Cyscale

aws

AWS Cloud Security Cheat Sheet

Enhance your cloud security using these essential commands to safeguard your storage resources, implement logging and set IAM policies! Using this cheatsheet, you can secure your AWS environment in no time.

Passwords policy – IAM

Set IAM password policy expiry date within 90 days or less

```
aws iam update-account-password-policy --max-password-age 90
```

Ensure IAM password policy prevents password reuse (24 times)

```
aws iam update-account-password-policy --password-reuse-prevention 24
```

Storage

Enable MFA Delete on S3 buckets

```
aws s3api put-bucket-versioning --profile <profile> --bucket <bucketName> --versioning-configuration Status=Enabled,MFADelete=Enabled --mfa "arn:aws:iam::<accountNumber>:mfa/root-account-mfa-device <MFACode>"
```

Enable rotation for customer created CMKs

```
aws kms enable-key-rotation --key-id <kmsKeyID>
```

Enable EBS encryption by default

```
aws --region <region> ec2 enable-ebs-encryption-by-default
```

Ensure that S3 Buckets are configured with 'Block public access'

```
aws s3api put-public-access-block --bucket <bucketName> --public-access-block-configuration "BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolicy=true,RestrictPublicBuckets=true"
```

Logging

Enable CloudTrail in all regions

```
aws cloudtrail create-trail --name <trailName> --s3-bucket-name <bucketForCloudtrail> --is-multi-region-trail
```

Enable CloudTrail log file validation

```
aws cloudtrail update-trail --name <trailName> --enable-log-file-validation
```

Ensure CloudTrail trails are integrated with CloudWatch Logs

```
aws cloudtrail update-trail --name <trailName> --cloud-watch-logs-log-group-arn <cloudtrailLogGroupArn> --cloud-watch-logs-role-arn <cloudtrailCloudwatchLogsRoleArn>
```

Enable IAM Access analyzer for all regions

```
aws accessanalyzer create-analyzer --analyzer-name <analyzerName> --type <value>
```

Ensure that Object-level logging for read events is enabled for S3 bucket

```
aws cloudtrail put-event-selectors --region <regionName> --trail-name <trailName> --event-selectors '[{ "ReadWriteType": "ReadOnly", "IncludeManagementEvents":true, "DataResources": [{ "Type": "AWS::S3::Object", "Values": ["arn:aws:s3:::<bucketName>/"] }] }]'
```

Ensure that Object-level logging for write events is enabled for S3 bucket

```
aws cloudtrail put-event-selectors --region <region-name> --trail-name <trailName> --event-selectors '[{ "ReadWriteType": "WriteOnly", "IncludeManagementEvents":true, "DataResources": [{ "Type": "AWS::S3::Object", "Values": ["arn:aws:s3:::<bucketName>/"] }] }]'
```

You can find these commands, and more, in Cyscale. The Cyscale Platform is a powerful cloud security solution that automates cloud misconfiguration checks, strengthens cloud security, and simplifies compliance tasks. By leveraging advanced contextual analysis and providing actionable insights, the platform empowers organizations to confidently embrace the cloud while ensuring a robust security posture. Streamline your cloud security management and gain peace of mind with Cyscale.