AWS Config SQS Integration

v1.2

Table of Contents

[Introduction 3](#_Toc512954612)

[High Level Flow 3](#_Toc512954613)

[AWS Configuration 3](#_Toc512954614)

[ServiceNow Configuration 4](#_Toc512954615)

[Update sets 4](#_Toc512954616)

[AWS Config Integration Configuration 4](#_Toc512954617)

Introduction

For customers who have enabled IP Access Controls enabled having AWS Configuration change notification events forwarded to the instance can be a challenge due to the large ranges of IPs that must be whitelisted. In addition, they are subject to change by AWS, so diligence is required on the part of the customer to keep up with the changes.

This document outlines an alternative approach, put together by the ServiceNow ITOM Rangers, utilizing an SQS queue in AWS to receive configuration notifications, and a probe that is executed on a MID server to collect the SQS messages. This setup removes the need to whitelist any IPs.

High Level Flow

AWS first collects and forwards AWS configuration changes to an SNS Topic. From there the SNS Topic is configured to send messages to an AWS SQS queue. The ServiceNow instance executes a JavaScript probe on the MID server that collects messages from the SQS queue. The sensor for the probe then utilizes the out-of-the-box AWS Config processor to process the configuration messages.

AWS Configuration

The first step in the configuration process, is to setup an SQS queue in AWS to receive the SNS notifications. There are two queue types that can be used. The client interface for the two queue types is identical, so the choice of queues is up to the customer, and depends on their needs.

* Standard queues
  + Unlimited throughput
  + At-least once delivery – but the same message MAY be delivered multiple times
  + Best-effort ordering – it is NOT guaranteed messages will arrive in the order they are delivered from SNS
  + Available in all regions
* FIFO queue
  + Up to 3,000 messages per second utilizing batching
  + Exactly once processing – messages are guaranteed to only be delivered once
  + First In First Out delivery – messages are guaranteed to come out of the queue in the same order they go in
  + Currently only available in a limited number of AWS regions



Once the queue is setup, the next steps are nearly identical to out-of-the-box AWS Config setup. AWS Config needs to be setup to send config notifications to an SNS Topic. However, when setting up the SNS Topic, the topic should be configured to send messages to the new SQS queue instead of directly to the ServiceNow REST interface.

AWS has an option to subscribe the queue to an SNS Topic. This is the easiest process to ensure the queue is connected correctly to SNS Topic.

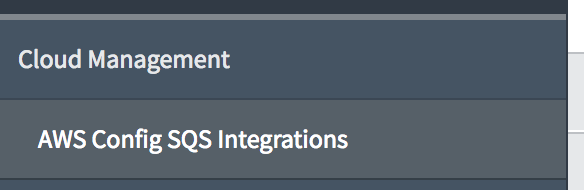
ServiceNow Configuration

Most of the configuration for the SQS integration will be done on the ServiceNow side.

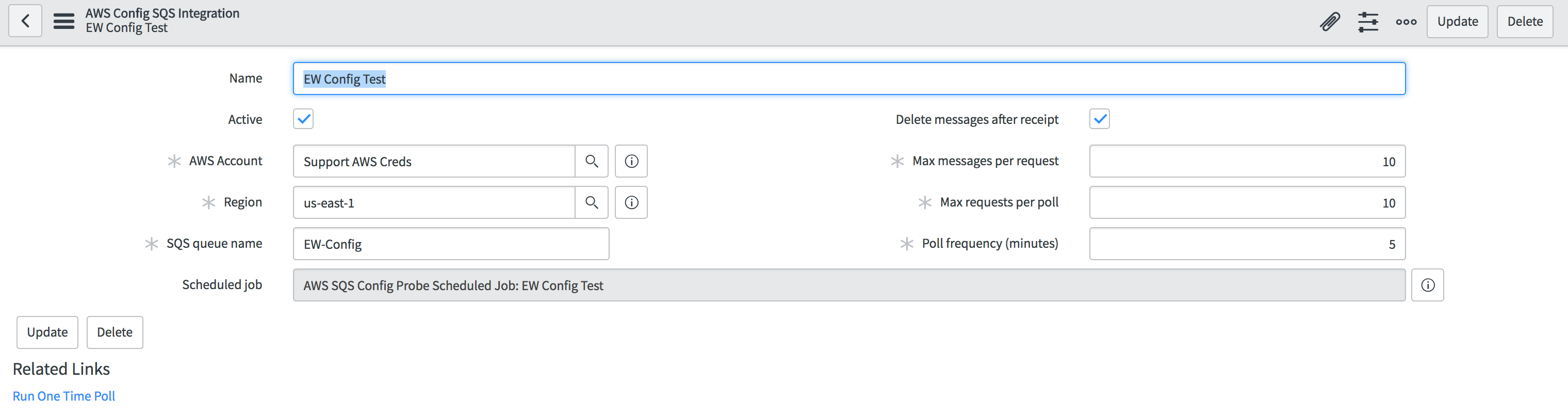
Update set

There is one update set to apply:

* AWS SQS Config Integration v1.2
  + AWS SQS Probe/Sensor
  + AWS SQS Mid Server Script include
  + AWS SQS Configuration Reference Qualifier Script Include
  + AWS SQS Probe Runner Script include
  + AWS SQS Config Integration table and business rules

AWS Config Integration Configuration

Once the update set has been applied a new menu option will be available – AWS Config SQS Integrations. Selecting this option will take you to the table of SQS Config Integration configurations.



The Configuration Page consists of several options.

* **Name**: Name of the SQS Config Integration Configuration. Updates to the name of the config cascade to the underlying scheduled job for ease of reference.
* **Active**: Marks this configuration as active or inactive – changing this flag will cascade down to the underlying scheduled job
* **AWS** **Account**: AWS Service Account that will be used when connecting the SQS queue. This must match the account under which the SQS queue is defined.
* **Region**: AWS region in which the queue is defined. This must match the region the SQS queue is defined in.
* **SQS queue name**: Name of the SQS to collect configuration events from.
* **Delete messages after receipt**: Flag to indicate if messages should be removed from the queue after reception. This is recommended unless you have other processes also relying on the queue and cleaning up the messages. Not checking this may result in the same message being processed over and over.
* **Max messages per request**: AWS supports a maximum return size of 10 messages per request. This value can be set from 1 to 10. Note that by design SQS may not return a full set of messages even if more than the maximum defined here are available.
* **Max requests per poll**: The maximum number of polls the probe will attempt against SQS before returning the results to the instance. If any poll results in no returned messages prior to the max requests per poll being reached, then polling for that cycle will also stop.
* **Poll frequency (minutes)**: Time, in minutes, between SQS polls. A poll is a series of SQS requests to the SQS queue. Each request will be for a number of messages up to the “Max messages per request” messages from the SQS queue. During a single poll requests are repeated until either the max requests per poll is reached OR the SQS queue returns an empty response. It is possible to receive an empty request from SQS even though some messages may still exist in the queue, but over the course of future polls they will be received. A FIFO queue can be used for a more definitive delivery option. For efficiency, the current setup does not offer the use of long polling but this could be added in a future update if it is deemed necessary. Long polling results in a longer wait for a response from SQS but also gives the opportunity to collect more available messages.
* **Scheduled Job**: A read-only field with a reference link to the underlying scheduled job. The scheduled job created when the initial configuration record is created and is removed when the configuration record is removed via business rules. Business rules are also used to synchronize the Active flag, Job name, and Job Frequency with the configuration entry.
* **Run One Time Poll UI Action**: This action will initiate a single poll utilizing the current configuration. The one-time poll executes regardless of the state of the Active flag. The poll will update CIs if SQS config messages are in the queue.