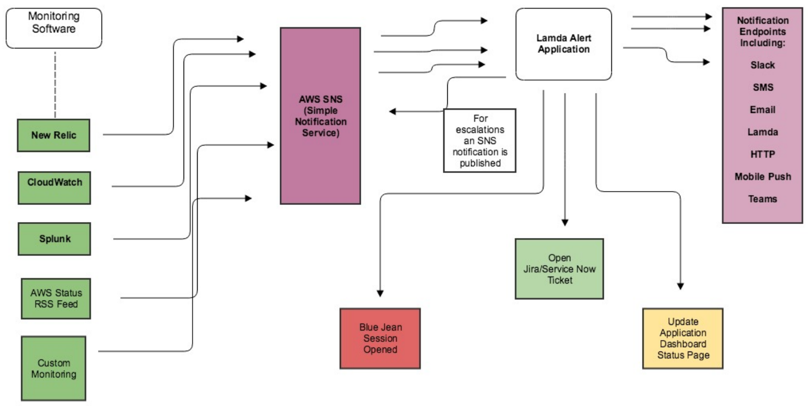
BAAT Incident Monitoring, Alerting and Resolution Strategy with SNS

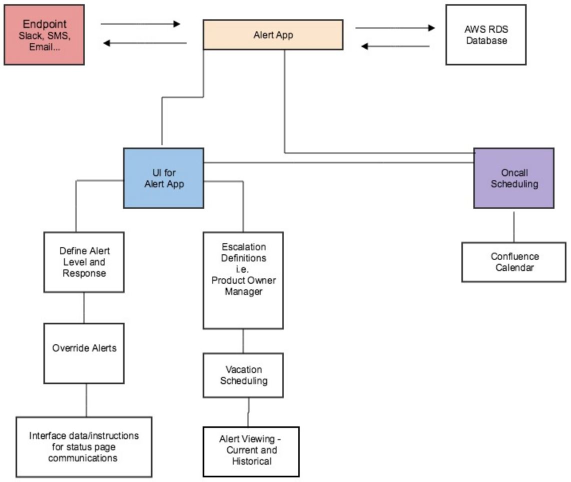
Features and Functionality	
Alerting	Alerting can come from a variety of sources including Splunk, New Relic and CloudWatch. We will be using Amazon SNS which can be feed by any monitoring package. Alerts can be sent as email, SMS, Slack post, Teams post, mobile push or http service request. Alerts can be targeted to a specific person in a schedule and then in conjunction with the escalation feature to a product manager and then to an escalation manager.
Problem Remediation	We will be creating and feeding an incident database that will allow for the possibility of both manual and automated remediation. Manually, we will send out a link to a solutions database that will make available previous similar problems with their respective solutions. This process allow for the possibility of automated remediation or self healing procedures.
Incident Escalation	Each incident will send out an alert to the person on call. If it is not answered in a preconfigured amount of time the incident will be escalated.
Automated ticket generation	When an alert is received, a Service Now or JIRA ticket will be automatically generated with a link listed in the alert text.
Blue Jeans session automatically created	An optional Blue Jeans session can be created for an incident.
Alert Muting	Alerts can optionally be muted for testing and operational purposes.
On call personal scheduling for directed alerts	We will use the Confluence calendar to schedule personnel on teams to be designated as the on call person.
Incidents to appear in a status page for effected applications	We will have an application status page for each application. This application will show details about their application including New Relic metrics and incident tickets relating to the application.
Linked to status page	Brainstorming - Confluence Status Page
Search the knowledge base	Search box that points to the back-end for lookup
Related EPICs	**BAAT-6434** - Incident Management Infrastructure for BAAT Applications Closed **BAAT-8696** - All BAAT applications and processes monitored and feed into an alerting/incident management system Closed **BAAT-8697** - Alerting System for BAAT Applications Closed **BAAT-6430** - Self-Service :: Reporting/Customer Communications on the progress and state of BAAT apps In Progress

Product	Link	Comments
SNS	https://aws.amazon.com/sns/	
RDS	https://aws.amazon.com/rds/	AWS RDS would be used as the unifying database Database structure here - Slack Alerting
lambda	https://aws.amazon.com/lambda/	A alert published to SNS would trigger a lambda process and send an alert
SNS to Slack	http://notes.webutvikling.org/send-aws-cloudwatch-alarms-to-slack/	We are currently using this mechanism with CircleCI.
Ansible - SNS	http://docs.ansible.com/ansible/latest/modules/sns_topic_module.html	Might be handy to have ansible populate /manage sns
New Relic/Splunk - SNS	https://docs.aws.amazon.com/sns/latest/dg/SendMessageToHttp.html	How to create an notification channel in New Relic that sends alert to SNS

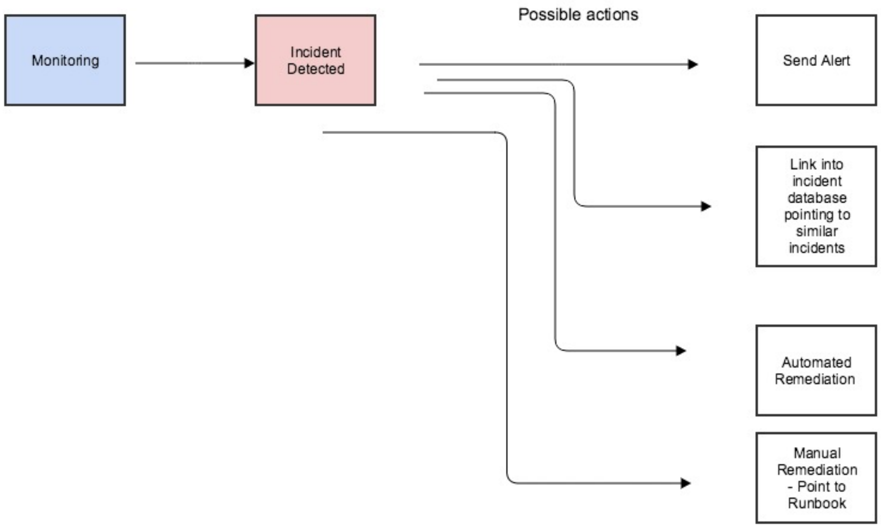
I am reworking a diagram from a previous page because after coming across AWS SNS, it appears this makes more sense as a basis for alerting then Slack. It offers the ability to publish messages to your endpoint of choice (HTTP, SQS, Lambda, mobile push, email, or SMS) . SNS is well integrated with AWS CloudWatch and offers Lambda as a way to process alerts. It is also not dependent on Slack but can use Slack as a alert mechanism as well as email, Teams, SNS, telephone etc.


Monitoring Software
New Relic
CloudWatch
Splunk
AWS Status RSS Feed
Custom Monitoring
AWS SNS (Simple Notification Service)
For escalations an SNS notification is published
Lamda Alert Application
Notification Endpoints Including:
Slack
SMS
Email
Lamda
HTTP
Mobile Push
Teams
Blue Jean Session Opened
Open Jira/Service Now Ticket
Update Application Dashboard Status Page

Alert Application Detail


Endpoint Slack, SMS, Email...
Alert App
AWS RDS Database
UI for Alert App
Oncall Scheduling
Confluence Calendar
Define Alert Level and Response
Override Alerts
Interface data/instructions for status page communications
Escalation Definitions i.e. Product Owner Manager
Vacation Scheduling
Alert Viewing - Current and Historical

Basic Functionality and Flow for Incident Management


Possible actions
Monitoring
Incident Detected
Send Alert
Link into incident database pointing to similar incidents
Automated Remediation
Manual Remediation - Point to Runbook