# AWS Config Configuration Guide

# CloudTrail

CloudTrail is service that logs all management events (such as user action) and data events (such as lambda execution). We need a S3 bucket to store event logs for all regions which will be created during enable process. CloudTrail can also output logs to CloudWatch. This is optional but recommended for further log analysis.

## Enable CloudTrail

**Notice: Only need enable CloudTrail once on a single region for whole AWS account.**

AWS Console -> Services -> CloudTrail -> Getting Started

*Optional: Data Events - S3: Select all S3 buckets in your account*

*Optional: Data Events - Lambda: Log all current and future functions*

S3 bucket name: redbend-it-trail1. Bucket located in it-prod account.

# AWS Config

Ensure AWS resources configuration compliance. Define rules that are either event-based or time-triggered to check resource configuration. Events can be sent to SNS topic for user notification.

## Enable AWS Config

Notice: Config need to be enabled on each region separately to monitor local resources.

Go to AWS Console -> Services -> Config -> Getting Started

Record all resources supported in this region: Check

Include global resources (e.g., AWS IAM resources): Check

**Notice: Only need to check this on one region for an AWS account.**

Amazon S3 bucket: redbend-aws-config-bucket. Bucket located in it-prod account.

AWS Config rule: See below section.

## Enable AWS Config Managed rules

AWS Config comes with a set of pre-defined rule templates. Enable recommended pre-defined rules:

Go to AWS Console -> Services -> Config -> Rules -> Add Rules, Choose below items from the template list.

Cloudtrail\_enabled: Check if Cloudtrail is enabled

ec2\_stopped\_instance: Check if there are instances in stopped state for longer than 30 days

required\_tags: Requires common resource have following tags: Owner, Purpose, Project

restricted\_incoming\_traffic: Scans unrestricted ports on 22/3389/3306/4333/1521

ec2\_volume\_inuse\_check: Check if there are not-used EBS disk

eip\_attached: Check if all EIP are being used

encrypted\_volumes: Requires EC2 Volumes to be encrypted

## Aggregated View

An Aggregator is setup for a centralized view for all AWS Config Service Events. To see all events for all AWS accounts and regions, please logon to it-prod AWS account -> AWS Config service -> Frankfurt region -> Aggregated view.

# Production Environment Configuration and Facts

AWS Config S3 Bucket: redbend-aws-config-bucket. Registered in it-prod account.

AWS Config SNS Topic: arn:aws:sns:<region>:<account\_id>:redbend-aws-config-topic

Cloudtrail S3 Bucket: redbend-cloudtrail-bucket. Registered in it-prod account.

|  |
| --- |
|  |
|  |