Intcomex Operating Procedures

AWS Objective

This document aims to establish the standardized technical procedures used by Intcomex consulting team for the management and operation of environments on AWS. The procedures detailed here guarantee continuity, traceability, security and consistency in the administration of customer services and resources, ensuring compliance with good practices and operational requirements.

Scope

This document applies to all Intcomex -managed deployments and technical operations on customer infrastructure on AWS. It includes procedures related to:

- KMS Key Management
- Patching
- Restores from AWS Backup
- IAM Audits
- Public endpoint management
- Infrastructure Change Management
- Other critical processes for the stable and secure operation of cloud environments

The scope covers production, staging and development environments, both in automated and manual operations, and is aligned with the security and operation policies defined in the general SOP.

Audience

This document is aimed at:

- Cloud consultants assigned to customer accounts
- Second and Third Level Technical Support Staff
- Operations and infrastructure managers

- Compliance and security officers
- Internal collaborators responsible for operational tasks related to AWS environments

It can also be used as a reference by the client's staff or auditors, when it is necessary to validate the procedures applied to their environments.

Contents

1. **KMS Key Rotation Procedure (Customer Managed Keys)** 4

2. **Patching and Rollback Procedure** 4

3. **Restore procedure from AWS Backup** 5

4. **IAM Audit and Access Review Procedure** 5

5. **Procedure for Public Endpoint Documentation**...6

6. **Incident Response Procedure** 7

7. **Infrastructure Change Management Procedure** 7

8. **Procedure for the Review and Attention of Operational Alerts** 9

1. KMS Key Rotation Procedure (Customer Managed Keys)

Objective: Establish a clear and repeatable process for manually rotating customer- managed KMS keys on AWS.

Recommended Frequency: Yearly

Responsible: Consultant assigned to the client's account
Steps:

1. Log in to the AWS KMS console
2. Identify the active CMK Customer Managed
3. Validate that auto-rotation is not enabled
4. Create a new key with the same policies and tags
5. Assign the new key to resources that use the old key (EBS, RDS, S3, etc.)
6. Verify the operation of the services with the new key
7. Progressively deactivate the old key

Why it's done: This reduces the risk of persistent key compromise and is a security best practice aligned with compliance standards.

2. Patching and Rollback Procedure

Objective: To ensure that the application of patches to the operating system and software is carried out in a controlled manner, with the possibility of reversal.

Maintenance window: 5-6 hours (depending on customer)

Steps:

1. Notify the customer 48 hours in advance
2. Generate a full backup of the server before patching
3. Apply the patch in a sandbox (if available)
4. Apply in Production
5. Verify services and functionalities
6. In case of failure, restore from backup

Why it's done: It allows systems to be kept up to date without compromising operational continuity.

3. Restore procedure from AWS Backup

Objective: To document the process of restoring a workload from AWS Backup to incidents or recovery.

Steps:

1. Access AWS Backup
2. Select the resource to restore
3. Choosing the right restore point
4. Validate Restore Target Configuration
5. Run the restore
6. Validate connectivity, services, DNS, and full operation

Why it's done: Ensures that a critical resource can be quickly recovered while minimizing data loss and downtime.

4. IAM Audit and Access Review Procedure

Objective: To periodically verify compliance with the principle of least privilege in IAM users.

Frequency: Quarterly

Steps:

1. List all active IAM users
2. Check recent usage for each account
3. Validate assigned permissions
4. Compare with the user's current role and access requirements
5. Remove unused or unnecessary access
6. Documenting Changes Made

Why it's done: Mitigates the risk of excessive access, orphaned users, or insecure configurations.

5. Procedure for Public Endpoint Documentation

Objective: Maintain an up-to-date inventory of all public endpoints exposed by customers.

Steps:

1. Access the customer environment
2. Identify publicly accessible resources (CloudFront, ALB, public IPs, domains)
3. Update the endpoint spreadsheet with:
   - URL/IP
   - Associated resource
   - Date of creation
   - Current status
4. Validate TLS encryption and valid certificates
5. Confirm that they are protected with WAF if applicable

Why it's done: Maintaining control of the surface exposed to the internet is key to proactive security.

6. Incident Response Procedure

Objective: Guide the response to security or availability incidents reported by the customer or detected via alerts.

Steps:

1. Receive alerts via email or monitoring system
2. Assigned consultant investigates the cause
3. Check logs in CloudTrail, Inspector, CloudWatch
4. Apply temporary mitigation (e.g., block IP, stop instances)
5. Notifies the customer of the finding and measures applied
6. Document the incident

Why it's done: It facilitates a quick and orderly response, minimizing the impact and maintaining traceability.

7. Infrastructure Change Management Procedure

Objective:
Define the structured process for requesting, evaluating, approving, implementing, and documenting changes to the AWS cloud infrastructure, ensuring traceability, risk control, and proper communication between stakeholders.

Procedure:

1. Change Request
   - The change must be requested using the *Change Request* (RFC) template, either by the client or the consulting team.
   - It should include: description, reason for the change, estimated impact, tentative window, responsible, estimated rollback, and affected services.
2. Change Assessment
   - The change is evaluated by the assigned consultant and/or technical lead to validate:

        - Technical feasibility.
        - Associated risks.
        - Adequate window.
        - Existence of prior endorsements and evidence if applicable.

3. Approval
    - Minor changes may be approved by the responsible consultant.
    - Major changes require review by the client or operations leader (depending on the scope of the project).
4. Planning
    - The date and time of execution is defined.
    - Communication to the client is coordinated, including the scope, possible impacts and estimated execution and validation times.
5. Change Execution
    - The change is implemented as planned.
    - Operational results are validated through operation, access, and performance tests.
    - The result of the execution is documented.
6. Rollback (if applicable)
    - In the event of a failure, the previously defined rollback plan is executed, using backups, snapshots or other restoration mechanisms.
7. Closing of the Change
    - The ICR – Implemented Change Log *template is completed*.
    - The result is communicated to the customer.
    - The architecture documentation is updated if the change was structural.

Tools used:

- Email
- Shared technical documentation

8. Procedure for the Review and Attention of Operational Alerts

Objective:
To establish the process by which the alerts generated by the AWS environment are managed, guaranteeing their timely attention and clear communication with the customer.

Procedure:

1. Alert generation
    - Alerts are generated by services such as:
        - **CloudWatch** (metrics and logs).
        - **X-Ray** (application traceability).
        - **Amazon Inspector** (security).
        - **CloudTrail / AWS Config** (changes and compliance).
2. Reception
    - Alerts are delivered via email to the consultant responsible for the account.
    - Some alerts may also be notified by the customer directly.
3. Validation
    - The assigned consultant accesses the affected environment.
    - Review usage graphs (CPU, memory, disk, network), events, and logs.
    - Determine if it is a one-off spike, a false positive, or an incident to escalate.
4. Classification
    - Criticality is determined:
        - Informative.
        - Warning.
        - Critical.
5. Action
    - Corrective actions are executed as needed:
        - Service restart.

        - Scaling.
        - Resource adjustment.
        - Contact AWS Support if applicable.

6. Registration
    - Action taken by email is documented.
    - In the event of a critical incident, a final report is issued.
7. Tracking
    - If the incident requires subsequent review, it is scheduled for analysis or monthly review.

Proactive Review Frequency:

- Every one or two months, depending on the stability of the environment.

Tools used:

- CloudWatch, X-Ray, CloudTrail, Config
- Email
- AWS Console and Internal Documentation