



# **Landing Zone Immersion Day**

*Lab 6 – Extend your Landing Zone*

---

**June 2018**

**Table of Contents**

Overview..... 3

Extend your Landing Zone – Add Centralized Logging Spoke ..... 3

Extend your Landing Zone – Add Config Rule..... 3

## Overview

This lab will walk you through the deployment of the Centralized Logging Spoke and the deployment of an additional Config Rule by updating the templates and manifest files.

This lab assumes you have completed **Lab 1 – Deploy the Landing Zone** and **Lab 5 – Deploy Centralized Logging**.

## Extend your Landing Zone – Add Centralized Logging Spoke

To add Centralized Logging Spoke to the account baseline, the manifest YAML file need to be edited.

1. Download `aws-landing-zone-configuration.zip` from the `aws-landing-zone-configuration-<accounted>-<region>` bucket in the Master Account to your laptop.
2. Scroll to the bottom of the Manifest YAML file and uncomment the following lines i.e. remove the '#' sign from in front of every line.

```
# - name: CentralizedLoggingSpoke
#   baseline_products:
#     - AWS-Landing-Zone-Account-Vending-Machine
#   template_file: templates/aws_baseline/aws-landing-zone-centralized-logging-
spoke.template
#   parameter_file: parameters/aws_baseline/aws-landing-zone-centralized-logging-
spoke.json
#   deploy_method: stack_set
```

## Extend your Landing Zone – Add Config Rule

To add additional Config Rules, the following two files need to be edited in the `aws-landing-zone-configuration.zip` and the zip file needs to be uploaded to the s3 bucket.

```
parameters/aws_baseline/aws-landing-zone-config-rules.json
templates/aws_baseline/aws-landing-zone-config-rules.template
```

1. Add a new Managed Config Rule to check for S3 bucket versioning, perform the following edits: **templates**/aws\_baseline/aws-landing-zone-config-rules.template

### a. Add to Parameters section:

```
EnableS3BucketVersioningRule:
  Type: String
  Description: "Enable S3 bucket versioning Config Rule?"
  Default: true
```

Landing Zone Immersion Day  
Lab 6 – Extending your Landing Zone

```
AllowedValues:
- true
- false
```

b. Add to Conditions section:

```
EnableS3BucketVersioning:!Equals
- !Ref EnableS3BucketVersioningRule
- 'true'
```

c. Add to Metadata section > AWS::CloudFormation::Interface: > Label > Parameters:

```
- EnableS3BucketVersioningRule
```

d. Add to Resources section:

```
CheckForS3BucketVersioning:
  Type: AWS::Config::ConfigRule
  Condition: EnableS3BucketVersioning
  Properties:
    Description: Checks whether versioning is enabled for your S3
    buckets.
    Scope:
      ComplianceResourceTypes:
        - AWS::S3::Bucket
    Source:
      Owner: AWS
      SourceIdentifier: S3_BUCKET_VERSIONING_ENABLED
```

2. Add a new Managed Config Rule to check for S3 bucket versioning, perform the following edits: **parameters**/aws\_baseline/aws-landing-zone-config-rules.json

a. Add this parameter

```
{
  "ParameterKey": "EnableS3BucketVersioningRule",
  "ParameterValue": "true"
},
```

3. Zip the contents of the directory back into the aws-landing-zone-configuration.zip.

**Note: Make sure the manifest.yaml is at the ROOT of the zip i.e. do not zip the folder.**

4. Upload aws-landing-zone-configuration.zip to the aws-landing-zone-configuration-<accounted>-<region> bucket in the Master Account. To upload the file, you can either use CLI or S3 Console

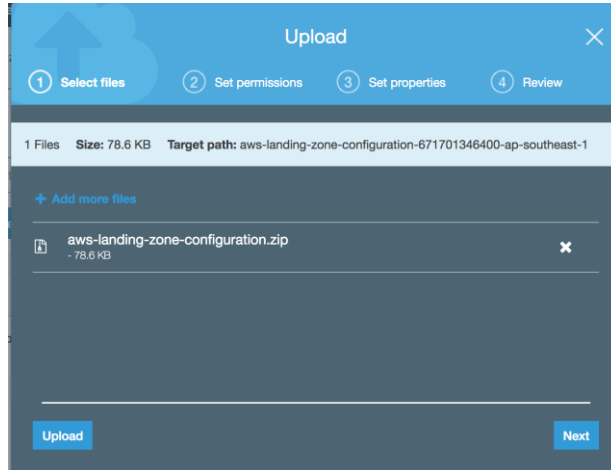
- [Option 1] Using CLI: Use the AWS CLI as the S3 bucket policy does not support uploads that do not include the **x-amz-server-side-encryption** header

requesting server-side encryption with SSE-KMS. From your local console run the following command:

```
aws s3 cp aws-landing-zone-configuration.zip s3://aws-landing-zone-configuration-<mastraccountnumber>-us-east-1/ --sse=aws:kms --sse-kms-key-id arn:aws:kms:us-east-1: <mastraccountnumber>:key/<encryptionkeyid>
```

*Your full encryption key ID ARN can be found when clicking on **AwsLandingZoneKMSKey** as outlined in step 8.d above.*

- [Option 2] Using S3 Console:
  - i. On S3 Console, Click on 'Upload'
  - ii. Click 'Add files'
  - iii. Select the aws-landing-zone-configuration.zip file



5.

- iv. Click 'Next'
- v. Click 'Next' one more time
- vi. Under 'Encryption' select 'AWS KMS master-key'
- vii. From the drop down select 'AwsLandingZoneKMSKey'

## Landing Zone Immersion Day

### Lab 6 – Extending your Landing Zone

The screenshot shows the AWS S3 'Upload' console window. The top navigation bar includes a blue arrow icon, the title 'Upload', and a close button. Below the navigation bar, there are four steps: 'Select files' (checked), 'Set permissions' (checked), 'Set properties' (active, circled in red), and 'Review' (circled in red). The 'Set properties' section contains several options: 'Standard' (selected), 'Standard-IA', 'One Zone-IA', and 'Reduced redundancy'. Under the 'Encryption' section, there is a note 'Protect data at rest by using Amazon S3 master-key or by using AWS KMS master-key.' and three radio buttons: 'None', 'Amazon S3 master-key', and 'AWS KMS master-key' (selected). Below the radio buttons is a dropdown menu showing 'AwsLandingZoneKMSKey'. The 'Metadata' section has a note 'Metadata is a set of name-value pairs. You cannot modify object metadata after it is uploaded.' and a table with two columns: 'Header' and 'Value'. At the bottom, there are three buttons: 'Upload' (blue), 'Previous' (light blue), and 'Next' (light blue).

viii. Click 'Upload'

6. Check CodeBuild for errors

7. Check the Code Pipeline for errors...