Standard Operating Procedure – Intcomex

This document aims to provide the policies and procedures that Intcomex follows for the secure, standardized, and reliable management of customer accounts on Amazon Web Services (AWS). Its content reflects internal practices and recommendations applied in environments under our management. This SOP seeks to align the operation to good cloud security practices, facilitate audits, and ensure consistency in service delivery.

Scope

This document applies to all customer accounts managed by Intcomex within the AWS platform, where the team of consultants has full or partial operational control. It covers operations ranging from user creation and management, access control, security monitoring, service deployment, to backup and disaster recovery. Also included are the best practices for customers who have shared control, with the goal of standardizing security and operational efficiency across all the environments under our management.

Target Audience

This SOP is aimed at:

- Intcomex technical consultants assigned to customer accounts.
- Support and monitor team members.
- Management personnel involved in overseeing cloud operations.
- Customers who need to understand the policies and practices implemented by Intcomex.
- Auditors or entities that require operational or compliance evidence related to AWS management.

Contents

1. Root Account Management and Programmatic Access

The root account is the most privileged identity in AWS, so restricting its use and programmatic access is critical to avoid greater risks. We encourage the root account to be used only in exceptional cases and with enhanced security.

Procedures and validations:

- Disable programmatic access to the root account when you have control over it, thus minimizing the risk of key exposure that could give full access to the account.
- Create service users with access key and appropriate roles for the necessary operations, applying the principle of least privilege to limit access.
- Do not use the root account for daily activities and do not document its use to reduce the possibility of errors or unauthorized access with high privileges.
- Implement MFA in the root account managed through 1Password, under the control of the assigned consultant, adding an extra layer of protection against improper access.
- Link the root account to a corporate email from the person in charge to ensure that critical alerts and notifications are received.

2. CloudTrail Enablement and Monitoring

CloudTrail is the foundational tool for monitoring and auditing activity on AWS. We ensure that it is enabled for all accounts and regions, with protected logs and proper retention to respond to incidents and audits.

Procedures and validations:

- Enable CloudTrail across all accounts and regions under control to ensure full visibility into cloud events and activities.
- Store logs in CloudWatch with a minimum retention of 180 days, facilitating audits and historical reviews for incident detection.
- Implement centralized CloudWatch to consolidate logs, improving log management and analysis, especially without the use of AWS Organization.

3. IAM User Management and Access Control

Identity and access management (IAM) is key to controlling who can do what on AWS. Our approach is to create a controlled process for creating, assigning, and periodically reviewing users and permissions.

Procedures and validations:

- User creation process requested by the client, tested and executed by an assigned consultant, to maintain control and traceability in the creation of accesses.
- Assign roles and policies following the principle of least privilege, using default or customized policies depending on the scenario, to limit access to only what is strictly necessary and reduce risk.
- Password rotation every 180 days via AWS configuration, which helps reduce the window of opportunity for unauthorized access due to compromised passwords.
- Mandatory Power Verification (MFA) for all users, improving security against unauthorized access attempts.
- Quarterly review of active users and permissions to adjust access and avoid accumulation of unnecessary permissions or inactive users.

4. Deployments and change control

Controlling how changes are applied to infrastructure is vital to maintaining stability and security. We apply processes that combine manual and automated deployments, with pre- testing and rollback plans.

Procedures and validations:

- Deployments can be manual or automated using Terraform and CI/CD pipeline with GitHub Actions, facilitating controlled and reproducible deployments.
- Always test changes in quality environments before production to minimize risks of negative impact on production.
- Establish a rollback plan to revert changes if something fails, ensuring rapid recovery from failures.

5. Network Architecture and Security Rules

We segment the network into subnets to isolate functions, enforce strict security groups, and control traffic with services such as AWS WAF and CloudFront to protect exposed endpoints.

Procedures and validations:

- Separate VPCs into frontend, backend, data, and jumpbox subnets for management, limiting traffic reach and improving security by zones.
- Restriction of traffic between subnets according to the three-layer application model to prevent unnecessary access between components.
- Use AWS WAF and CloudFront to protect public applications with TLS using ACM, mitigating application-layer attacks and securing encryption.
- Limit ports and protocols only to those necessary between subnets, reducing the attack surface.
- Administrative access is only from jumpbox subnet, never from the internet, to protect management access and avoid direct exposure.
- Maintain an up-to-date inventory of public endpoints and monitor them with tools such as Route 53, controlling exposure points to detect changes or vulnerabilities.
- Use of TLS for external traffic and KMS for encryption at rest, ensuring confidentiality and integrity of data in transit and at rest.

6. KMS Key Management and Rotation

Proper management of encryption keys is critical to protecting sensitive data. We adapt the administration according to whether the keys are managed by AWS or by the customer.

Procedures and validations:

- Preferential use of AWS Managed KMS, with AWS responsibility for management, minimizing operational burden and risks for the customer.
- In case of Customer Managed KMS, the customer controls the administration with our support, providing flexibility and control when the customer requires it.

- Recommend annual manual rotation for Customer Managed keys, to maintain key security through periodic renewal.
- Apply custom policies to control key access, limiting who can use or manage keys to reduce risk.
- Document and verify rotation with reports and recommended processes (to be implemented), to maintain traceability and compliance with good practices.

7. Security Incident Detection and Response

We actively monitor with native AWS tools and respond to incidents through an assigned team, prioritizing fast communication and effective resolution.

Procedures and validations:

- Monitoring with CloudTrail, Amazon Inspector, AWS Config, and CloudWatch, enabling anomalous activity or security risks to be detected.
- Responsible for incident management is the assigned consultant, in coordination with the client, facilitating a quick and efficient response.
- Communication via email between client and consultant for incident management, maintaining clear traceability and coordination.
- No response drills or formal testing are carried out, as this is currently outside the scope of the service.
- Updating the process according to emerging scenarios, to adapt the response to new risks or experiences.

8. Patching and Updating

Keeping systems up to date is key to security. We apply planned patches, with maintenance windows and rollback plans to minimize impacts.

Procedures and validations:

- Maintenance window of 5 to 6 hours according to the customer's operating hours, to minimize interruptions during off-peak hours.
- Generate backups before applying critical updates, facilitating quick restoration in case of failures.
- Rollback plan that may include manual uninstallation of patches or backup restoration, ensuring continuity of service in the event of problems.
- Documentation of applied patches, to maintain history for auditing and analysis.

9. Backup and Recovery

We perform automated backups with proper retention and periodic restore testing to ensure availability and disaster recovery.

Procedures and validations:

- Full daily backup with a minimum of 7-day retention on AWS Backup, ensuring recovery from recent data loss.
- Responsible for verifying and managing backups: technical team client and assigned consultant, ensuring compliance and availability.
- Periodic restore tests performed at the time of deployment or according to the client, validating the effectiveness of the backups.
- Default retention policy: daily 7 days, weekly 4 weeks, monthly 1 month, annual 1 year, complying with operational and regulatory requirements.
- Procedures for urgent restoration with post-restore validation (DNS, IP, load), minimizing downtime and ensuring operational service.
- Documented disaster recovery plan according to client, facilitating coordinated response to critical events.

10. Review of alerts and audits

We use various tools for the review of alerts and audits, maintaining active and continuous control, although certain processes are outside the contractual scope.

Procedures and validations:

- Use of CloudWatch, Amazon Inspector, CloudTrail and AWS Config to monitor alerts, allowing incidents or anomalies to be detected in the infrastructure.
- The cloud consulting department is responsible for reviewing and responding to alerts, ensuring centralized and efficient management.
- Alert management is done via email, providing a clear and traceable mechanism for communication with the customer.
- The frequency of audits and logs review depends on the client or scenario, being usual every 3 or 6 months to balance resources and needs.
- No incident response tests or drills are carried out, as they are not part of the current scope of work.
- Regular audit reports and specific reports are removed from the current scope, concentrating on active alert management.

11. Infrastructure Change Management

This section describes the formal procedure for requesting, assessing, approving, implementing, and documenting infrastructure changes in managed environments. The aim is to ensure that any modifications are carried out in a controlled manner, minimizing the impact on services and ensuring the traceability of the changes made.

Procedure

- **Change Request:** Any modification to the infrastructure must be initiated by a Change Request, which must contain:
    - Detailed description of the change.
    - Justification or reason for the change.
    - Affected components (servers, services, networks, etc.).
    - Preliminary impact assessment.

- Date and time proposed for execution.
- Role responsible for change.

This step ensures traceability from the beginning, understanding of the purpose and possible scope of the change.

- **Change Assessment:** The technical team responsible should:
  - Review potential impacts to the availability, security, or performance of the environment.
  - Validate the viability of the change.
  - Assess the need for maintenance windows.
  - Define rollback plans.

This process ensures that the change has been assessed in terms of technical and business risk.

- **Change Approval:** The change must be approved by:
  - The technical manager assigned to the customer.
  - The customer (in the case of collaboratively managed environments).
  - In some cases, by an internal government team.

Ensure organizational control and informed consent prior to implementing change.

- **Communication of the Change**: Once approved, the following must be communicated:
  - To the internal teams involved.
  - To the customer, if necessary.
  - By email with the summary of the change and

execution plan. This ensures that all actors are informed before

applying for the modification.

- **Change Execution**
  - The change is made in the approved maintenance window.
  - The implementation plan is followed, and the behavior of the system is monitored.

- If something fails, the previously defined rollback plan is activated.

This step ensures that the change is executed under control, monitoring and with rapid correction mechanisms.

- **Change Validation Once the change has been applied:**
  - The affected services are validated.
  - The environment is monitored to confirm stability.
  - Relevant observations are documented.

This ensures that the change was effective and did not generate unwanted side effects.

- **Closing and Documentation At the end of the process:**
  - The change history (ICR log) is updated.
  - The final result is documented.
  - All relevant emails and reports are archived.

This ensures traceability and audit compliance in managed environments.

12. Documentation and continuous improvement

Although many processes already have defined procedures, we encourage the creation, documentation and continuous updating of them to improve quality and compliance.

Procedures and validations:

- Update procedures when new scenarios or changes arise in the technological or regulatory environment, adapting practices to reality.
- Use this documentation as a basis for internal training, onboarding of new employees, and external or internal audits.
- Promote constant communication with the client to validate and adjust procedures according to their needs and evolution.