S3 Bucket Policy Examples - Explained

# 1. Granting Permissions to Multiple Accounts with Conditions

📄 Description: Allows specific AWS accounts to upload objects with a required ACL (public-read).

✅ Use Case: Shared public uploads (e.g., images).

{  
 "Version": "2012-10-17",  
 "Statement": [{  
 "Sid": "AddCannedAcl",  
 "Effect": "Allow",  
 "Principal": {  
 "AWS": [  
 "arn:aws:iam::111122223333:root",  
 "arn:aws:iam::444455556666:root"  
 ]  
 },  
 "Action": ["s3:PutObject", "s3:PutObjectAcl"],  
 "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/\*",  
 "Condition": {  
 "StringEquals": {  
 "s3:x-amz-acl": ["public-read"]  
 }  
 }  
 }]  
}

# 2. Granting Read-Only Access to Anonymous Users

📄 Description: Enables public read-only access to all objects in the bucket.

✅ Use Case: Hosting static websites.

{  
 "Version": "2012-10-17",  
 "Statement": [{  
 "Sid": "PublicRead",  
 "Effect": "Allow",  
 "Principal": "\*",  
 "Action": ["s3:GetObject", "s3:GetObjectVersion"],  
 "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/\*"  
 }]  
}

# 3. Limiting Access to Specific IP Addresses

📄 Description: Denies all access unless the request originates from a specific IP range.

✅ Use Case: Allow access only from corporate IPs.

{  
 "Version": "2012-10-17",  
 "Statement": [{  
 "Sid": "IPAllow",  
 "Effect": "Deny",  
 "Principal": "\*",  
 "Action": "s3:\*",  
 "Resource": [  
 "arn:aws:s3:::DOC-EXAMPLE-BUCKET",  
 "arn:aws:s3:::DOC-EXAMPLE-BUCKET/\*"  
 ],  
 "Condition": {  
 "NotIpAddress": {  
 "aws:SourceIp": "54.240.143.0/24"  
 }  
 }  
 }]  
}

# 4. Allowing Both IPv4 and IPv6 Addresses

📄 Description: Allows access from both IPv4 and IPv6 ranges while denying certain subranges.

✅ Use Case: Use in dual-stack environments.

{  
 "Version": "2012-10-17",  
 "Statement": [{  
 "Sid": "AllowIPmix",  
 "Effect": "Allow",  
 "Principal": "\*",  
 "Action": "s3:\*",  
 "Resource": [  
 "arn:aws:s3:::DOC-EXAMPLE-BUCKET",  
 "arn:aws:s3:::DOC-EXAMPLE-BUCKET/\*"  
 ],  
 "Condition": {  
 "IpAddress": {  
 "aws:SourceIp": [  
 "54.240.143.0/24",  
 "2001:DB8:1234:5678::/64"  
 ]  
 },  
 "NotIpAddress": {  
 "aws:SourceIp": [  
 "54.240.143.128/30",  
 "2001:DB8:1234:5678:ABCD::/80"  
 ]  
 }  
 }  
 }]  
}

# 5. Restricting Access by HTTP Referer (Website)

📄 Description: Allows access only when the request includes a specific HTTP referer header.

✅ Use Case: Serve assets only from your own domain.

{  
 "Version": "2012-10-17",  
 "Statement": [{  
 "Sid": "AllowFromWebsite",  
 "Effect": "Allow",  
 "Principal": "\*",  
 "Action": ["s3:GetObject", "s3:GetObjectVersion"],  
 "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/\*",  
 "Condition": {  
 "StringLike": {  
 "aws:Referer": [  
 "http://www.example.com/\*",  
 "http://example.com/\*"  
 ]  
 }  
 }  
 }]  
}

# 6. Granting Permission to Amazon CloudFront OAI

📄 Description: Grants a CloudFront Origin Access Identity permission to read objects.

✅ Use Case: Secure content delivery via CloudFront.

{  
 "Version": "2012-10-17",  
 "Statement": [{  
 "Sid": "CloudFrontAccess",  
 "Effect": "Allow",  
 "Principal": {  
 "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity EH1HDMB1FH2TC"  
 },  
 "Action": "s3:GetObject",  
 "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/\*"  
 }]  
}

# 7. Adding a Bucket Policy to Require MFA

📄 Description: Denies access to sensitive folders unless MFA was used during authentication.

✅ Use Case: Protect sensitive data like tax documents.

{  
 "Version": "2012-10-17",  
 "Statement": [{  
 "Sid": "DenyWithoutMFA",  
 "Effect": "Deny",  
 "Principal": "\*",  
 "Action": "s3:\*",  
 "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/taxdocuments/\*",  
 "Condition": {  
 "Null": {  
 "aws:MultiFactorAuthAge": true  
 }  
 }  
 }]  
}

# 8. Cross-Account Upload with Bucket-Owner Control

📄 Description: Allows another account to upload if the object ACL grants full control to the bucket owner.

✅ Use Case: Partner uploads where you retain full control.

{  
 "Version": "2012-10-17",  
 "Statement": [{  
 "Sid": "CrossAccountUploadControl",  
 "Effect": "Allow",  
 "Principal": {  
 "AWS": "123456789012"  
 },  
 "Action": "s3:PutObject",  
 "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/\*",  
 "Condition": {  
 "StringEquals": {  
 "s3:x-amz-acl": "bucket-owner-full-control"  
 }  
 }  
 }]  
}

# 9. Permissions for Amazon S3 Inventory and Analytics

📄 Description: Grants S3 permission to write inventory and analytics export data to a destination bucket.

✅ Use Case: Store exported reports for analysis.

{  
 "Version": "2012-10-17",  
 "Statement": [{  
 "Sid": "InventoryExport",  
 "Effect": "Allow",  
 "Principal": {  
 "Service": "s3.amazonaws.com"  
 },  
 "Action": "s3:PutObject",  
 "Resource": "arn:aws:s3:::destinationbucket/\*",  
 "Condition": {  
 "ArnLike": {  
 "aws:SourceArn": "arn:aws:s3:::sourcebucket"  
 },  
 "StringEquals": {  
 "aws:SourceAccount": "123456789012",  
 "s3:x-amz-acl": "bucket-owner-full-control"  
 }  
 }  
 }]  
}

# 10. Permissions for Amazon S3 Storage Lens

📄 Description: Allows Storage Lens to export metrics to a bucket.

✅ Use Case: Storage insights and optimization.

{  
 "Version": "2012-10-17",  
 "Statement": [{  
 "Sid": "S3StorageLensExport",  
 "Effect": "Allow",  
 "Principal": {  
 "Service": "storage-lens.s3.amazonaws.com"  
 },  
 "Action": "s3:PutObject",  
 "Resource": "arn:aws:s3:::destination-bucket/destination-prefix/StorageLens/111122223333/\*",  
 "Condition": {  
 "StringEquals": {  
 "aws:SourceAccount": "111122223333",  
 "aws:SourceArn": "arn:aws:s3:your-region:111122223333:storage-lens/your-dashboard-configuration-id",  
 "s3:x-amz-acl": "bucket-owner-full-control"  
 }  
 }  
 }]  
}