AWS Service Approval Accelerator: Amazon SQS

Date: 2019-07-23

## 

The Service Accelerator document is meant to provide a concise presentation of information to help organizations learn specific security patterns that can be implemented as part of their service configuration. Since many security programs follow the same security domains, this format provides a simple way to share the information and expedite the approval process for AWS services. The process to create this document involves a deep dive review of how the service works through hands on experience, documentation review, and discussion with AWS service teams.

The information in the Detailed Security Configuration section is meant to answer configuration/implementation questions from an operational perspective. Organizations can use the specific guidance in this document to create codified controls that meet their specific control requirements.

Detailed Security Configuration

Overview

This section is meant to provide an opinionated approach towards the implementation security controls by security domain. Although the approaches may not be a fit for all use cases or complete for production use, they are meant to guide the audience towards current best practices and design considerations to achieve security control objectives.

**Controls and Architectures**

This table maps Security Domain to the corresponding controls and architectural best practices as documented in AWS’ public documentation, white papers, and blog posts.

| **Security Domain** | **Control & Architectural Suggestions** | **References** |
| --- | --- | --- |
| Network Isolation | As a managed service, SQS is protected by the AWS global network security procedures as described in the “Network Security” section of the [AWS Security Whitepaper](https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf) and in more detail in [compliance reports](https://aws.amazon.com/compliance/resources/) and 3rd party audit findings available to AWS customers.  As a user of AWS SQS you are not required to configure network settings for the SQS service. | [AWS Security Whitepaper](https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf) [AWS compliance reports](https://aws.amazon.com/compliance/resources/) |
| Inter-network traffic privacy | Access to SQS via the network is enabled through [published APIs](https://docs.aws.amazon.com/AWSSimpleQueueService/latest/APIReference/Welcome.html).  SQS endpoints are available both over HTTP (for legacy clients) and HTTPS [1]  For both HTTP and HTTPS requests to the service, requests must be signed by using an access key ID and a secret access key – either associated with an IAM principal or you can use the AWS Security Token Service (STS) to generate temporary security credentials that you can use to sign requests.  To ensure that data to the SQS queue is not sent or received without encryption, you must create a queue access policy per queue that denies the following for all principals:  Sample policy:  {  "Version": "2012-10-17",  "Id": "arn:aws:sqs:eu-west-1:<account num>:somequeue/SQSDefaultPolicy",  "Statement": [  {  "Sid": "Sid1524736966546",  "Effect": "Deny",  "Principal": "\*",  "Action": [  "SQS:GetQueueAttributes",  "SQS:GetQueueUrl",  "SQS:SendMessage",  "SQS:ChangeMessageVisibility",  "SQS:DeleteMessage",  "SQS:PurgeQueue",  "SQS:ReceiveMessage"  ],  "Resource": "arn:aws:sqs:eu-west-1:205477738723:qtiyapa",  "Condition": {  "StringEquals": {  "aws:SecureTransport": "false"  }  }  }  ]  } | [1] <https://docs.aws.amazon.com/general/latest/gr/rande.html#sqs_region> |
| Encryption of data at-rest | SQS currently supports data encryption at rest using Server-Side Encryption (SSE) and the AWS Key Management service in the US East and US West regions. As of April 2018, this is not supported for other regions.  In regions where SSE-KMS is not supported, you can choose to:   1. Encrypt message payloads on the client side before it is sent to the SQS service 2. Use the SQS extended client to use the S3 service and make use of SSE-KMS |  |
| Encryption of data in-transit | See inter network traffic privacy |  |
| Encryption Key Management | Encryption keys that are used when SQS with SSE is enabled are managed by the key management service (KMS). If you provide your own key material for customer managed keys (CMKs) – you are responsible for managing its lifecycle. If using the AWS-managed CMK, this is done for you automatically.  You can enable SSE for SQS when creating the queue[1] or retroactively enable it for queues that were not created with SSE support [2] | SSE SQS FAQ: <https://aws.amazon.com/sqs/faqs/#sse>  [1] <https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-create-queue-sse.html>  [2] <https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-configure-sse-existing-queue.html> |
| Isolation of physical hosts | N/A: This is an AWS managed service and AWS is responsible for implementing controls around service isolation. | [AWS Security Whitepaper](https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf) [AWS compliance reports](https://aws.amazon.com/compliance/resources/) |
| Restricting administrative access to certain individuals within the company. | All SQS API actions are controlled using the Identity and Access Management (IAM) service. By default, users do not have privileges to perform any API actions unless explicitly granted.  Actions that impact the creation, deletion of queues should be locked down to administrative users, e.g.   * CreateQueue * DeleteQueue * AddPermission * RemovePermission * TagQueue (optional – if tagging is enforced for billing etc) * UntagQueue (optional – if tagging is enforced for billing etc)   Allow end users to send messages, delete messages, and list queues.  SQS supports resource level permissions within IAM, which means that you can allow users to interact with a subset of queues within SQS – allowing for granular access control, if you are creating users that have explicit permissions to a particular set of queues. |  |
| Authentication and authorization | Amazon SQS offers access policy options broadly categorized as resource-based policies and user policies. Access policies you attach to your queues referred to as resource-based policies.  You may choose to use resource-based policies, user policies, or a combination of these to manage permissions to your Amazon SQS queues.   * Use resource-based policies (SQS Access Policies) when you require centralised control for a shared queue – e.g. if an SQS queue is provisioned in one account and principals in another account need access to it. * Use user policies to allow users to be able to invoke SQS APIs * If users require fine grained access to queues, you can further narrow down user policies to allow/deny actions on particular queues using resource-level permissions | [1] <https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-security.html> |
| Auditing of all Interactions with SQS | Amazon SQS is integrated with CloudTrail, a service that captures specific API calls made to Amazon SQS from your AWS account and delivers the log files to an Amazon S3 bucket that you specify.  The following actions are logged in cloudtrail:   * [AddPermission](http://docs.aws.amazon.com/AWSSimpleQueueService/latest/APIReference/API_AddPermission.html) * [CreateQueue](http://docs.aws.amazon.com/AWSSimpleQueueService/latest/APIReference/API_CreateQueue.html) * [DeleteQueue](http://docs.aws.amazon.com/AWSSimpleQueueService/latest/APIReference/API_DeleteQueue.html) * [PurgeQueue](http://docs.aws.amazon.com/AWSSimpleQueueService/latest/APIReference/API_PurgeQueue.html) * [RemovePermission](http://docs.aws.amazon.com/AWSSimpleQueueService/latest/APIReference/API_RemovePermission.html) * [SetQueueAttributes](http://docs.aws.amazon.com/AWSSimpleQueueService/latest/APIReference/API_SetQueueAttributes.html)   **\*\*Note that data level events (Put\*, Get\*) are not logged by Cloudtrail. If you care about these events, you will currently need to implement logging for these within your application code.**  Using the information collected by CloudTrail, you can determine what request was made to Amazon SQS, the source IP address from which the request was made, who made the request, when it was made, and so on. This information helps you to track changes made to your AWS resources and to troubleshoot operational issues. CloudTrail makes it easier to ensure compliance with internal policies and regulatory standards. For detailed information see: [**Logging Amazon SQS Actions Using AWS CloudTrail**](https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/logging-using-cloudtrail.html)   * Technical auditors will want to check for the AddPermission and RemovePermission, SetQueueAttributes actions recorded in cloudtrail to check for change in access control policies. * Where administrators of queues are separate from users of queues, it could be useful to detect CreateQueue and DetectQueue events | [AWS CloudTrail User Guide](http://docs.aws.amazon.com/awscloudtrail/latest/userguide/)  <https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-access-metrics.html>  <https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/logging-using-cloudtrail.html> |
| Logging with Encryption | [CloudTrail Logs can be encrypted](http://docs.aws.amazon.com/awscloudtrail/latest/userguide/encrypting-cloudtrail-log-files-with-aws-kms.html) using customer-managed KMS keys. Be aware that data events are not logged by cloudtrail (PutMessage, Get\*). Your application must enable custom logging for these events if needed. |  |
| Compliance Framework reference material for AWS SQS | SQS is in scope for a number of compliance programs that are listed here. Reports for some of these programs can be downloaded via AWS Artifact.  <https://aws.amazon.com/compliance/services-in-scope/> | <https://aws.amazon.com/artifact/> |
| Alerting and Incident Management | You can use CloudTrail to watch Amazon SQS and report when something is wrong:  CloudTrail events of interest that should be monitored and alerted on   * [AddPermission](http://docs.aws.amazon.com/AWSSimpleQueueService/latest/APIReference/API_AddPermission.html) * [CreateQueue](http://docs.aws.amazon.com/AWSSimpleQueueService/latest/APIReference/API_CreateQueue.html) * [DeleteQueue](http://docs.aws.amazon.com/AWSSimpleQueueService/latest/APIReference/API_DeleteQueue.html) * [PurgeQueue](http://docs.aws.amazon.com/AWSSimpleQueueService/latest/APIReference/API_PurgeQueue.html) * [RemovePermission](http://docs.aws.amazon.com/AWSSimpleQueueService/latest/APIReference/API_RemovePermission.html) * [SetQueueAttributes](http://docs.aws.amazon.com/AWSSimpleQueueService/latest/APIReference/API_SetQueueAttributes.html) |  |