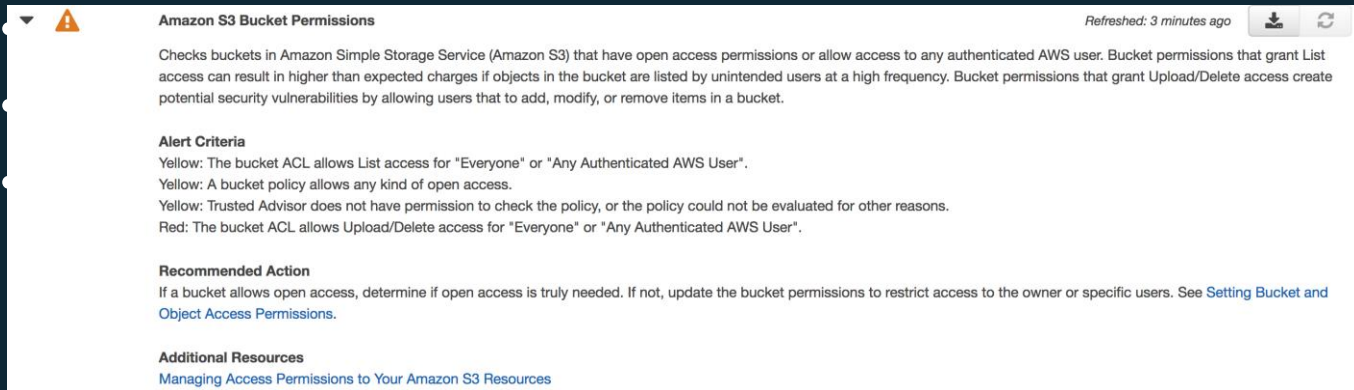
**Bucket access  
control view  
S3 console**



**Object  
encryption status  
S3 inventory**

# Monitoring with Trusted Advisor

- Trusted Advisor service provided by AWS Support has three Amazon S3-related checks



The screenshot shows the 'Amazon S3 Bucket Permissions' check in the AWS Trusted Advisor console. The check is marked with a yellow warning icon. The text describes the check's purpose: to identify buckets with open access permissions that could lead to higher charges or security vulnerabilities. It includes sections for 'Alert Criteria' (listing yellow and red alerts), 'Recommended Action' (advising on restricting access), and 'Additional Resources' (linking to a guide on managing permissions).

**Amazon S3 Bucket Permissions** Refreshed: 3 minutes ago

Checks buckets in Amazon Simple Storage Service (Amazon S3) that have open access permissions or allow access to any authenticated AWS user. Bucket permissions that grant List access can result in higher than expected charges if objects in the bucket are listed by unintended users at a high frequency. Bucket permissions that grant Upload/Delete access create potential security vulnerabilities by allowing users that to add, modify, or remove items in a bucket.

**Alert Criteria**

Yellow: The bucket ACL allows List access for "Everyone" or "Any Authenticated AWS User".  
Yellow: A bucket policy allows any kind of open access.  
Yellow: Trusted Advisor does not have permission to check the policy, or the policy could not be evaluated for other reasons.  
Red: The bucket ACL allows Upload/Delete access for "Everyone" or "Any Authenticated AWS User".

**Recommended Action**

If a bucket allows open access, determine if open access is truly needed. If not, update the bucket permissions to restrict access to the owner or specific users. See [Setting Bucket and Object Access Permissions](#).

**Additional Resources**

[Managing Access Permissions to Your Amazon S3 Resources](#)

# Bucket Permission Check on S3 Console <sup>New</sup>

*Examines bucket ACLs and bucket policies to determine if the bucket is publicly accessible.*

## 📦 Checks buckets in S3 that have open access permissions

- Bucket permissions that grant LIST access to everyone can result in higher than expected charges if objects in the bucket are listed by unintended users at a high frequency
- Bucket permissions that grant Upload/Delete access to everyone create potential security vulnerabilities by allowing anyone to add, modify, or remove items in a bucket

## 📦 Terminology:

- PUBLIC: means any authenticated AWS user + Everyone (making 'anonymous' calls)
- ACCESS: means READ, WRITE, READ\_ACP, WRITE\_ACP

## 📦 Bucket permission check does not check Object ACLs





# Bucket Access Control View – What it Looks Like?

Welcome to Amazon S3. Create a new bucket or select an existing bucket to view objects or configure properties. [Documentation](#)

Amazon S3 [Switch to old console](#) [Intro to new console](#) [Quick Tips](#)

Search the Bucket

[+ Create bucket](#) [Delete bucket](#) [Empty bucket](#) 67 Buckets **3 Public** 2 Regions [Refresh](#)

Bucket name	Access	Region	Date created
a-Shawn	Not public *	US West	Dec 04
akiaia4fhnvwtkn2o6acomhaystacksoftwarear	Public	US West	Today
akiaia6lrzy4mflppvacomhaystacksoftwarear	Not public *	US West	Yesterday
akiainz2dyr4ppipg4jqcomhaystacksoftwarearq	Not public *	US West	Dec 20
akiais2xhe6jheqhur7acomhaystacksoftwarearq	Public	US West	Dec 30
akiais2xhe6jheqhur7acomhaystacksoftwarearq-us-west-2	Not public *	Oregon	Dec 04
akiaia4fhnvwtkn2o6acomhaystacksoftwarear	Not public *	EU (Ireland)	Today
akiaia6lrzy4mflppvacomhaystacksoftwarear	Not public *	EU (Frankfurt)	Yesterday
akiainz2dyr4ppipg4jqcomhaystacksoftwarearq	Not public *	Asia Pacific	Dec 20
akiais2xhe6jheqhur7acomhaystacksoftwarearq	Public	(Sydney)	Dec 30
akiais2xhe6jheqhur7acomhaystacksoftwarearq-us-west-2	Not public *	EU (Ireland)	Dec 31
akiaia4fhnvwtkn2o6acomhaystacksoftwarear	Not public *	EU (Frankfurt)	Today
akiaia6lrzy4mflppvacomhaystacksoftwarear	Not public *	Asia Pacific	Dec 20
akiainz2dyr4ppipg4jqcomhaystacksoftwarearq	Not public *	Sydney	Dec 30
akiais2xhe6jheqhur7acomhaystacksoftwarearq	Not public *	(Sydney)	Dec 31
akiais2xhe6jheqhur7acomhaystacksoftwarearq-us-west-2	Not public *	Asia Pacific	Today
akiainz2dyr4ppipg4jqcomhaystacksoftwarearq	Not public *	(Sydney)	Dec 20

# Bucket Access Control View – What it Looks Like?

Welcome to Amazon S3. Create a new bucket or select an existing bucket to view objects or configure properties. [Documentation](#) ✕

Amazon S3 [Switch to old console](#) [Intro to new console](#) [Quick Tips](#)

Permissions

Buckets with any public access (read/write)

Buckets with public read access

Buckets with public write access

akiaia6lrzy4mflppvacomhaystacksoftwarear	Not public *	US West	Yesterday
akiainz2dyr4ppig4jqcomhaystacksoftwarearq	Not public *	US West	Dec 20
akiais2xhe6jheqhur7acomhaystacksoftwarearq	Public	US West	Dec 30
akiais2xhe6jheqhur7acomhaystacksoftwarearq-us-west-2	Not public *	Oregon	Dec 04
akiai4fnvwtlkn2o6acomhaystacksoftwarear	Not public *	EU (Ireland)	Today
akiaia6lrzy4mflppvacomhaystacksoftwarear	Not public *	EU (Frankfurt)	Yesterday
akiainz2dyr4ppig4jqcomhaystacksoftwarearq	Not public *	Asia Pacific	Dec 20
akiais2xhe6jheqhur7acomhaystacksoftwarearq	Public	(Sydney)	Dec 30
akiais2xhe6jheqhur7acomhaystacksoftwarearq-us-west-2	Not public *	EU (Ireland)	Dec 31
akiai4fnvwtlkn2o6acomhaystacksoftwarear	Not public *	EU (Frankfurt)	Today
akiaia6lrzy4mflppvacomhaystacksoftwarear	Not public *	Asia Pacific	Dec 20
akiainz2dyr4ppig4jqcomhaystacksoftwarearq	Not public *	Sydney	Dec 30
akiais2xhe6jheqhur7acomhaystacksoftwarearq	Not public *	(Sydney)	Dec 31
akiais2xhe6jheqhur7acomhaystacksoftwarearq-us-west-2	Not public *	Asia Pacific	Today
akiainz2dyr4ppig4jqcomhaystacksoftwarearq	Not public *	(Sydney)	Dec 20

# Bucket Access Control View – What it Looks Like?

Welcome to Amazon S3. Create a new bucket or select an existing bucket to view objects or configure properties. [Documentation](#) ×

Amazon S3 Switch to old console Intro to new console Quick Tips

Q permission Public: Read × permission Public: Write ×

[+ Create bucket](#) [Delete bucket](#) [Empty bucket](#) 3 Buckets **3 Public** 2 Regions ↻

Bucket name <span>↓</span>	Access <span>↓</span> ⓘ	Read <span>↓</span>	Write <span>↓</span>	Source <span>↓</span>	⚙
Buckete-50	<b>Public</b>	Everyone	Not everyone	ACL	
Bucketf-21	<b>Public</b>	Not everyone	Everyone	ACL, Bucket policy	
Bucketg-92384	<b>Public</b>	Everyone	Everyone	Bucket policy	

# Bucket Access Control View – What it Looks Like?

AMAZON S3

Global Username Support

All Buckets > Buckets-50

Overview Properties **Permissions** Management

S3 Access Control List (ACL) Public Bucket policy Public CORS configuration

Access for your AWS account

This bucket has public access. Permissions below grant access to everyone in the world.

Account	List objects	Write objects	Read bucket ACL	Write bucket ACL
<input type="radio"/> displayname1	Yes	-	Yes	Yes

Access for other AWS accounts

+ Add account Delete

Account	List objects	Write objects	Read bucket ACL	Write bucket ACL
<input type="radio"/> Displayname1	Yes	-	Yes	Yes
<input type="radio"/> Displayname2	-	-	-	-
<input type="radio"/> 79a59df00b949e55d96a1e698fbacedf6e09d98eac8f8d5218e7cd47ef2be	-	Yes	-	-
<input type="radio"/> 79a59df00b949e55d96a1e698fbacedf6e09d98eac8f8d5218e7cd47ef2be	-	Yes	Yes	-

Public access

Group	List objects	Write objects	Read bucket ACL	Write bucket ACL
<input type="radio"/> Everyone	Yes	-	-	-

S3 Log Delivery group

Group	List objects	Write objects	Read bucket ACL	Write bucket ACL
-------	--------------	---------------	-----------------	------------------

# Monitoring with AWS Config

- Managed rules to identify insecure bucket configurations:
  - s3-bucket-public-write-prohibited
  - s3-bucket-public-read-prohibited
  - s3-bucket-ssl-requests-only
- Managed rules to verify that Amazon S3 features are enabled
  - Logging
  - Versioning
- **Visualize** the changes in your Amazon S3 bucket configurations (policies, versioning, lifecycle rules)
- **Alerted** of changes via Amazon SNS

## s3-bucket-public-read-prohibited

Checks that your S3 buckets do not allow public read access. If an S3 bucket policy or bucket ACL allows public read access, the bucket is noncompliant.

---

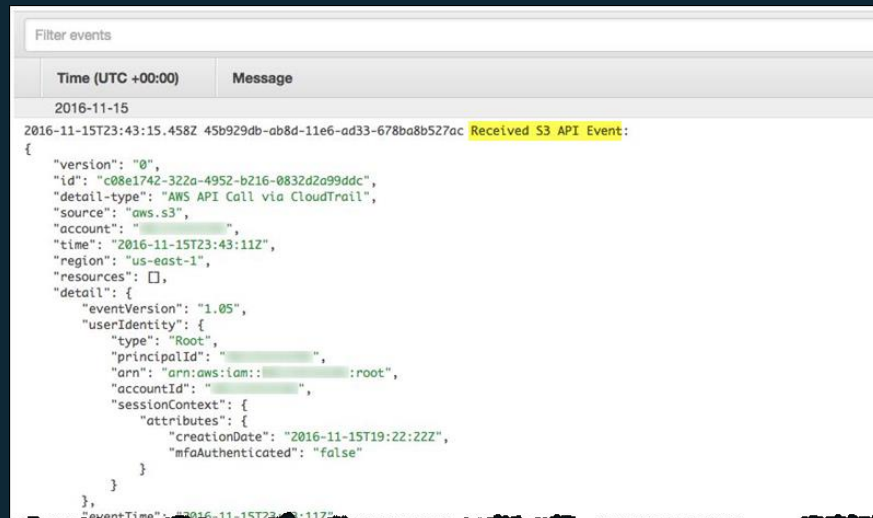
## s3-bucket-public-write-prohibited

Checks that your S3 buckets do not allow public write access. If an S3 bucket policy or bucket ACL allows public write access, the bucket is noncompliant.

---

# Monitoring with AWS CloudTrail

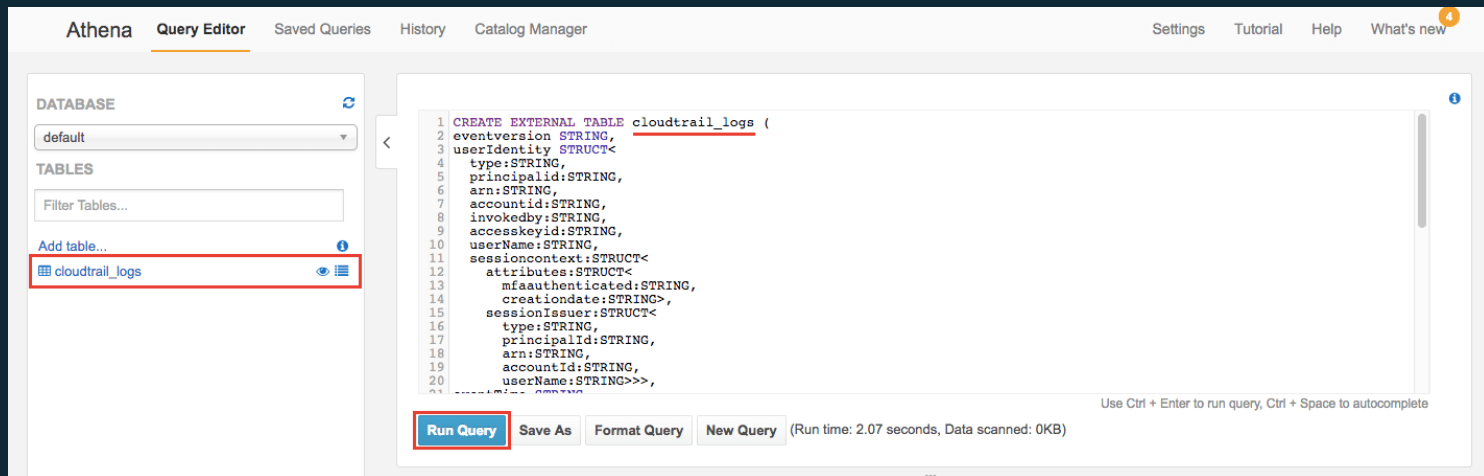
- All bucket-level actions sent to AWS CloudTrail
- Optional: object-level actions sent to AWS CloudTrail
  - Per-bucket, per-prefix, or per-object basis or for all buckets in account
  - Can be sent to Amazon CloudWatch Logs
  - Event types sent to AWS CloudTrail can be customized (read, write, or both)
- Details available for investigation via AWS CloudTrail include:
  - Source IP address
  - UserAgent
  - Access key used in the request
  - Request ID and Extended Request ID



```
Filter events
Time (UTC +00:00)  Message
2016-11-15
2016-11-15T23:43:15.458Z 45b929db-ab8d-11e6-ad33-678ba8b527ac Received S3 API Event:
{
  "version": "0",
  "id": "c08e1742-322a-4952-b216-0832d2a99ddc",
  "detail-type": "AWS API Call via CloudTrail",
  "source": "aws.s3",
  "account": " ",
  "time": "2016-11-15T23:43:11Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "eventVersion": "1.05",
    "userIdentity": {
      "type": "Root",
      "principalId": " ",
      "arn": "arn:aws:iam:: :root",
      "accountId": " ",
      "sessionContext": {
        "attributes": {
          "creationDate": "2016-11-15T19:22:22Z",
          "mfaAuthenticated": "false"
        }
      }
    }
  }
},
"eventTime": "2016-11-15T23:43:11Z"
```

# Monitoring with Amazon Athena

- Query Amazon S3 access logs or CloudTrail logs for S3-specific actions using standard SQL queries
- Enter DDL statement from <http://docs.aws.amazon.com/athena/latest/ug/cloudtrail-logs.html>
- Example query on the next slide lists all access attempts for a basketball.jpg request between 05-Oct-2017 and 29-Nov-2017, providing the user agent, source IP address, HTTP Response Code, and timestamp



The screenshot displays the Amazon Athena Query Editor interface. On the left sidebar, the 'DATABASE' dropdown is set to 'default', and the 'TABLES' list includes 'cloudtrail\_logs', which is highlighted with a red box. The main editor area contains a SQL DDL statement for creating an external table named 'cloudtrail\_logs'. The statement is as follows:

```
1 CREATE EXTERNAL TABLE cloudtrail_logs (  
2 eventversion STRING,  
3 useridentity STRUCT<  
4 type:STRING,  
5 principalid:STRING,  
6 arn:STRING,  
7 accountid:STRING,  
8 invokedby:STRING,  
9 accesskeyid:STRING,  
10 username:STRING,  
11 sessioncontext:STRUCT<  
12 attributes:STRUCT<  
13 mfaauthenticated:STRING,  
14 creationdate:STRING>,  
15 sessionissuer:STRUCT<  
16 type:STRING,  
17 principalid:STRING,  
18 arn:STRING,  
19 accountId:STRING,  
20 username:STRING>>),  
21 ...
```

At the bottom of the editor, there are buttons for 'Run Query', 'Save As', 'Format Query', and 'New Query'. The 'Run Query' button is also highlighted with a red box. Below the buttons, it indicates '(Run time: 2.07 seconds, Data scanned: 0KB)'. The top navigation bar includes 'Athena', 'Query Editor', 'Saved Queries', 'History', 'Catalog Manager', 'Settings', 'Tutorial', 'Help', and 'What's new'.



Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS

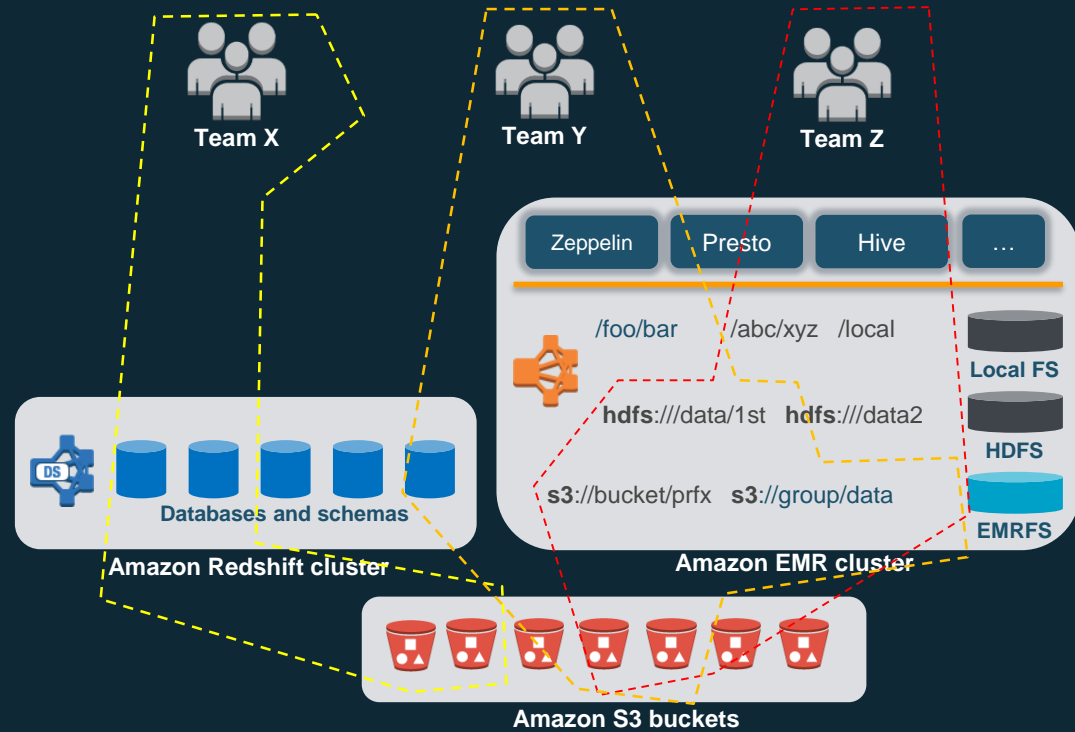
- What data do I have in the cloud?
- Where is it located?
- How is data being shared and stored?
- How can I classify data in near-real time?
- What PII/PHI is possibly exposed?
- How do I build workflow remediation for my security and compliance needs?



# The Data Lake Security Challenge

“Fine-grained” data and resource ownership

- Teams share **S3 buckets and clusters**
- Access control complex to set up and maintain
- Common in a “**shared services**” architecture



“Fine-grained”  
ownership



# Data Lake Security & Governance

**AWS Identity and Access Management (IAM)**

Default

Amazon Cognito

Amazon CloudWatch & AWS CloudTrail

AWS KMS/Encryption

AWS Directory Service

Apache Ranger for EMR (Apache Atlas in Q4-2018)

Security &  
Governance



AWS KMS



Apache Ranger

