SBC AWS Landing Zone Project

**AWS Control Tower setup & Guide**

**Version 1.0 Date: 26-May-2022**

1, AWS Control Tower setup

**Objective:**

* 1. AWS Control Tower automates the setup of a landing zone by using best-practice templates for identity, federated access, guardrails, and account structure.
  2. The AWS Control Tower dashboard provides visibility into your landing zone environment, an aggregated view of OUs and accounts in the organization.

2, Prerequisites:

2.1 [Sign up for AWS](https://docs.aws.amazon.com/controltower/latest/userguide/setting-up.html#setting-up-signup) Management account

2.2 [IAM User](https://docs.aws.amazon.com/controltower/latest/userguide/setting-up.html#setting-up-iam) with Admin privilege in Management account

2.3 Automated pre-launch checks for your management account

2.4 AWS Control Tower sets up the landing zone, it automatically runs a series of pre-launch checks in your account.

2.5 There's no action required on your part for these checks, which ensure that your management account is ready for the changes that establish your landing zone.

**Note:** By default, all accounts are subscribed to these services.

3, AWS SSO Setup Consideration:

3.1 AWS Control Tower home Region must be the same as the AWS SSO Region.

3.2 Here in our SBC’s Control Tower setup, we are using **External Identity Provider** as the identity resource.

***Note:***For more information on AWS SSO setup please refer the document: SBC\_Azure AD SSO integration with AWS Single Sign-on\_V1.0.docx

4, Requirements for account email addresses

4.1 A set of new unique **“Email addresses”** we required for setting up a new control tower landing zone.

4.2 Audit account – This account is for our team of users that need access to the audit information made available by AWS Control Tower.

4.3 Log archive account – This account is for our team of users that need access to all the logging information for all of your enrolled accounts within registered OUs in your landing zone.

Note: These accounts are set up in the Security Organizational Unit.

5, Landing zone configuration

5.1 Open AWS Console and Navigate to AWS Control tower

5.2 verify that working in our desired home Region for AWS Control Tower. choose Set up your landing zone.

5.3 In this section of the setup process, add any additional AWS Regions that you require

5.4 The panel shows you the current Region selections. Open the dropdown menu to see a list of additional Regions available for governance.

5.5 Check the box next to each Region to bring into governance by AWS Control Tower.

6, Configure Organizational units (OUs)

6.1 AWS Control Tower relies upon a Foundational OU that is initially named the Security OU.

6.2 Security OU contains two shared accounts, which by default are called the log archive account and the audit account.

6.3 We can setup more Additional OU’s

7, Configure Shared accounts

7.1 At the console, enter a name for the account initially called the log archive account. Provide a unique email address for this account.

7.2 Enter a name for the account initially called the audit account. Provide a unique email address for this account.

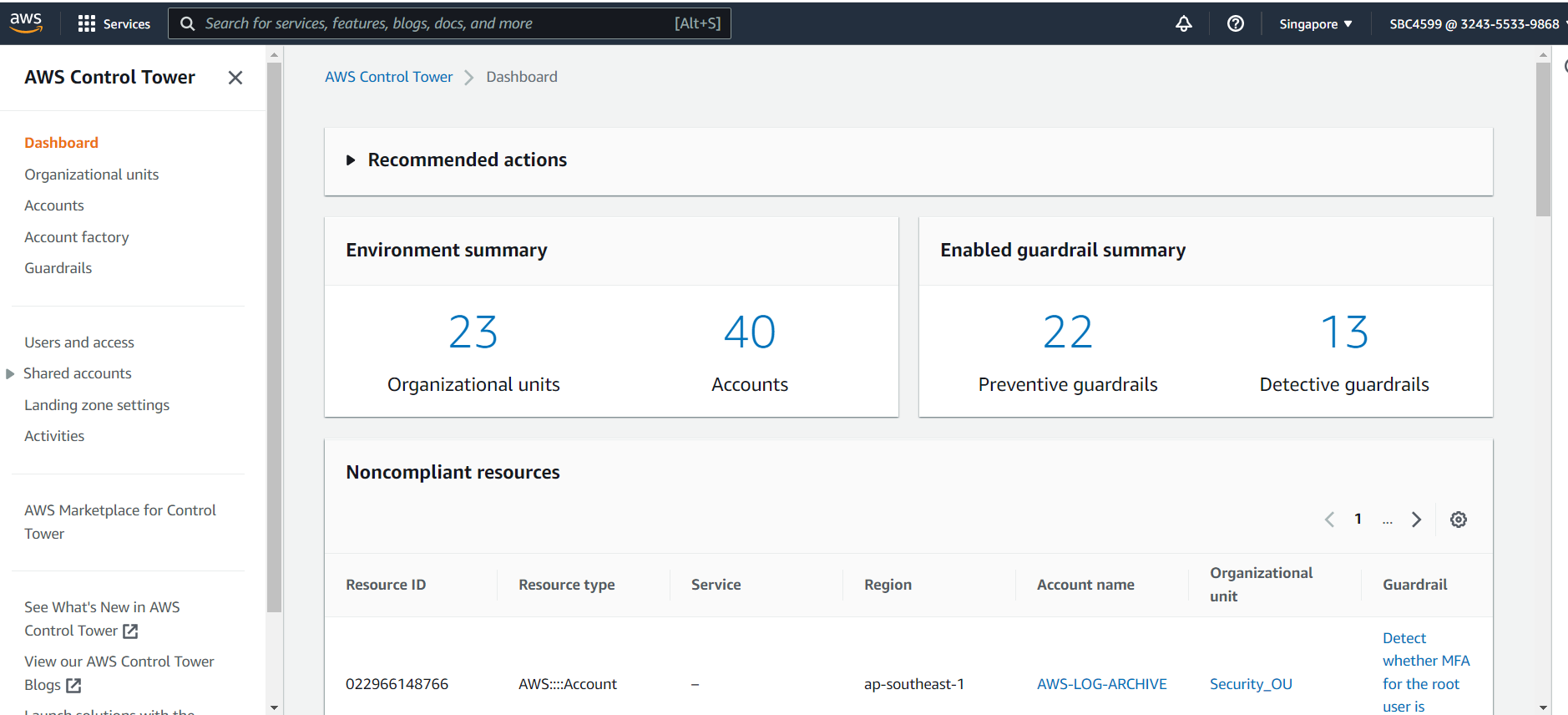
8, Review and set up the landing zone

8.1 At the console, review the Service permissions, and choose I understand the permissions AWS Control Tower will use to administrator AWS resources and enforce rules on my behalf.

8.2 To finalize, selections and initialize launch, choose Set up landing zone.

9, AWS Control Tower Overview

**Common – Dashboard**

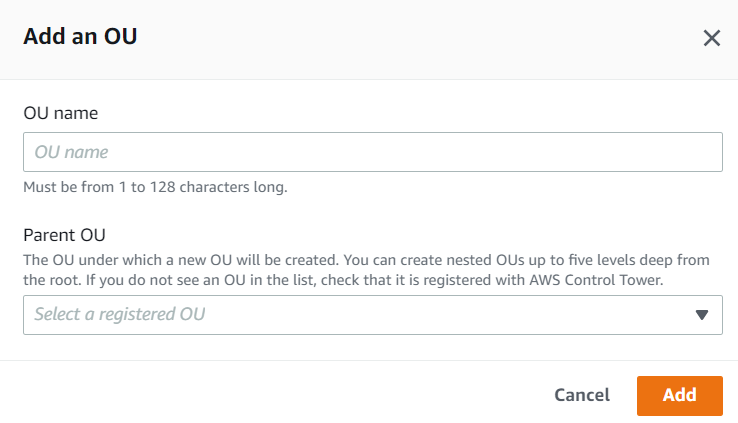
****

**9.1 Organizations**

9.1.1 Under Control Tower – Organizations Unit (OUs) are groups of AWS accounts that are administered as a single logical unit.

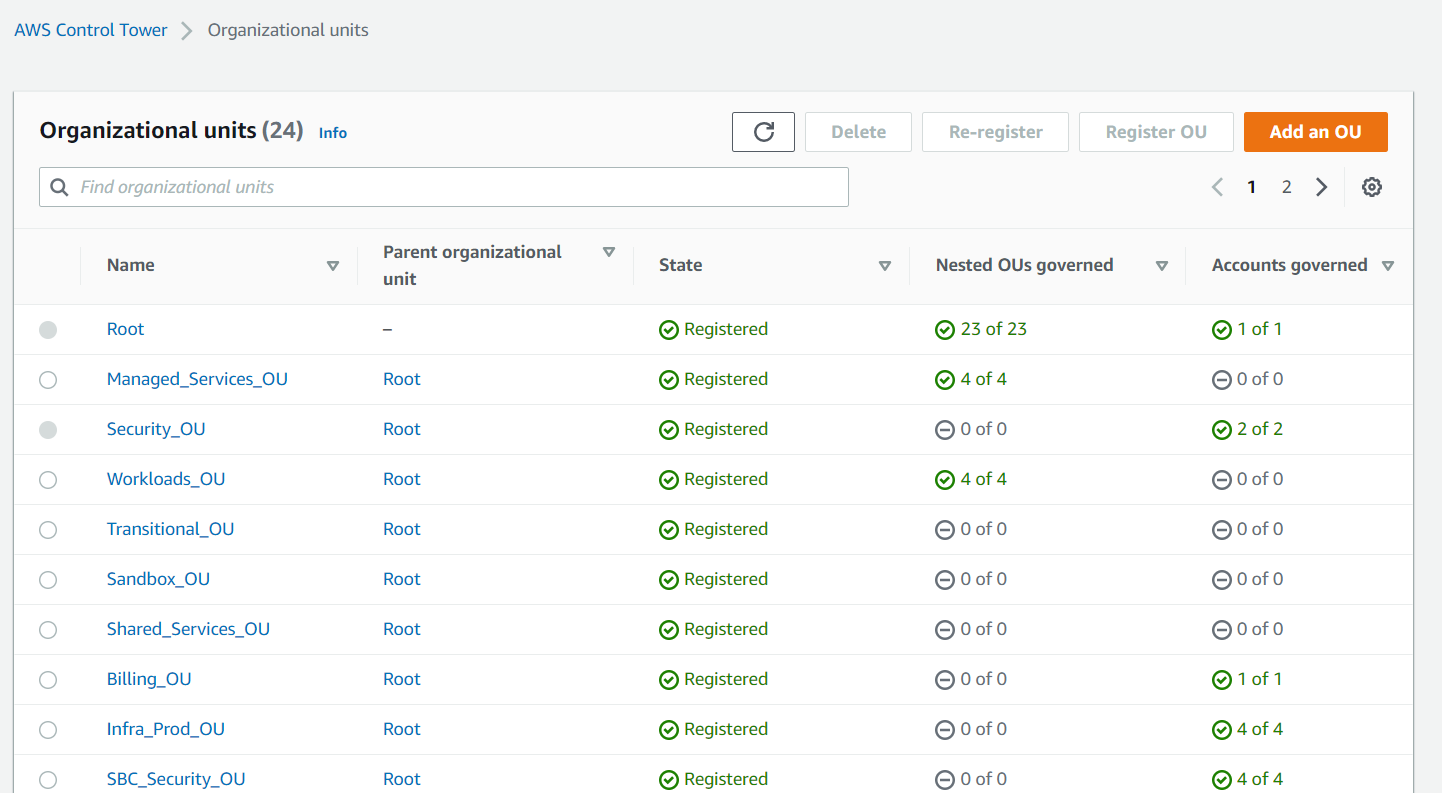
9.1.2 Certain OUs are governed by AWS Control Tower so that guardrails can be applied to the accounts.

9.1.3 Creating OUs - To create a new OU in AWS Control Tower, choose Add an OU.



9.1.4 To register an OU in AWS Control Tower, choose Register OU

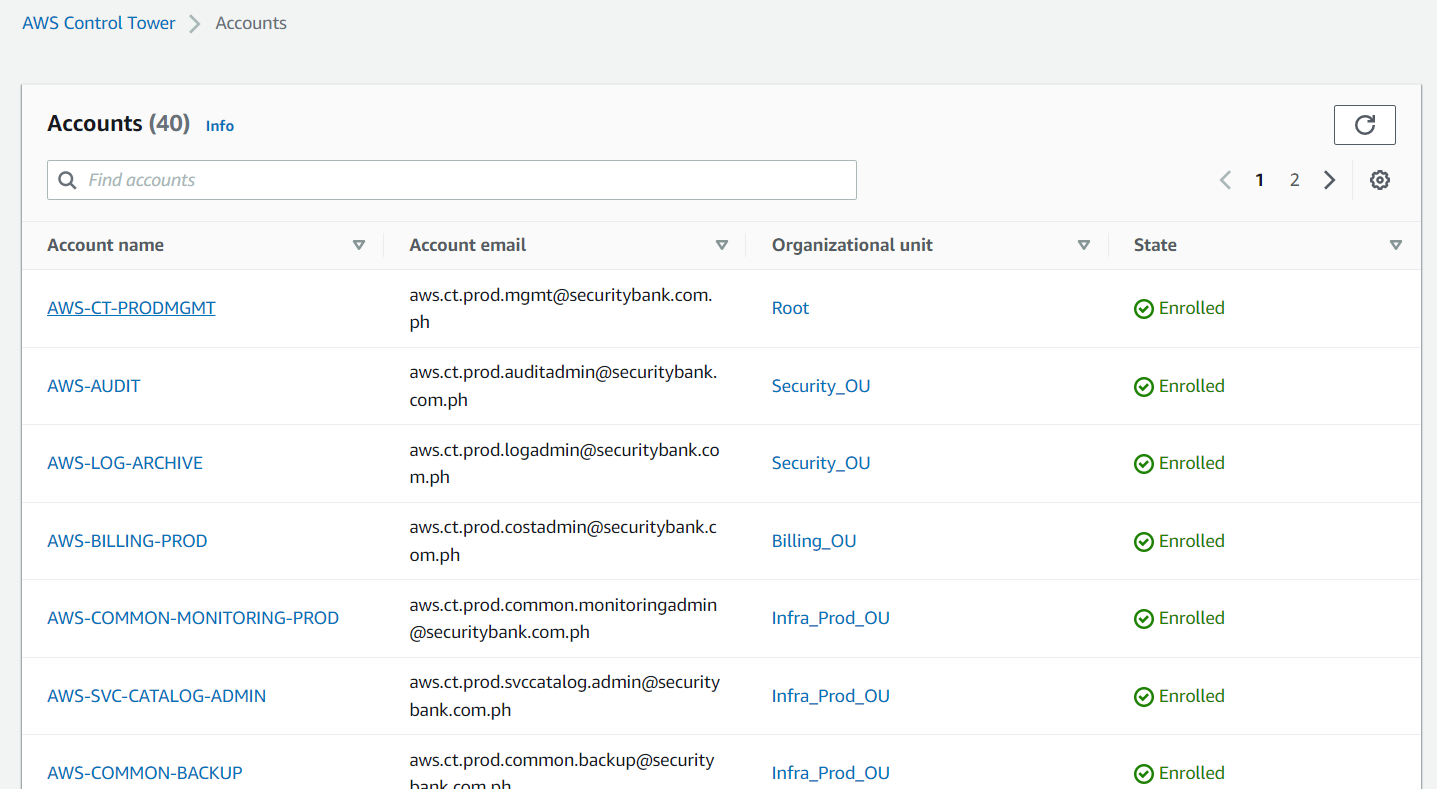
9.1.5 Registering OU, will extends AWS Control Tower governance to the OU and all of its member accounts.

****

**9.2 Accounts**

9.2.1 Under Control Tower -> Accounts, we can view our newly created & Migrated AWS accounts under our current AWS Organization.

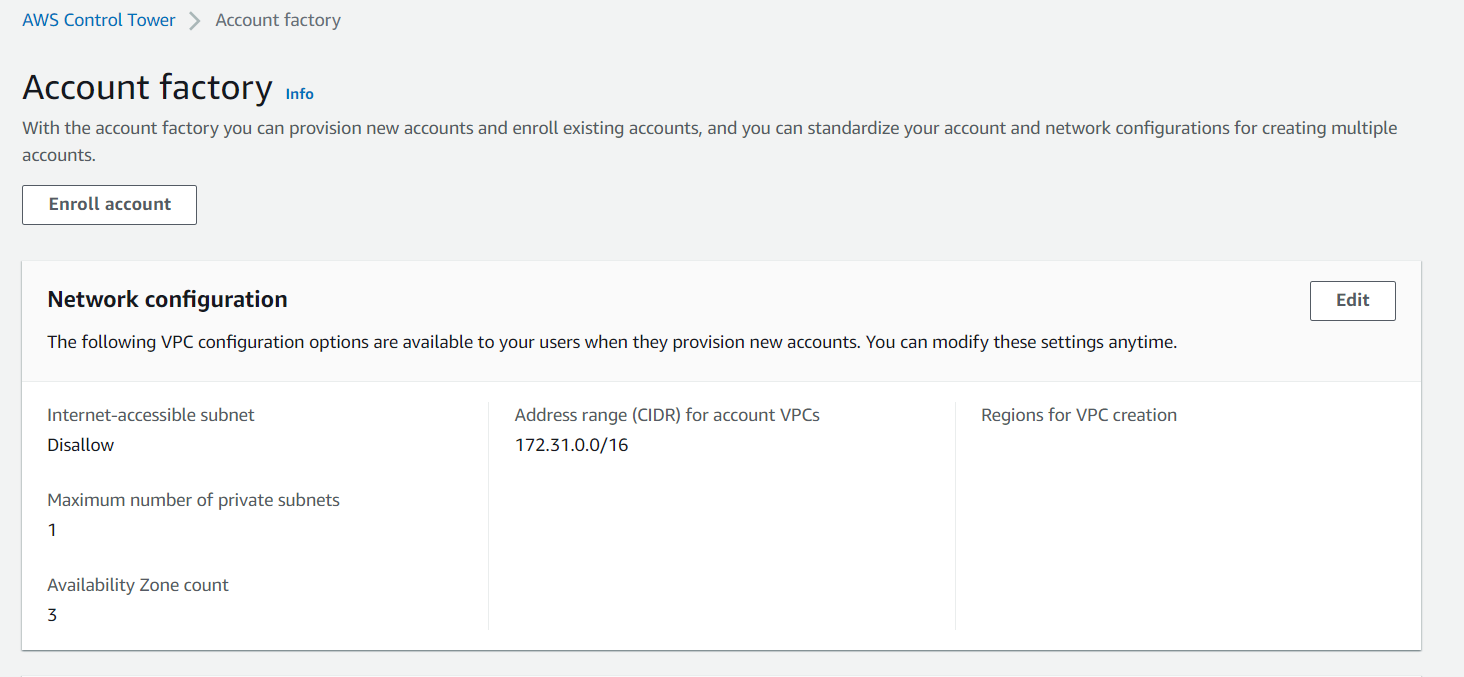
9.2.2 Individual account’s email ID, Organizational Unit and Enrollment status can be viewed with enabled guardrails.

****

**9.3 Account Factory**

9.3.1 Under Control Tower -> Account Factory we can provision new accounts and enroll existing accounts.

9.3.2 Standardize our account and network configuration by enrollment.

****

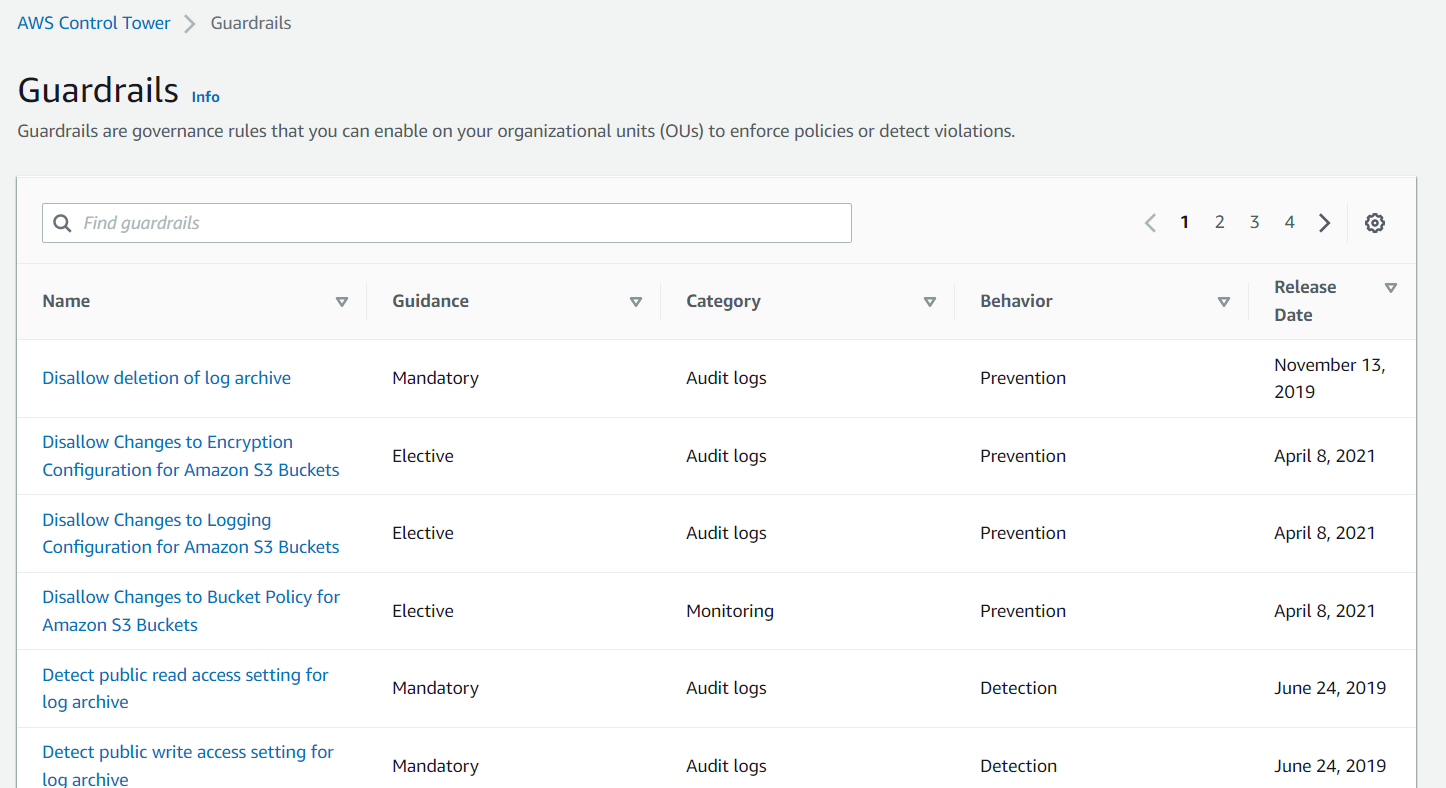
**Note:** For more information on Account Enrollment kindly follow the detailed steps in document - SBC\_AWS Landing Zone\_Migration & Enrollment\_V1.0

**9.4 Guardrails**

9.4.1 Under Control Tower -> Guardrails (AWS Managed – Strongly recommended, Mandatory, Elective categories) are there.

9.4.2 These are governance rules for your AWS environment.

9.4.3 A guardrail enabled on an organizational unit (OU) continuously enforces or detects compliance with the stated intent on all resources in the child accounts under the OU.

****

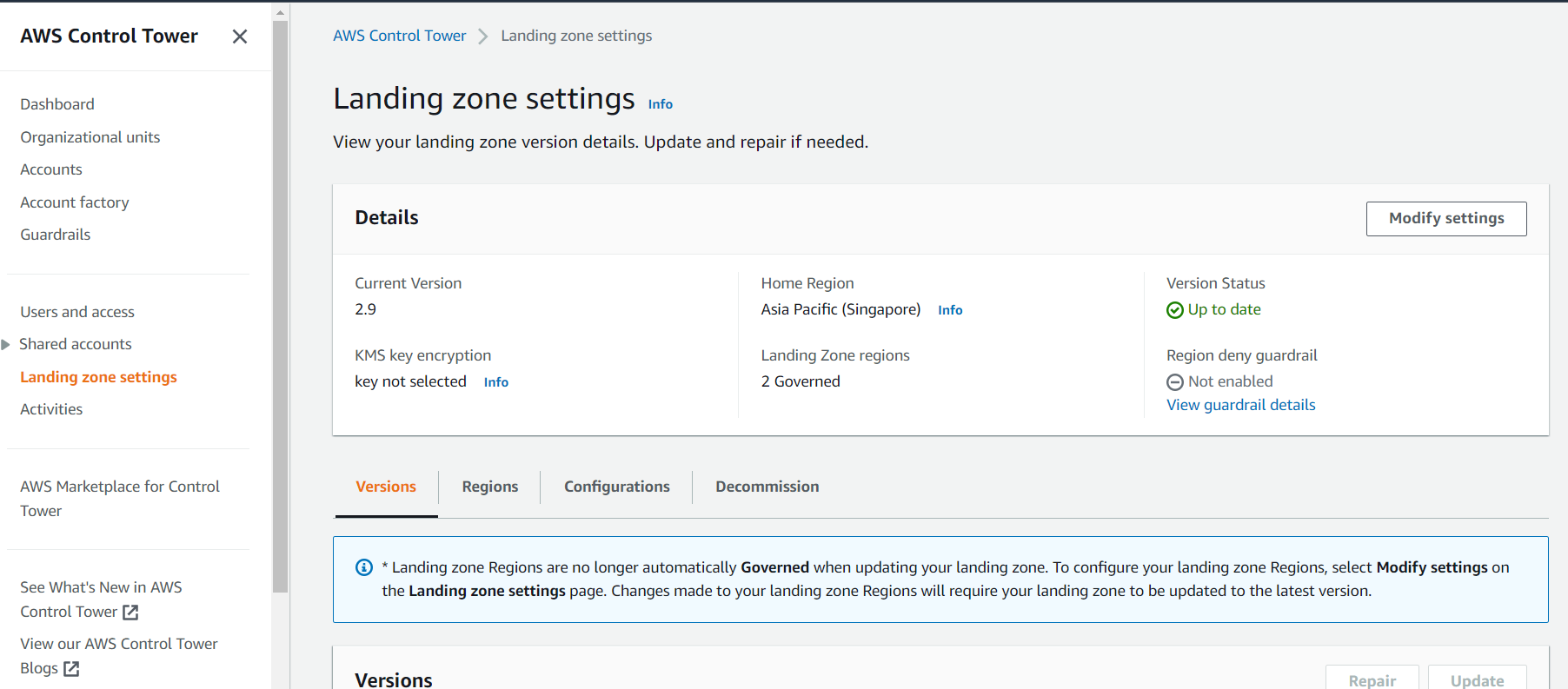
**Note:** For more information about Guardrails please follow detailed documentation -

**9.5 Landing Zone Settings**

**9.5.1 Version Tab:** we can choose an available version for “Update” or “Repair”.

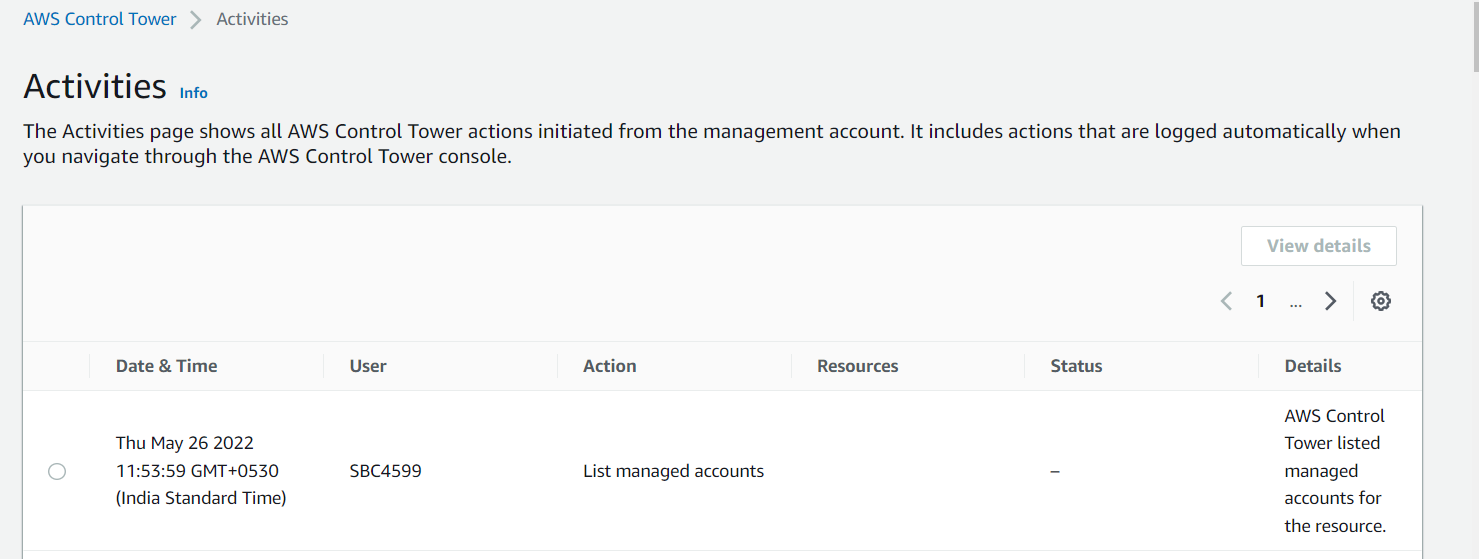
* Update becomes available for any major update to AWS Control Tower, or when there's expanded functionality.
* Choose Repair to view the AWS Control Tower update page and bring your landing zone back into a consistent state after drift occurs.

**9.5.2 Region tab**: We can view regions that control tower are available and governed.

****

**9.6 Activities**

From Control Tower -> Activities -> We can view all AWS Control Tower actions initiated from the management account and actions that are logged automatically.

****