Baseline for Amazon Web Services accounts

# Baseline for Amazon Web Services accounts

The Ministry of Justice (MoJ) has a 'lowest common denominator' for security-related promises, capabilities and configurations of MoJ Amazon Web Services (AWS) accounts.

The baseline is not a holistic list of dos and don'ts, but a *minimum* line in the sand for what 'at least' **must** be done.

## The base principle

All MoJ AWS accounts **must** utilise a series of agreed configurations to enable and support good tenancy within AWS and a suitable cyber security posture.

### Anti-solutionising

This baseline discusses outcomes not *how* the baseline will be achieved/implemented.

The MoJ Cyber Security team strongly encourage the use of the highest abstraction level of services available from AWS to achieve these goals, and minimising the amount of custom code and configuration which needs to be developed (and thereafter, maintained) to satisfy each baseline.

## Security incidents

The CyberSecurity team should be added as a security contact for all Information security incidents generated by AWS. The contact details for an AWS Account can be updated using the reference [here](https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/manage-account-payment.html#manage-account-payment-alternate-contacts).

* Full Name: Operational Security Team
* Title: Mx
* Email Address: [OperationalSecurityTeam@justice.gov.uk](mailto:OperationalSecurityTeam@justice.gov.uk)

## Baseline

### GuardDuty

Leverage AWS' commodity IDS solution to detect/protect from malicious or unauthorised behavior.

|  |  |  |
| --- | --- | --- |
| What must be in place | Monitoring | Resolution/Escalation if baseline is broken/violated |
| [GuardDuty](https://aws.amazon.com/guardduty/) is enabled on all accounts, in all regions, all of the time. | Alerts fire when GuardDuty is not enabled in a MoJ AWS account. Alerts fire for at least HIGH and above (or some version of) GuardDuty matches. | GuardDuty is automatically re-enabled. |

### CloudTrail

Leverage AWS' native activity audit platform (with adequate non-repudiation) to capture what AWS user (IAM etc) activity and changes are made within our AWS accounts

|  |  |  |
| --- | --- | --- |
| What must be in place | Monitoring | Resolution/Escalation if baseline is broken/violated |
| [CloudTrail](https://aws.amazon.com/cloudtrail/) is enabled within all accounts, all of the time. CloudTrail logs are carbon copied to an AWS account controlled by Cyber Security. | Alerts fire when CloudTrail is not enabled in an MoJ AWS account. | CloudTrail is automatically re-enabled. |

### Config

Leverage AWS' native AWS configuration activity audit platform to capture what changes are being made to AWS configurations.

|  |  |  |
| --- | --- | --- |
| What must be in place | Monitoring | Resolution/Escalation if baseline is broken/violated |
| [Config](https://aws.amazon.com/config/) is enabled within all accounts, all of the time. Config logs are carbon copied to an AWS account controlled by CyberSecurity via CloudTrail. | Alerts fire when Config is not enabled in an MoJ AWS account. | Config is automatically re-enabled. |

### Tagging

[Tag](https://aws.amazon.com/answers/account-management/aws-tagging-strategies/) all of our AWS objects, so we know they have a purpose and are intentional with defined ownership.

We have our own [infrastructure ownership/tagging standards](https://ministryofjustice.github.io/technical-guidance/documentation/standards/documenting-infrastructure-owners.html#documenting-owners-of-infrastructure).

|  |  |  |
| --- | --- | --- |
| What must be in place | Monitoring | Resolution/Escalation if baseline is broken/violated |
| All relevant AWS objects are tagged as per MoJ requirements. | Creating AWS user is notified automatically in increasing urgency when object is untagged. AWS account owner (and increasing escalation) is automatically notified when objects remained untagged. | Untagged objects are forcefully and automatically shutdown/disabled or isolated after 7 consecutive days of not being tagged. |

### Regions

Do not use non-EU AWS [regions](https://docs.aws.amazon.com/general/latest/gr/rande.html) for strategic compliance and performance reasons.

|  |  |  |
| --- | --- | --- |
| What must be in place | Monitoring | Resolution/Escalation if baseline is broken/violated |
| No AWS account can create resources outside of AWS EU regions. | Alerts fire when non-EU resources are created to both the infrastructure teams and resource creator. | Non-EU resources are automatically and forcefully shut down after 12 hours. |

### Identity and Access Management

Enforce [Identity and Access Management](https://aws.amazon.com/iam/) and Joiners, Movers and Leavers (JML) within AWS. We also need to ensure accounts that legitimately exist are well protected.

|  |  |  |
| --- | --- | --- |
| What must be in place | Monitoring | Resolution/Escalation if baseline is broken/violated |
| AWS user accounts have a defined and peer reviewed method for request/creation. Viable, authoritative and 'single source of truth' documentation exists to describe each AWS account and who should and should not have access (in terms of roles). Idle AWS user accounts are suspended. MFA is required, always, enforced by policy. Root user account usage is considered abnormal. Passphrase and/or MFA seed cycled on every AWS root account use. | AWS group account owners are alerted when new AWS accounts are created. Idle (30 or more consecutive days of non-activity) AWS user accounts issue suspension notices to AWS group account owners and target users. Where an account does not have MFA, the user and AWS group account owners are notified after 7 consecutive days. Any login or use of an AWS root account issues login alerts to the AWS group account owners. | Idle AWS user accounts are automatically suspended past threshold. Non-MFA AWS user accounts are automatically suspended past threshold. Alerts fire when an AWS root user account is used but the credentials are not updated within 7 days of utilisation. |

For more information on MFA, see the [Multi-Factor Authentication guidance](multi-factor-authentication-mfa-guide.html).

### Encryption

Leverage native AWS configuration options to make reasonable efforts to protect data.

|  |  |  |
| --- | --- | --- |
| What must be in place | Monitoring | Resolution/Escalation if baseline is broken/violated |
| All AWS objects supporting encryption must have it enabled. | S3 buckets without suitable SSE-\* encryption enabled are alerted to resource creator and account owner. | After 7 days of non-action, alerts are sent to central hosting infrastructure teams, Head of Hosting and MoJ Cyber Security. |

### 'World' Access

Ensure that public access to AWS data storage and compute is intentional, to avoid the 'leaky bucket' problem, and to aid attack surface minimisation.

|  |  |  |
| --- | --- | --- |
| What must be in place | Monitoring | Resolution/Escalation if baseline is broken/violated |
| All AWS S3 objects should be not world (public) readable unless specifically intended to do so. | S3 objects are programmatically reviewed (including 'open' ones) against the source infrastructure-as-code, if there is a mismatch the resource creator and AWS account owner notified. | After 7 days of non-action, alerts are sent to central hosting infrastructure teams, Head of Hosting and MoJ Cyber Security. After 7 days, the S3 object permissions are forcefully and automatically changed to remove 'world' access. |
| Compute (for example, EC2 or ECS) instances should not be directly accessible from public networks unless through specific intentional design and should be behind CloudFront and/or applicable load balancing (preferring AWS LB technology). It must be truly exceptional for common service ports (for example, TCP80 or TCP443) to be served directly from compute resources. | Compute instances are programmatically reviewed to ensure they are not internet-accessible unless explicitly designed and documented to be so. If there is a mismatch the resource creator and AWS account owner notified. | After 7 days of non-action, alerts are sent to central hosting infrastructure teams, Head of Hosting and MoJ Cyber Security. After 7 days, the relevant security groups are forcefully and automatically changed to remove 'world' access. |

### SecurityHub

[SecurityHub](https://aws.amazon.com/security-hub/) enabled where possible.

Over time we will be able to leverage this more, but in the immediate future this will enable us to do CIS-based scans.

|  |  |  |
| --- | --- | --- |
| What must be in place | Monitoring | Resolution/Escalation if baseline is broken/violated |
| SecurityHub is enabled on all accounts, in all regions, all of the time. | Alerts fire when SecurityHub is not enabled in a MoJ AWS account. | SecurityHub is automatically re-enabled. |

## Implementation

Various [AWS account baseline templates](https://github.com/ministryofjustice/cloud-platform-infrastructure/tree/main/cloudformation/aws-account-baseline-templates) have been developed and published for use.