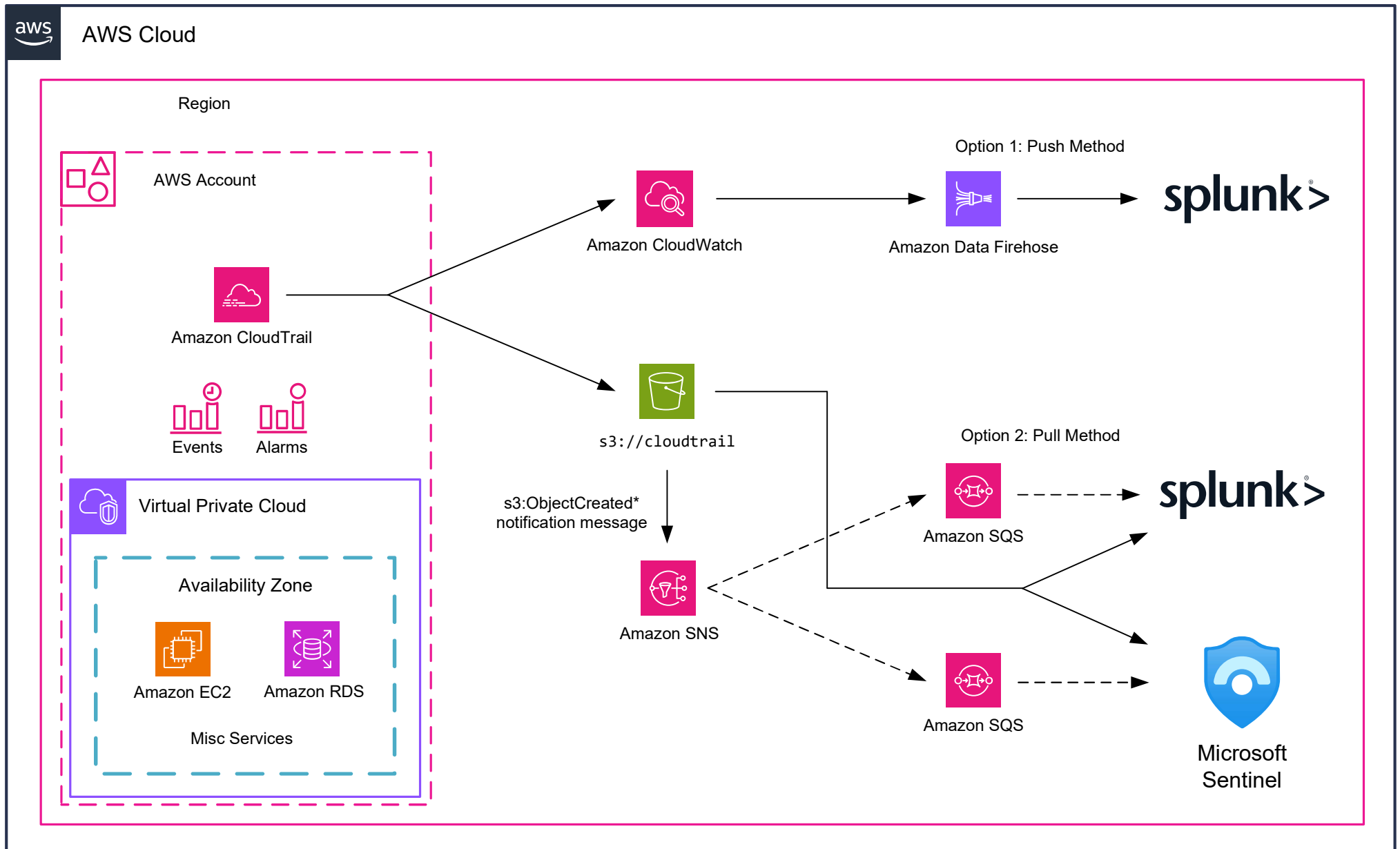
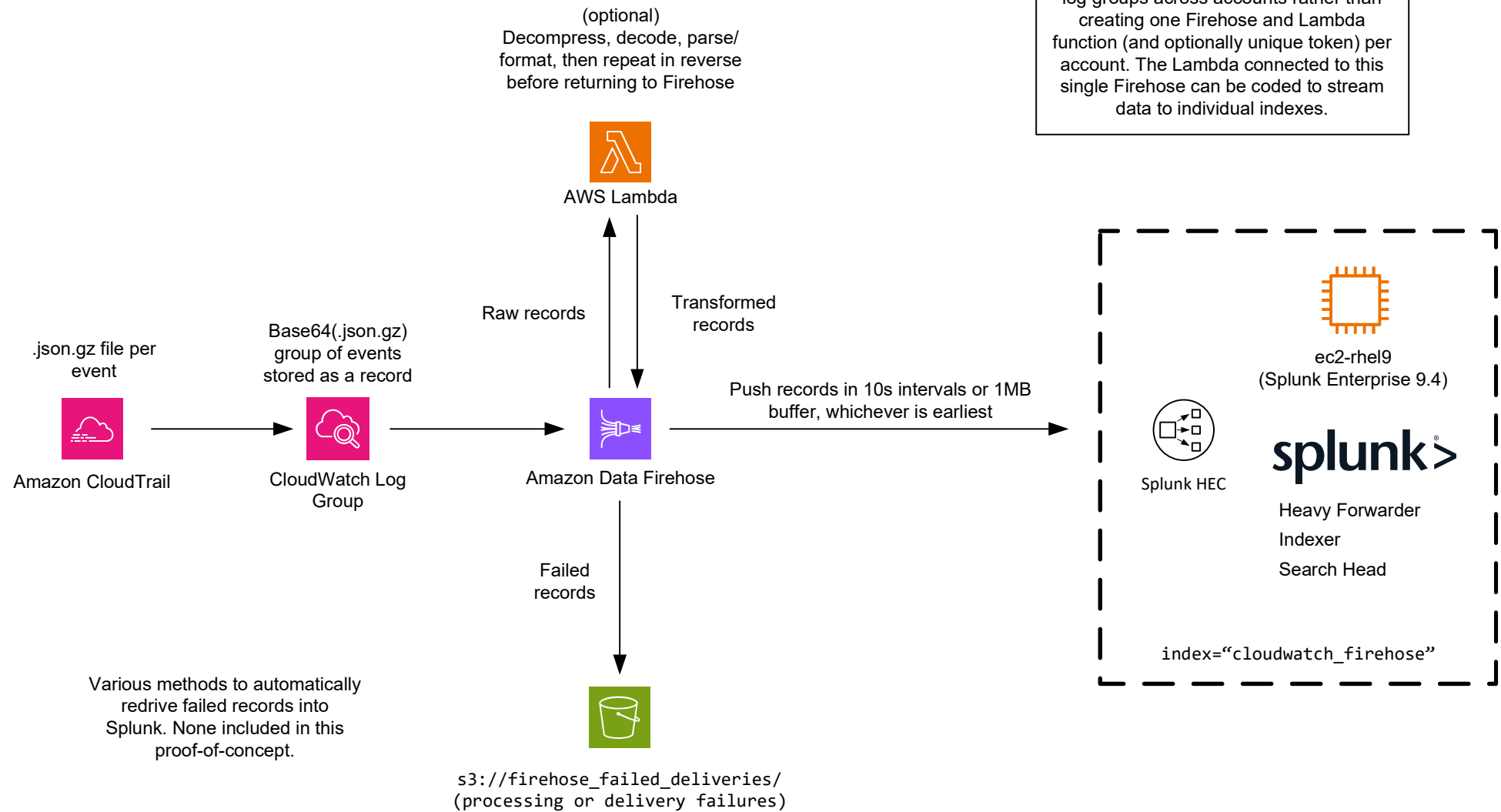


AWS CloudTrail Forwarding to Splunk Enterprise and Microsoft Sentinel Concept Diagram

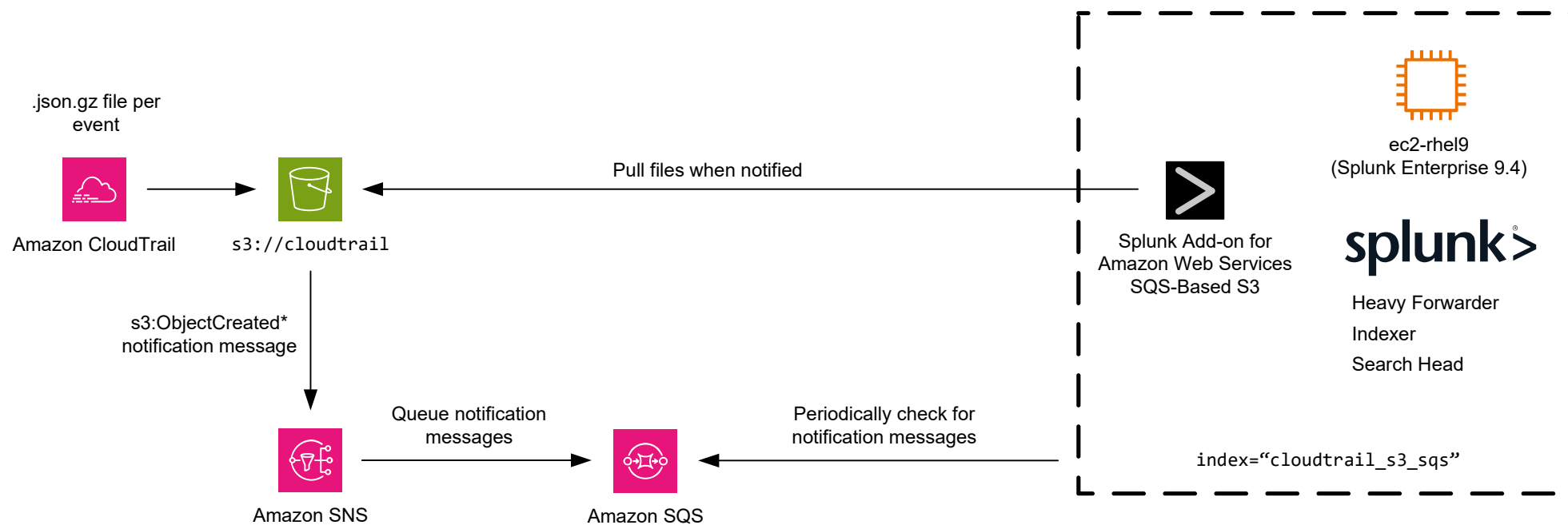


AWS CloudTrail to Splunk Enterprise via Firehose

In a multi-AWS account setup, it is an option to use one Firehose subscribed to log groups across accounts rather than creating one Firehose and Lambda function (and optionally unique token) per account. The Lambda connected to this single Firehose can be coded to stream data to individual indexes.



AWS CloudTrail to Splunk Enterprise via S3



AWS CloudTrail to Microsoft Sentinel via S3

