### acm: certificates_expiry

Are certificates expiring soon?

Expired certificates can make services inaccessible for your customers.

Recommended to enable AutoRenew option or renew manually before certificates expiry

| Region | Certificate | Message | Action |
|---|---|---|---|
| us-east-1 | somecompany.co \| ce79be85-8f98-4809-9632-f5500fbc7bc6 | Certicate is valid for more than 3 months | All good |
| us-east-1 | somecompany.com \| ce79be85-8f98-4809-9632-f5500fbc7bc6 | Certicate is valid for more than 3 months | All good |
| us-east-1 | somecompany.com \| ce79be85-8f98-4809-9632-f5500fbc7bc6 | Certicate is valid for more than 3 months | All good |
| us-east-1 | somecompany.com \| ce79be85-8f98-4809-9632-f5500fbc7bc6 | Certicate is valid for more than 3 months | All good |

### ebs: volumes_encrypted_at_rest

Are EBS volumes encrypted at rest?

Data at rest should always be encrypted

Recommended to enable encryption for EBS volumes

| Region | Volume | Message | Action |
|---|---|---|---|
| us-east-1 | Unassigned \| vol-1234567890abcd | Encryption not enabled | Enable encryption at rest |

### ec2: security_groups_open_to_world

Are there any security groups open to world?

Security group open to world posses serious security threat so we need to allow only intended parties to access

Recommended to configure security groups as tight as needed

| Region | SecurityGroup | Message | Action |
|---|---|---|---|
| us-east-1 | somecompany-migration \| sg-12345acbde | Security group is restricted to few IP ranges | All good |
| us-east-1 | launch-wizard-1 \| sg-12345acbde | Security group is open to entire world | Remove rule containing IP range: 0.0.0.0/0. |

### ec2: security_groups_wide_port_range

<table>
<tr><td colspan="4">Are there any security groups with wide range of ports?</td></tr>
<tr><td colspan="4">Security group should not expose wide range of port as it will be valnerable for port scan attacks</td></tr>
<tr><td colspan="4">Recommended to expose only port used by application</td></tr>
<tr><th>Region</th><th>SecurityGroup</th><th>Message</th><th>Action</th></tr>
<tr><td>us-east-1</td><td>somecompany-migration | sg-12345acbde</td><td>Exposes only specific ports</td><td>All good</td></tr>
<tr><td>us-east-1</td><td>launch-wizard-1 | sg-12345acbde</td><td>Exposes only specific ports</td><td>All good</td></tr>
</table>

### iam: admin_count

<table>
<tr><td colspan="3">Are there too many admins for the account?</td></tr>
<tr><td colspan="3">It is hard to manage security goals when there too many admins as chances of mistakes increases</td></tr>
<tr><td colspan="3">Recommended to have 2-3 admins per account</td></tr>
<tr><th>AdminUsers</th><th>Message</th><th>Action</th></tr>
<tr><td>user, user, user_somecompany</td><td>Account has 3 admins</td><td>All good</td></tr>
</table>

### iam: password_policy

<table>
<tr><td colspan="3">Is account password policy following best practices?</td></tr>
<tr><td colspan="3">It is important to have secure password policy as leaked or weak passwords can give direct access to attackers</td></tr>
<tr><td colspan="3">Recommended to have secure password policy</td></tr>
<tr><th>Option</th><th>Message</th><th>Action</th></tr>
<tr><td>Minimum Password Length</td><td>This has a recommended value</td><td>All good</td></tr>
<tr><td>Require Symbols</td><td>Already Enabled</td><td>All good</td></tr>
<tr><td>Require Numbers</td><td>Already Enabled</td><td>All good</td></tr>
<tr><td>Require Uppercase Characters</td><td>Already Enabled</td><td>All good</td></tr>
<tr><td>Require Lowercase Characters</td><td>Already Enabled</td><td>All good</td></tr>
<tr><td>Expire Passwords</td><td>Already Enabled</td><td>All good</td></tr>
<tr><td>Max Password Age</td><td>This has a recommended value</td><td>All good</td></tr>
<tr><td>Password Reuse Prevention</td><td>This has a recommended value</td><td>All good</td></tr>
<tr><td>Hard Expiry</td><td>This has a recommended value</td><td>All good</td></tr>
</table>

### iam: root_user_access_keys_active

| | | |
|---|---|---|
| Are there any root user access keys active? | | |
| Root user access keys are unrestrictable hence shouldn't be used as damage will be determental if they gets leaked | | |
| Recommended to delete and never user root user access keys | | |
| **User** | **Message** | **Action** |
| <root_account> | Root user access keys are not active | All good |

### iam: cross_accounts_without_external_id

| | | |
|---|---|---|
| Are there accounts without ExternalId? | | |
| It is important to associate ExternalId for cross account role access | | |
| Recommended to use ExternalId for third party accounts | | |
| **Roles** | **Message** | **Action** |
| somecompanyCMS_lambda_function | Account undefined does not have ExternalId | Add an ExternalId |
| somecompanyCMS_StreamLogsToES | Account undefined does not have ExternalId | Add an ExternalId |
| somecompanyMigration | Account 393618672836 has ExternalId | All good |
| somecompanyWebsite_lambda_function | Account undefined does not have ExternalId | Add an ExternalId |
| AWSServiceRoleForAmazonElasticsearchService | Account undefined does not have ExternalId | Add an ExternalId |
| AWSServiceRoleForLambdaReplicator | Account undefined does not have ExternalId | Add an ExternalId |
| AWS_Events_Invoke_Step_Functions_1687295453 | Account undefined does not have ExternalId | Add an ExternalId |
| basic-lambda-role-only-for-testing | Account undefined does not have ExternalId | Add an ExternalId |
| CloudwatchLogsToS3Exporter | Account undefined does not have ExternalId | Add an ExternalId |
| someappCloudwatchAPIGatewayRole | Account undefined does not have ExternalId | Add an ExternalId |
| someappDynamoDBAndESLambdaRole | Account undefined does not have ExternalId | Add an ExternalId |
| someappDynamoDBLambdaRole | Account undefined does not have ExternalId | Add an ExternalId |
| | | |

| | | |
|---|---|---|
| someappElasticsearchLambdaRole | Account undefined does not have ExternalId | Add an ExternalId |
| someappS3LambdRole | Account undefined does not have ExternalId | Add an ExternalId |
| CMSPreviewIdentityAuthCognitoRole | Account undefined does not have ExternalId | Add an ExternalId |
| CognitoAccessForAmazonES | Account undefined does not have ExternalId | Add an ExternalId |
| Cognito_somecompanyWebsiteProdUsersAuth_Role | Account undefined does not have ExternalId | Add an ExternalId |
| Cognito_somecompanyWebsiteProdUsersUnauth_Role | Account undefined does not have ExternalId | Add an ExternalId |
| Cognito_someappBackendteamAuth_Role | Account undefined does not have ExternalId | Add an ExternalId |
| Cognito_someappBackendteamUnauth_Role | Account undefined does not have ExternalId | Add an ExternalId |
| Cognito_CMSProdPoolAuth_Role | Account undefined does not have ExternalId | Add an ExternalId |
| Cognito_CMSProdPoolUnauth_Role | Account undefined does not have ExternalId | Add an ExternalId |
| Cognito_KibanaUserAuth_Role | Account undefined does not have ExternalId | Add an ExternalId |
| Cognito_KibanaUserUnauth_Role | Account undefined does not have ExternalId | Add an ExternalId |
| PreviewsomeappAPILambdaRole | Account undefined does not have ExternalId | Add an ExternalId |
| PreviewsomeappBrightcoveVideoUploader | Account undefined does not have ExternalId | Add an ExternalId |
| PreviewWebsiteAPILambdaRole | Account undefined does not have ExternalId | Add an ExternalId |
| Prod__somecompanyCMS_lambda_function | Account undefined does not have ExternalId | Add an ExternalId |
| StepFunctionsRole | Account undefined does not have ExternalId | Add an ExternalId |
| Website-Preview-SMS-Role | Account undefined does not have ExternalId | Add an ExternalId |
| Website-Staging-SMS-Role | Account undefined does not have ExternalId | Add an ExternalId |

| | | |
|---|---|---|
| WebsitePreviewIdentityAuthCognitoRole | Account undefined does not have ExternalId | Add an ExternalId |

### iam: users_access_keys_unused

| |
|---|
| Are there any user access keys unused? |
| It is important to delete unused or unneeded access keys as it reduces risk of misusing them |
| Recommended to delete unused user access keys regularly |

| User | Message | Action |
|---|---|---|
| user | User access key 1 is actively used | All good |
| user | User access key 1 is actively used | All good |
| user | User access key 1 is actively used | All good |
| user | User access key 1 is actively used | All good |
| user | User access key 1 is actively used | All good |
| user | User access key 1 is actively used | All good |
| user | User access key 1 is actively used | All good |
| user | User access key 1 is actively used | All good |
| user | User access key 1 is actively used | All good |

### iam: users_access_keys_old

| |
|---|
| Are user access keys are too old? |
| It is important to rotate access keys regularly as it will reduce improper use |
| Recommended to rotate user access keys regularly |

| User | Message | Action |
|---|---|---|
| user | User access key 1 is not rotated from last 180 days | Rotate user access key 1 |
| user | User access key 1 is not rotated from last 180 days | Rotate user access key 1 |
| user | User access key 1 is not rotated from last 180 days | Rotate user access key 1 |
| user | User access key 1 is not rotated from last 180 days | Rotate user access key 1 |
| user | User access key 1 is rotated within last 180 days | All good |
| user | User access key 1 is rotated within last 180 days | All good |
| user | User access key 1 is rotated within last 180 days | All good |
| user | User access key 1 is rotated within last 180 days | All good |
| user | User access key 1 is rotated within last 180 days | All good |

### iam: user_accounts_mfa_enabled

Are there any user access keys unused?

It is important to delete unused or unneeded access keys as it reduces risk of misusing them

Recommended to delete unused user access keys regularly

| User | Message | Action |
|---|---|---|
| user | User account is MFA enabled | All good |
| user | User account is not MFA enabled | Enable MFA for the user |
| user_somecompany | User account is MFA enabled | All good |
| user | User account is not MFA enabled | Enable MFA for the user |
| user | User account is MFA enabled | All good |
| user | User account is not MFA enabled | Enable MFA for the user |
| user | User account is not MFA enabled | Enable MFA for the user |
| user | User account is not MFA enabled | Enable MFA for the user |
| user_tensult | User account is MFA enabled | All good |
| user | User account is MFA enabled | All good |
| user | User account is not MFA enabled | Enable MFA for the user |
| user | User account is not MFA enabled | Enable MFA for the user |
| s3_somecompany | User account is not MFA enabled | Enable MFA for the user |
| user | User account is not MFA enabled | Enable MFA for the user |
| user-someapp | User account is MFA enabled | All good |

### trails: cloud_trails_bucket_access_logs

Are access logs enabled for buckets containing Cloud Trails?

Cloud trails contains important security information so we need to limit access to them and also enable access logs for such buckets

Recommended to enable access logs for buckets containing Cloud Trails

| Bucket | Message | Action |
|---|---|---|
| somecompany-logs | Access logs are not enabled | Enabled access logs |

### trails: cloud_trails_bucket_deletes_mfa_enabled

| | | |
|---|---|---|
| Is deleting cloud trails protected by MFA? | | |
| Cloud trails deletes should be MFA enabled so that attacker won't able to delete them | | |
| Recommended to enable MFA for deleting Cloud Trails | | |
| **Bucket** | **Message** | **Action** |
| somecompany-logs | Deletes are not MFA enabled | Enable MFADelete |

### trails: cloud_trails_enabled

| | | | |
|---|---|---|---|
| Is cloud trails enabled for account? | | | |
| Cloud trails helps understand who did what and this is utmost important when a security breach happens | | | |
| Recommended to enable cloud trails for all regions | | | |
| **Region** | **CloudTrails** | **Message** | **Action** |
| us-east-2 | someappTrails | Cloud trails are enabled | All good |
| us-east-1 | someappTrails | Cloud trails are enabled | All good |
| us-west-1 | someappTrails | Cloud trails are enabled | All good |
| us-west-2 | someappTrails | Cloud trails are enabled | All good |
| ca-central-1 | someappTrails | Cloud trails are enabled | All good |
| ap-south-1 | someappTrails | Cloud trails are enabled | All good |
| ap-northeast-2 | someappTrails | Cloud trails are enabled | All good |
| ap-southeast-1 | someappTrails | Cloud trails are enabled | All good |
| ap-southeast-2 | someappTrails | Cloud trails are enabled | All good |
| ap-northeast-1 | someappTrails | Cloud trails are enabled | All good |
| eu-central-1 | someappTrails | Cloud trails are enabled | All good |
| eu-west-1 | someappTrails | Cloud trails are enabled | All good |
| eu-west-2 | someappTrails | Cloud trails are enabled | All good |
| sa-east-1 | someappTrails | Cloud trails are enabled | All good |

### trails: cloud_trails_encryption_at_rest

Are Cloud trails encrypted at rest?

Critical data should always be encrypted at rest

Recommended to enable encryption at rest for CloudTrails

| Region | CloudTrail | Message | Action |
|---|---|---|---|
| us-east-2 | someappTrails | Encryption not enabled | Enable encryption at rest |
| us-east-1 | someappTrails | Encryption not enabled | Enable encryption at rest |
| us-west-1 | someappTrails | Encryption not enabled | Enable encryption at rest |
| us-west-2 | someappTrails | Encryption not enabled | Enable encryption at rest |
| ca-central-1 | someappTrails | Encryption not enabled | Enable encryption at rest |
| ap-south-1 | someappTrails | Encryption not enabled | Enable encryption at rest |
| ap-northeast-2 | someappTrails | Encryption not enabled | Enable encryption at rest |
| ap-southeast-1 | someappTrails | Encryption not enabled | Enable encryption at rest |
| ap-southeast-2 | someappTrails | Encryption not enabled | Enable encryption at rest |
| ap-northeast-1 | someappTrails | Encryption not enabled | Enable encryption at rest |
| eu-central-1 | someappTrails | Encryption not enabled | Enable encryption at rest |
| eu-west-1 | someappTrails | Encryption not enabled | Enable encryption at rest |
| eu-west-2 | someappTrails | Encryption not enabled | Enable encryption at rest |
| sa-east-1 | someappTrails | Encryption not enabled | Enable encryption at rest |

### trails: cloud_trails_global_service_events

Are global service events included in CloudTrails?

We need to enable this option to keep track of events from global service like IAM

Recommended to enable IncludeGlobalServiceEvents for CloudTrails

| Region | CloudTrail | Message | Action |
|---|---|---|---|
| us-east-2 | someappTrails | Global service events are included | All good |
| us-east-1 | someappTrails | Global service events are included | All good |
| us-west-1 | someappTrails | Global service events are included | All good |
| us-west-2 | someappTrails | Global service events are included | All good |
| ca-central-1 | someappTrails | Global service events are included | All good |
| ap-south-1 | someappTrails | Global service events are included | All good |
| ap-northeast-2 | someappTrails | Global service events are included | All good |
| ap-southeast-1 | someappTrails | Global service events are included | All good |
| ap-southeast-2 | someappTrails | Global service events are included | All good |
| ap-northeast-1 | someappTrails | Global service events are included | All good |
| eu-central-1 | someappTrails | Global service events are included | All good |
| eu-west-1 | someappTrails | Global service events are included | All good |
| eu-west-2 | someappTrails | Global service events are included | All good |
| sa-east-1 | someappTrails | Global service events are included | All good |

### trails: cloud_trails_log_validation

| |
|---|
| Is log file validation enabled for cloud trails? |
| Cloud trails helps understand who did what so enabling log file validation keep their integrity intact |
| Recommended to enable log file validation for all cloud trails |

| Region | CloudTrail | Message | Action |
|---|---|---|---|
| us-east-2 | someappTrails | Log validation is enabled for the cloud trail | All good |
| us-east-1 | someappTrails | Log validation is enabled for the cloud trail | All good |
| us-west-1 | someappTrails | Log validation is enabled for the cloud trail | All good |
| us-west-2 | someappTrails | Log validation is enabled for the cloud trail | All good |
| ca-central-1 | someappTrails | Log validation is enabled for the cloud trail | All good |
| ap-south-1 | someappTrails | Log validation is enabled for the cloud trail | All good |
| ap-northeast-2 | someappTrails | Log validation is enabled for the cloud trail | All good |
| ap-southeast-1 | someappTrails | Log validation is enabled for the cloud trail | All good |
| ap-southeast-2 | someappTrails | Log validation is enabled for the cloud trail | All good |
| ap-northeast-1 | someappTrails | Log validation is enabled for the cloud trail | All good |
| eu-central-1 | someappTrails | Log validation is enabled for the cloud trail | All good |
| eu-west-1 | someappTrails | Log validation is enabled for the cloud trail | All good |
| eu-west-2 | someappTrails | Log validation is enabled for the cloud trail | All good |
| sa-east-1 | someappTrails | Log validation is enabled for the cloud trail | All good |