

Tony Shen

AWS CONTROL TOWER

Contents

Introduction 3

AWS Organizations..... 3

Control Tower 10

Control Tower and Landing Zone..... 13

Control Tower API 18

Control Tower Documentation 34

Summary 35

References 35

Revision: v1, September 2019

Revision: v3, July 2025

Glossary

Term	Description
AWS	Amazon Web Services
CT	AWS Control Tower
LZ	AWS Landing Zone
CLI	Command Line Interface

Introduction

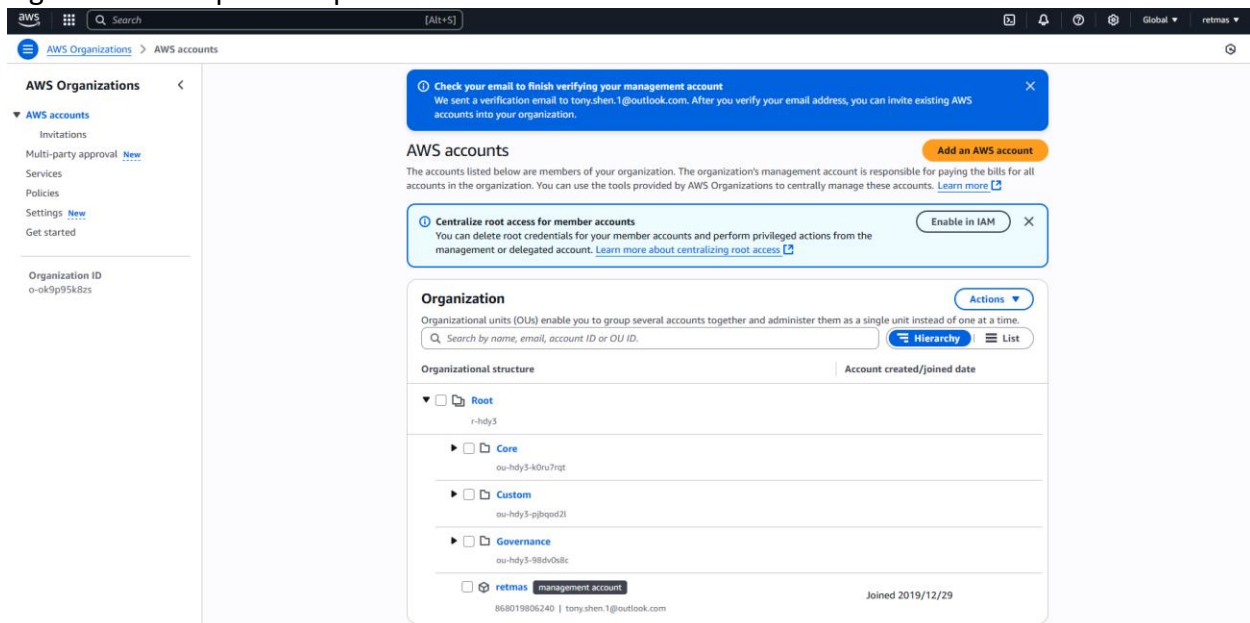
Control Tower is a service designed for creating and managing multi-account environments called AWS Organizations. Control Tower allows customer to organize multiple accounts into a logical entity Organization. Control Tower can create and manage multiple Organizations with each Organization having multiple AWS accounts in it. Organizations help an enterprise to standardize what they do in AWS. As easy to use and yet powerful tool, Control Tower helps an enterprise IT department in creating, managing, and enhancing Organizations.

AWS Organizations

Let's take a quick visual tour and see what Organizations are about.

Figure 1 below shows a simple Organization that Control Tower created. The Organization has three folders and one management account.

Figure 1 – A Simple Example



Control Tower (CT) created a hierarchy starting at **Root**. Under Root, it created **Core**, in which it deployed two AWS accounts, one for Logging, and the one for Auditing.

Parallel to Core, it created **Custom**, in there, reside user created AWS accounts. You can let CT create such an account for you. You can also import an existing AWS account. Those accounts are typically used to serve your business needs such as Accounting, Finance, HR, Sales, Inventory, Distribution, and/or Manufacturing.

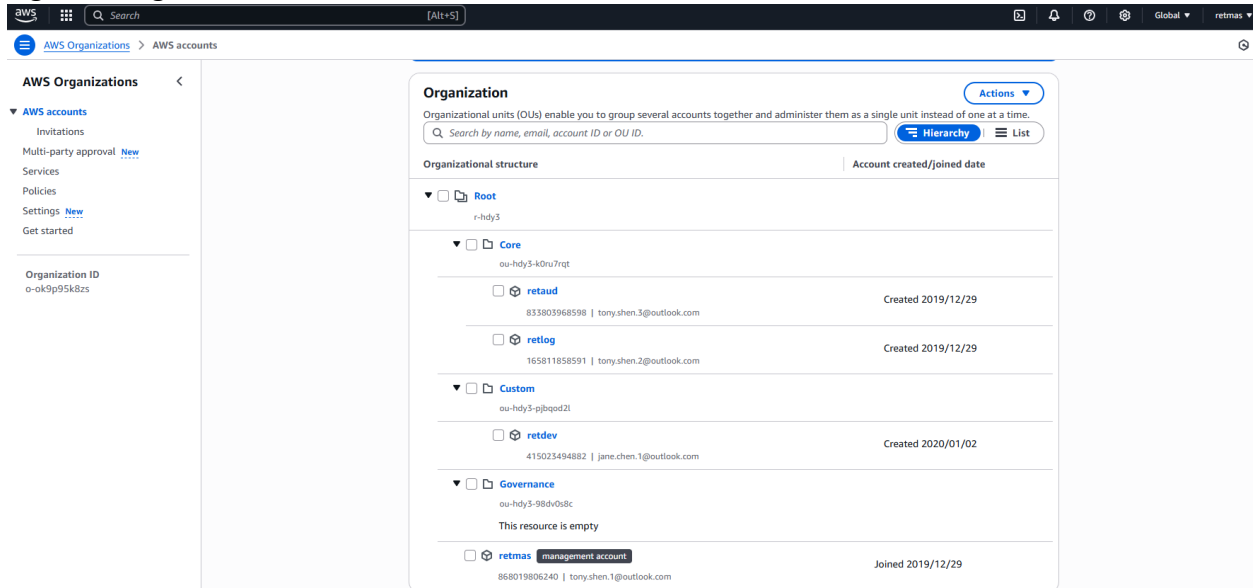
AWS Control Tower

Parallel to Core and Custom, CT created Governance, dedicated to AWS governance of accounts.

Finally, CT designated an account as your management account. It was the account from which you started CT and created the Organization of yours.

CT created this sample Organization automatically with minimum intervention from you.

Figure 2 Organization Basic Structure.



Now let's see what else Organizations involve.

AWS Organizations helps you centrally manage and govern your environment as you grow and scale your AWS resources. Using AWS Organizations, you can create accounts and allocate resources, group accounts to organize your workflows, apply policies for governance, and simplify billing by using a single payment method for all of your accounts. AWS Organizations is integrated with other AWS services so you can define central configurations, security mechanisms, audit requirements, and resource sharing across accounts in your organization. AWS Organizations is available to all AWS customers at no additional charge.

AWS Control Tower

Figure 3 – About Organizations

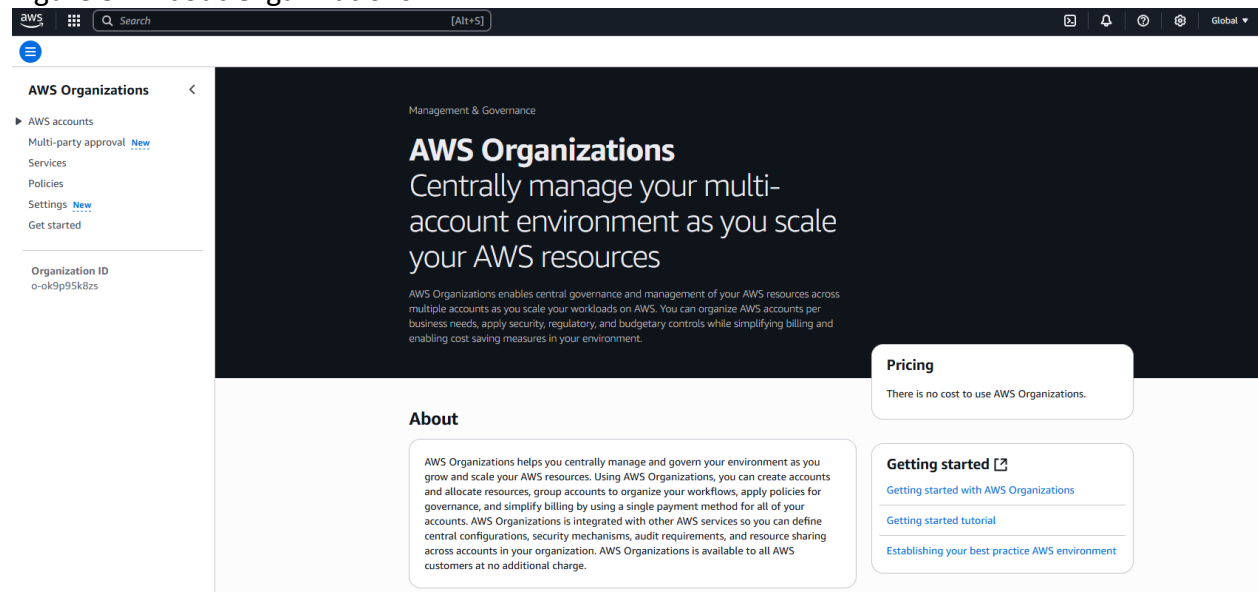
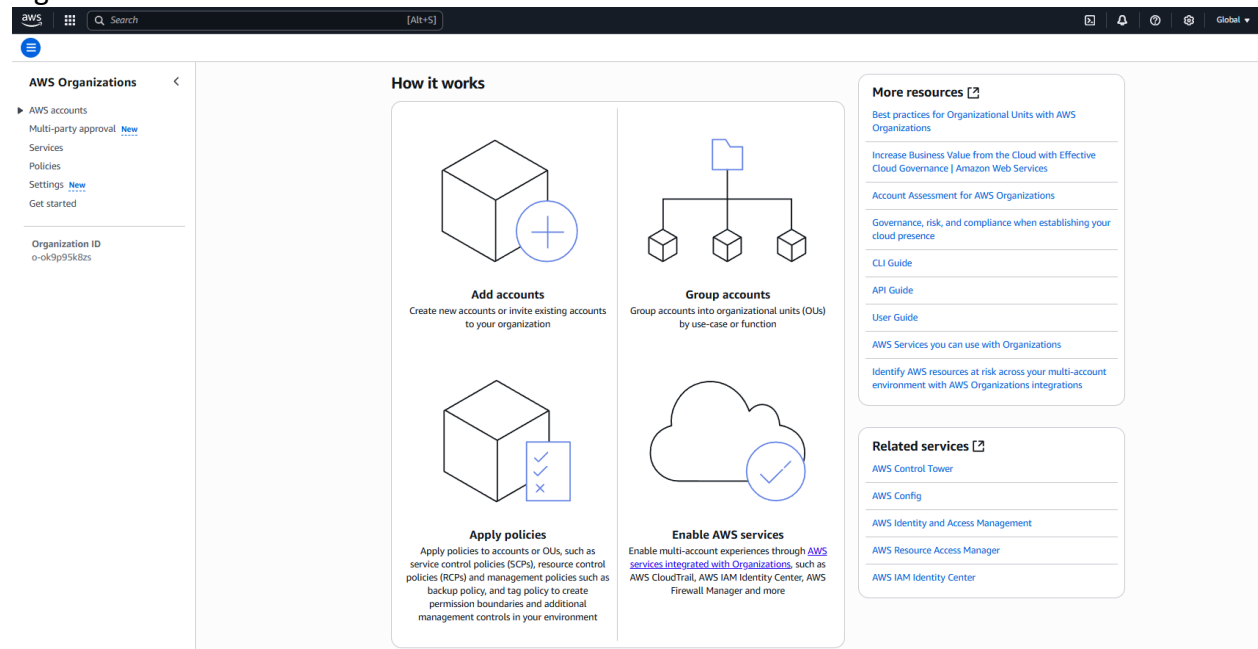


Figure 4 – How it works



AWS Control Tower

Figure 5 – Benefits and features

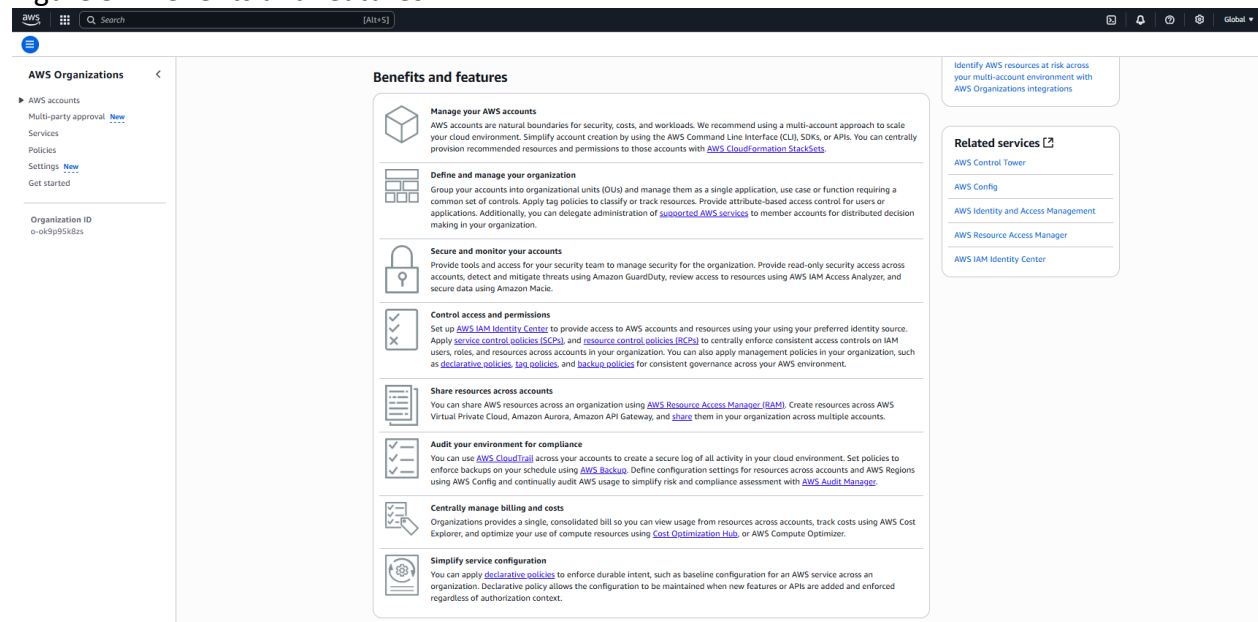
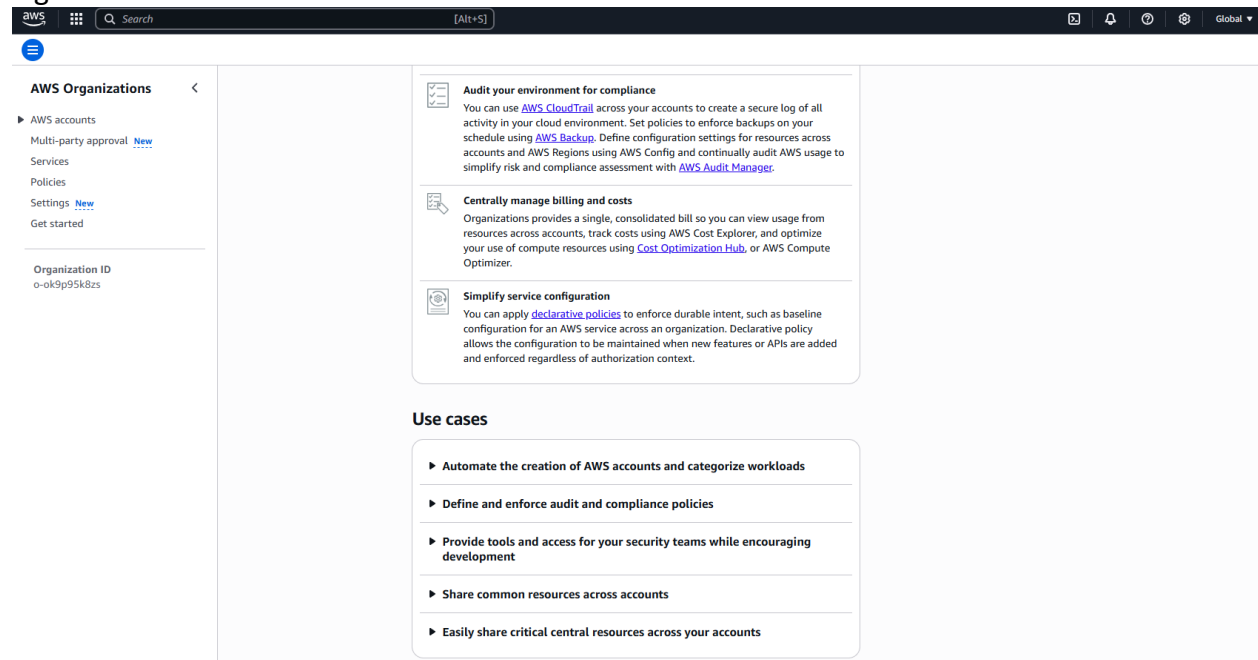


Figure 6 – Use Cases



AWS Control Tower

Figure 8 - Services

Services

You can configure supported AWS services to perform actions in your organization. A service for which you enable trusted access can retrieve information about the accounts, root, OUs, and policies for your organization. [Learn more](#)

Note: We recommend that you do not enable trusted access with an AWS service here. Instead, use the other AWS service's console to enable and disable trusted access with AWS Organizations. This allows the other service to perform any supporting tasks needed to enable or disable access with Organizations. For more information, see the documentation for the AWS service you want to use.

Integrated services

All services

Service	Trusted access	Enabled on
Amazon Detective Amazon Detective makes it easy to analyze, investigate, and quickly identify the root cause of potential security issues or suspicious activities. Amazon Detective automatically collects log data from your AWS resources and builds a linked set of data that enables you to easily conduct faster and more efficient security investigations.	Not enabled	-
Amazon DevOps Guru Amazon DevOps Guru uses machine learning to analyze operational data and identify behaviors that deviate from normal operating patterns. When operational issues are identified, DevOps Guru notifies you so that you can implement recommendations to improve your resources.	Not enabled	-
Amazon GuardDuty Amazon GuardDuty uses AI and ML with integrated threat intelligence from AWS and leading third parties to help protect your AWS accounts, workloads, and data from threats.	Not enabled	-
Amazon Inspector Amazon Inspector automatically discovers workloads, such as Amazon EC2 instances, containers, and Lambda functions, and scans them for software vulnerabilities and unintended network exposure.	Not enabled	-

Figure 9 – Services (Continued)

AWS Control Tower AWS Control Tower offers a straightforward way to set up and govern an AWS multi-account environment, following prescriptive best practices.	Enabled	December 29, 2019, 22:21 (UTC-6:00)
AWS Data Exchange AWS Data Exchange enables data providers to share data sets, recipients to access data grants, and subscribers to purchase data products from AWS Marketplace. It supports various data set types and integrates with AWS services like Amazon S3, API Gateway, Redshift, and Lake Formation.	Not enabled	-
AWS Health AWS Health provides ongoing visibility into your resource performance and the availability of your AWS services and accounts. AWS Health delivers events when your AWS resources and services are impacted by an issue or will be affected by upcoming changes. You can use the organizational view feature for AWS Health to get visibility into all events that occur in your organization. You can also use the AWS Health API to access the information programmatically.	Not enabled	-
AWS IAM Identity Center (AWS Single Sign-On) A managed service that makes it easy for you to centrally provide and manage single sign-on access to all your AWS accounts and cloud applications.	Enabled	December 29, 2019, 22:22 (UTC-6:00)
AWS Identity and Access Management AWS Identity and Access Management enables you to centrally manage root access for your organization. You can delete root credentials for member accounts and perform privileged actions.	Not enabled	-
AWS License Manager - Linux subscriptions AWS License Manager - Linux subscriptions provides you with the capability to view and manage commercial Linux subscriptions which you own and run on AWS. License utilization can be tracked across AWS Regions and accounts in AWS Organizations.	Not enabled	-

AWS Control Tower

Figure 10 - Policies

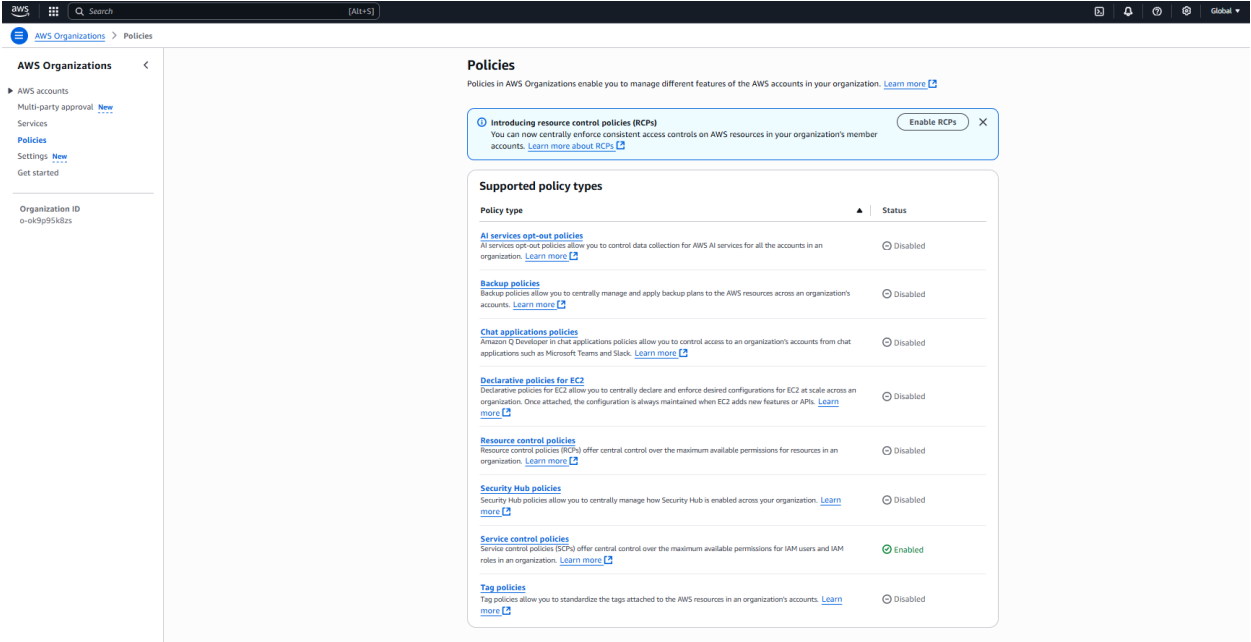
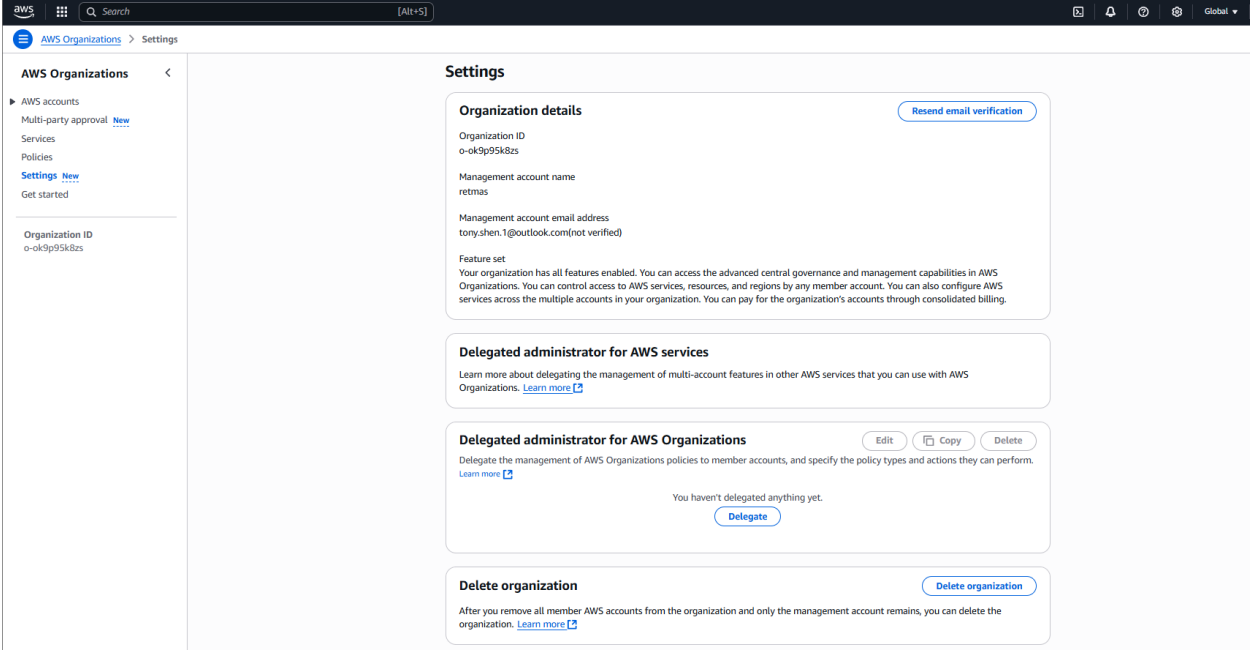


Figure 10 - Settings



AWS Control Tower

Figure 11 – Get started

The screenshot displays the AWS Organizations console interface. The top navigation bar includes the AWS logo, a search bar, and a [Alt+S] shortcut. The left sidebar shows the 'AWS Organizations' menu with options like 'AWS accounts', 'Multi-party approval', 'Services', 'Policies', 'Settings', and 'Get started'. The main content area is titled 'Get started' and features a 'Build your organization' section with four numbered steps: 1. Create accounts or invite existing accounts, 2. Organize your organization's member accounts into OUs, 3. Create policies, and 4. Enable AWS services that support AWS Organizations. To the right of this section is an 'Additional Information' sidebar with links to 'Best practices', 'Use cases', 'FAQs', 'Documentation', and 'API references'. Below the 'Build your organization' section, there is a 'Recommended organization structure' section with a link to 'Learn about our recommended OU structure'. At the bottom, a 'Feature spotlight' section highlights 'AWS Config' and 'AWS Security Hub' with brief descriptions and links to learn more.

Build your organization

When you sign in to your organization's management account, you can create accounts in your organization, invite existing accounts to join your organization, create and apply policies, and enable supported AWS services to work across the accounts in your organization.

- Create accounts or invite existing accounts**
Created accounts automatically become members of your organization. Invited accounts become members when they accept the invitation by replying to an email or by calling the [AcceptHandshake API](#). Member accounts are administered and managed by the organization. To easily access member accounts after creation, we recommend you enable [AWS IAM Identity Center \(AWS Single Sign-On\)](#).
- Organize your organization's member accounts into OUs**
Simplify management of your organization by grouping accounts into [organizational units \(OUs\)](#) and applying custom policies. This allows you to manage multiple accounts as a single unit and provide common permissions to groups of accounts within your organization. You can add nested OUs within each OU for more granular permissions, such as separating your production accounts from development accounts within each OU.
- Create policies**
Policies enable you to apply controls to the accounts in your organization. There are [several supported policy types](#) you can use to manage your organization. For example, [service control policies \(SCPs\)](#) specify the actions that are available to the users and roles in affected accounts. You can attach a policy to the entire organization, to OUs, or directly to an individual account.
- Enable AWS services that support AWS Organizations**
AWS has services that help you use AWS Organizations to secure, audit, and control the accounts in your environment. View the [list of supported services](#).

Additional Information

- [Best practices](#)
- [Use cases](#)
- [FAQs](#)
- [Documentation](#)
- [API references](#)

Recommended organization structure

Are you ready to build your OUs but are not sure where to start?

[Learn about our recommended OU structure](#)

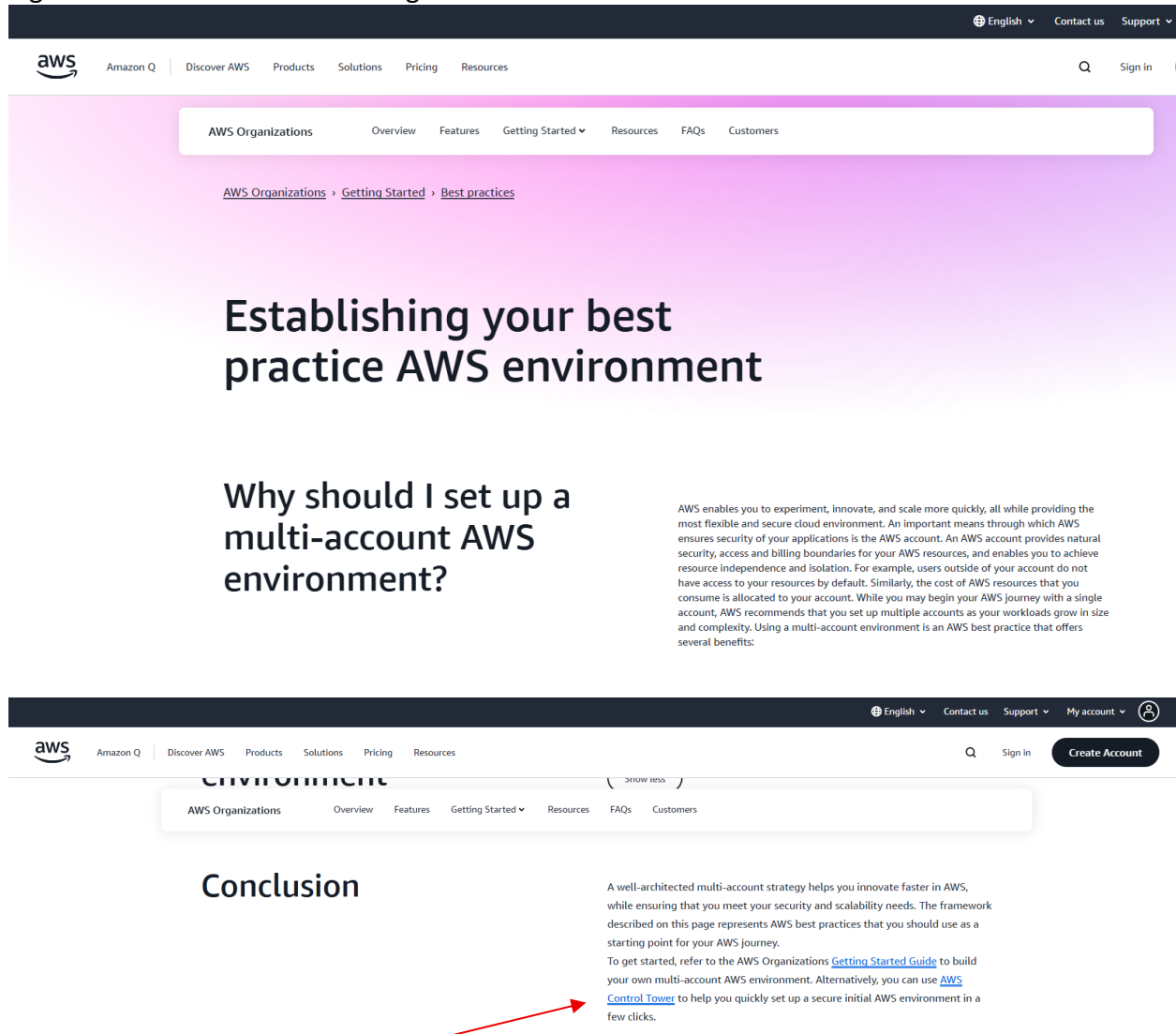
Feature spotlight

AWS Config
Assess, audit, and evaluate the configurations of your AWS resources. You can get an organization-wide view of your compliance status. You can also use AWS Config API operations to manage AWS Config rules and conformance packs across all AWS accounts in your organization. [Learn more](#)

AWS Security Hub
Ensure your organization meets industry standard security requirements and best practices with AWS Security Hub. When you use both Security Hub and AWS Organizations together, you can automatically enable Security Hub for all of your accounts, including new accounts as they are added. You can also designate a member account to manage Security Hub on behalf of the organization. [Learn more](#)

AWS Control Tower

Figure 12 – Learn more about Organizations



AWS Organizations is a service that helps you to manage your multi-account environment in AWS.

Control Tower is the tool that you can use to help you with Organizations.

Control Tower

To get an idea of how Control Tower works, see below Figure 13 Control Tower, Figure 14 Control Tower Dashboard, and Figure 15 Control Tower Dashboard (Continued)

AWS Control Tower

Figure 13 – Control Tower

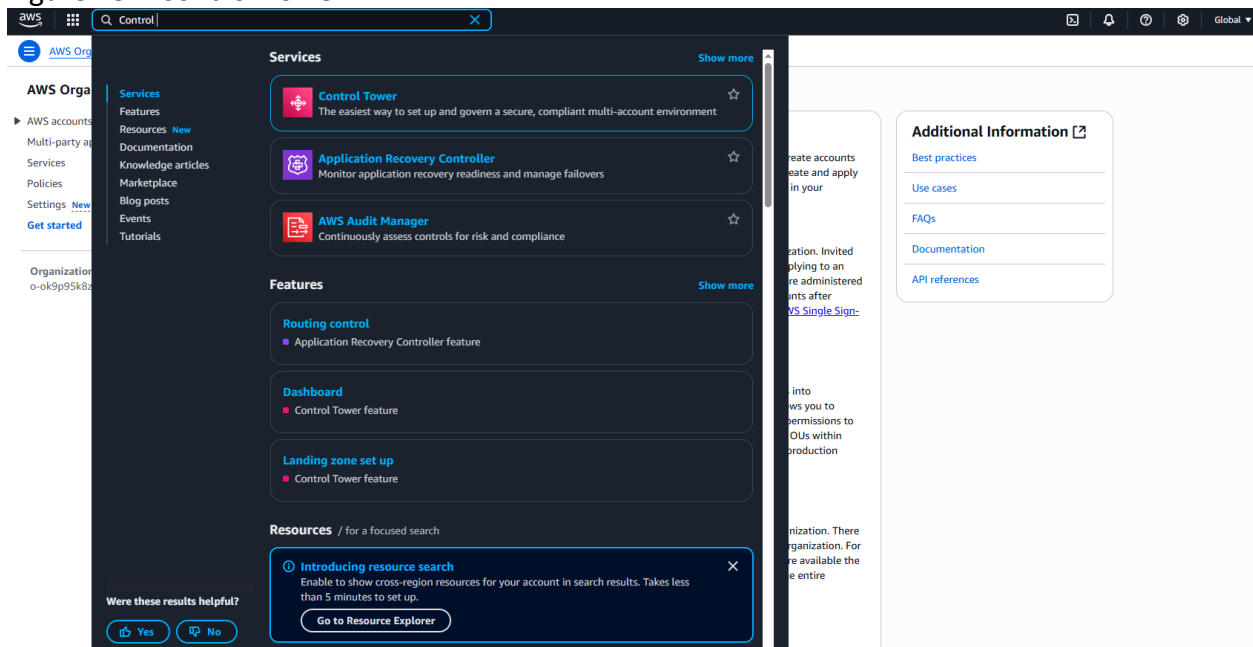


Figure 14 - Control Tower Dashboard

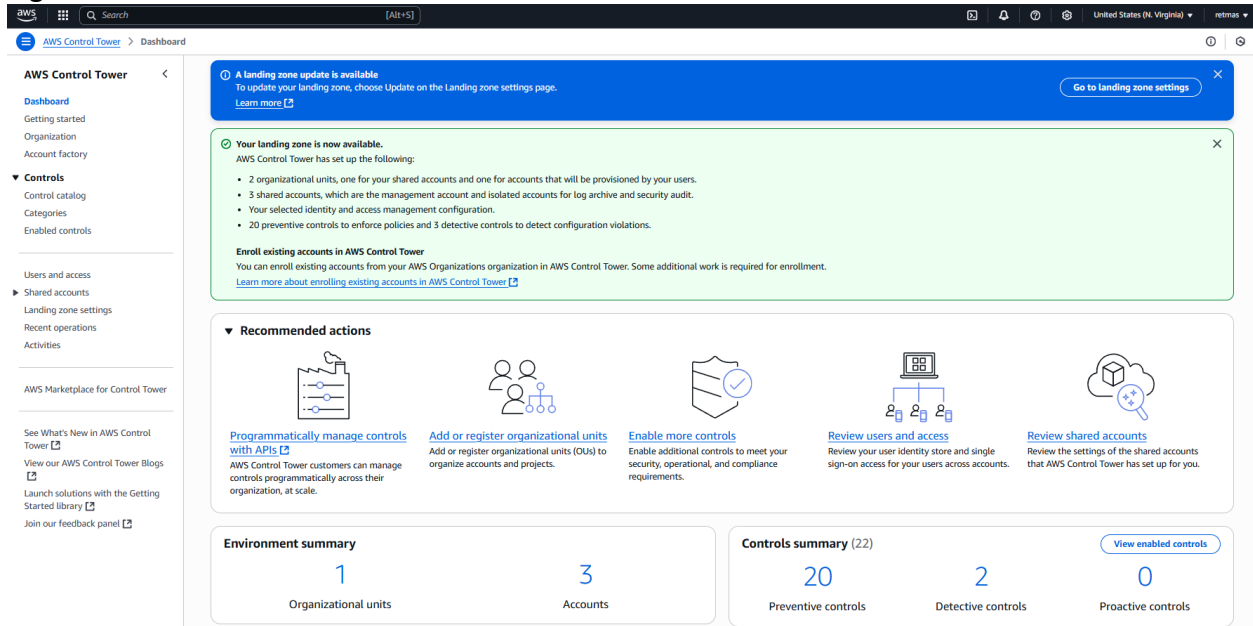


Figure 15 - Control Tower Dashboard (Continued)

[illegible]

Figure 16 - Control Tower Organization registered units and enrolled accounts

The screenshot displays the AWS Control Tower console interface. At the top, there's a navigation bar with the AWS logo, search icon, and user information (United States (N. Virginia), retmas). Below this, the left-hand navigation pane shows sections like Dashboard, Getting started, Organization (selected), Account factory, Controls, Users and access, Shared accounts, Recent operations, Activities, and AWS Marketplace for Control Tower. The main content area is titled "Organization" and features a blue banner at the top stating "A landing zone update is available". Below the banner, a message indicates that Organizational Units (OUs) are entities created within your organization to group accounts for governance. A table lists several OUs under the root "Root". Each row includes columns for Name, Baseline state, ID, Organizational units registered, and Accounts enrolled. The OUs listed are Governance, Core, retlog, retaud, Custom, retdev, and retmas.

Name	Baseline state	ID	Organizational units registered	Accounts enrolled
Root	Succeeded	r-hdy3	1 of 3	3 of 4
Governance	Not enabled	ou-hdy3-98dv0s8c	0 of 0	0 of 0
Core	Succeeded	ou-hdy3-k0ru7rqf	0 of 0	2 of 2
retlog	Enrolled	165811858591	-	-
retaud	Enrolled	833803968598	-	-
Custom	Drifted	ou-hdy3-pjbqdZl	0 of 0	0 of 1
retdev	Not enrolled	415023494882	-	-
retmas	Enrolled	868019806240	-	-

Control Tower and Landing Zone

Control Tower includes Landing Zone, a set of pre-configured settings for managing Organization effectively.

AWS keeps updating the Landing Zone from time to time. In Control Tower, you can check and update your LZ accordingly. Figure 17 shows the older version of LZ.

Figure 17 – Update Landing Zone

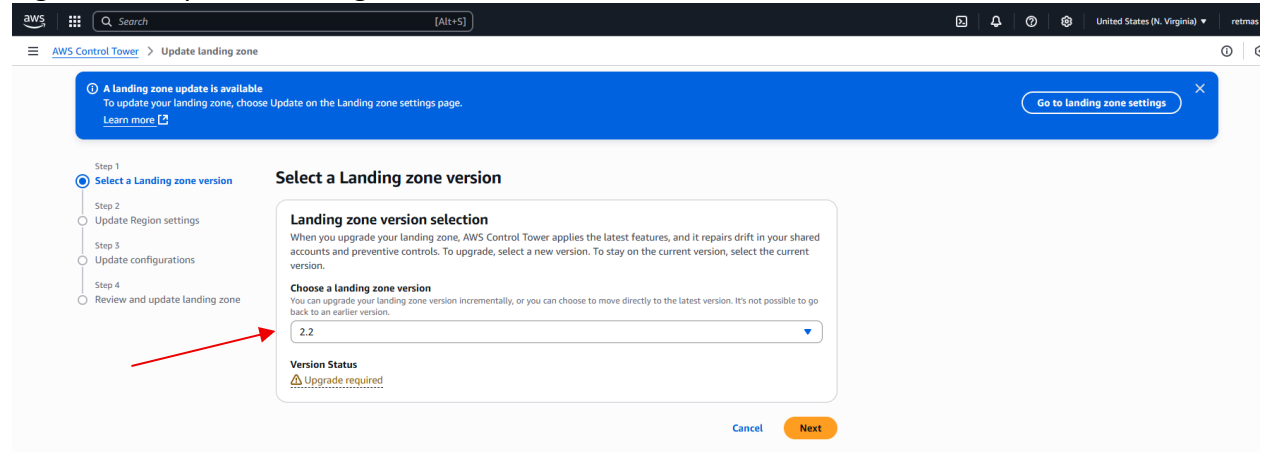
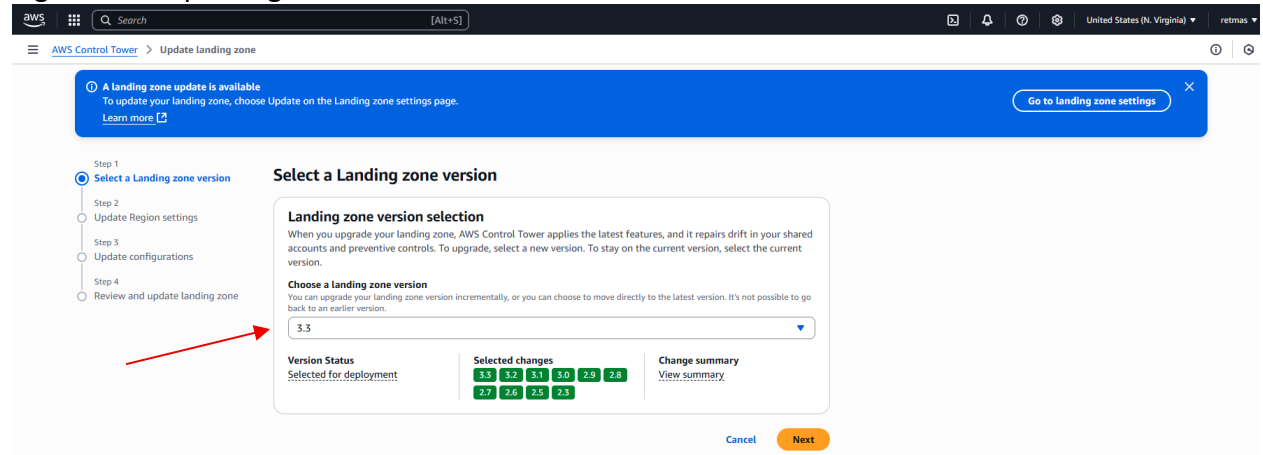


Figure 18 shows the latest version of LZ available for you to update to.

Figure 18 – Updating LZ to 3.3



An AWS account covers all AWS regions. When updating LZ, you can decide what regions to update and what regions not to update.

Figure 19 – Update Region Settings

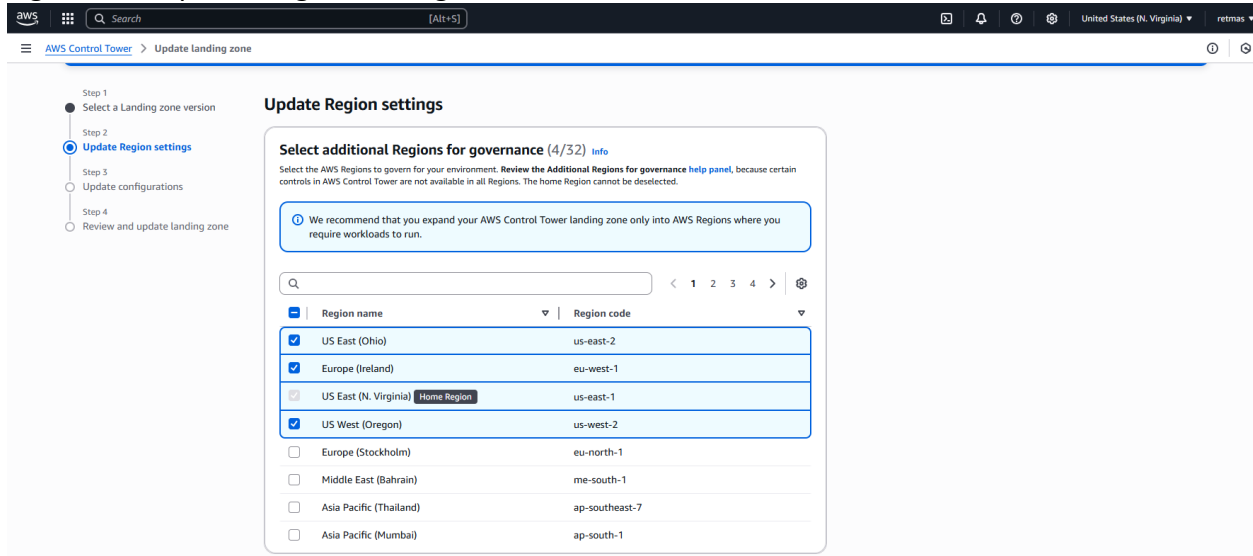
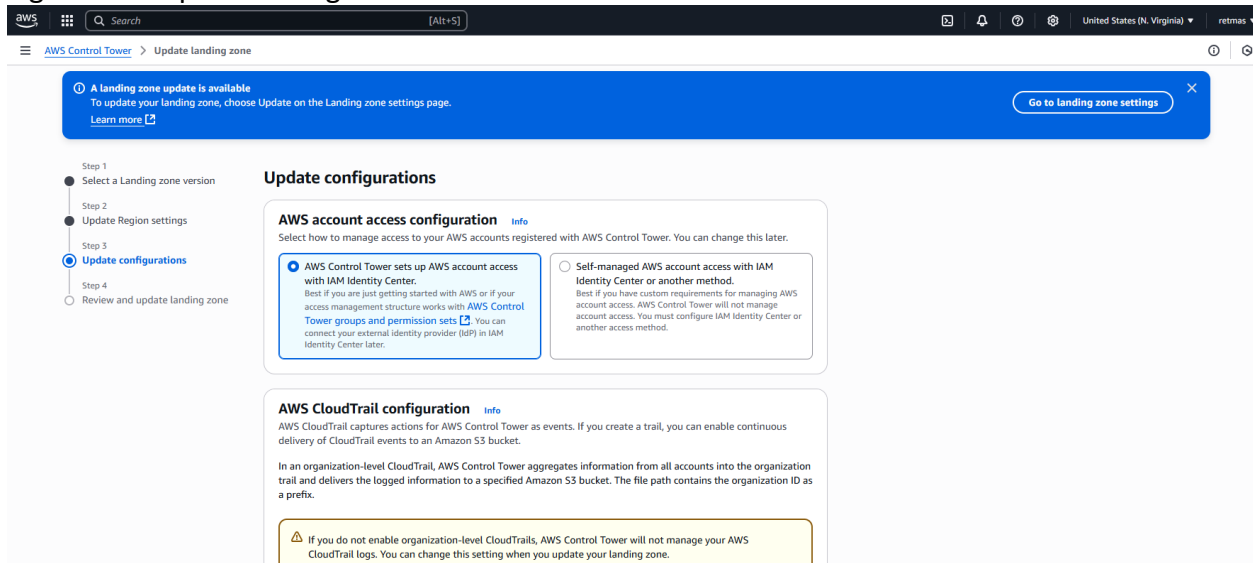


Figure 20 – Update configurations



AWS Control Tower

Figure 21 – Update configurations for CloudTrail

The screenshot shows the 'Update landing zone' configuration page in the AWS Control Tower console. The page is titled 'AWS CloudTrail configuration' and includes an 'Info' link. The text explains that AWS CloudTrail captures actions for AWS Control Tower as events and that you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket. It also states that in an organization-level CloudTrail, AWS Control Tower aggregates information from all accounts into the organization trail and delivers the logged information to a specified Amazon S3 bucket. The file path contains the organization ID as a prefix.

A warning box states: 'If you do not enable organization-level CloudTrails, AWS Control Tower will not manage your AWS CloudTrail logs. You can change this setting when you update your landing zone. AWS Control Tower strongly recommends that every organization or account establish AWS CloudTrail logging. You can create a custom trail that is not managed by AWS Control Tower, or you can select Enabled. A mandatory detective control detects whether enrolled accounts have enabled CloudTrail logging. [Learn more about AWS CloudTrail](#)'.

Below the warning box, there are two radio buttons: 'Enabled' (selected) and 'Not enabled'.

Below the radio buttons, there is a section titled 'Log configuration for Amazon S3 - optional' with an 'Info' link. It states: 'In these two fields, enter numbers that represent lifecycle retention times for the Amazon S3 logging bucket and the access logging bucket.'

There are two input fields: 'Amazon S3 bucket retention for logging' (Default: 1) and 'Format for logging' (years). Below the input fields, it states: 'Years must be expressed as integers from 1 to 15, with values up to 2 decimal places. Durations less than 1 year are expressed as days.'

Figure 22 - Update configurations for CloudTrail (Continued)

The screenshot shows the 'Update landing zone' configuration page in the AWS Control Tower console, continuing from the previous page. It shows the 'Log configuration for Amazon S3 - optional' section with an 'Info' link. It states: 'In these two fields, enter numbers that represent lifecycle retention times for the Amazon S3 logging bucket and the access logging bucket.'

There are two input fields: 'Amazon S3 bucket retention for logging' (Default: 1) and 'Format for logging' (years). Below the input fields, it states: 'Years must be expressed as integers from 1 to 15, with values up to 2 decimal places. Durations less than 1 year are expressed as days.'

Below the input fields, there is a section titled 'Amazon S3 bucket retention for access logging' (Default: 10) and 'Format for access logging' (years). Below the input fields, it states: 'Years must be expressed as integers from 1 to 15, with values up to 2 decimal places. Durations less than 1 year are expressed as days.'

Below the input fields, there is a section titled 'KMS Encryption - optional' with an 'Info' link. It states: 'AWS Key Management Service (KMS) helps you to create and manage cryptographic keys, and control your resources in AWS Control Tower. To select a key, check the box. The KMS key must have permissions for AWS CloudTrail and AWS Config. Multi-region keys are not supported. [Learn more about KMS](#)'.

There is a checkbox labeled 'Enable and customize encryption settings'. Below the checkbox, it states: 'To disable encryption settings, uncheck this box.'

Below the checkbox, there is a section titled 'AWS Backup' with an 'Info' link. It states: 'AWS Backup is a fully-managed service that helps you centralize and automate data protection across AWS services, in the cloud, and on premises.'

There are two radio buttons: 'Enable AWS Backup' (not selected) and 'AWS Backup is not enabled' (selected). Below the radio buttons, it states: 'AWS Backup will be enabled on your landing zone when landing zone update is complete. There is no setup fee and cost is based on use. [View AWS Backup pricing](#)'.

At the bottom of the page, there are three buttons: 'Cancel', 'Previous', and 'Next'.

AWS Control Tower

Figure 23 – Updating Landing Zone

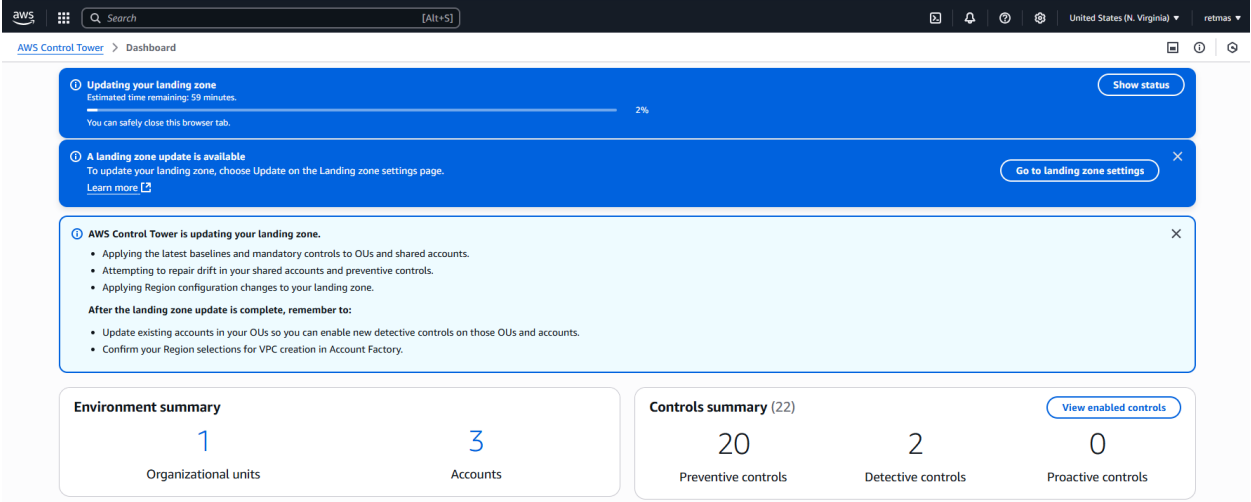
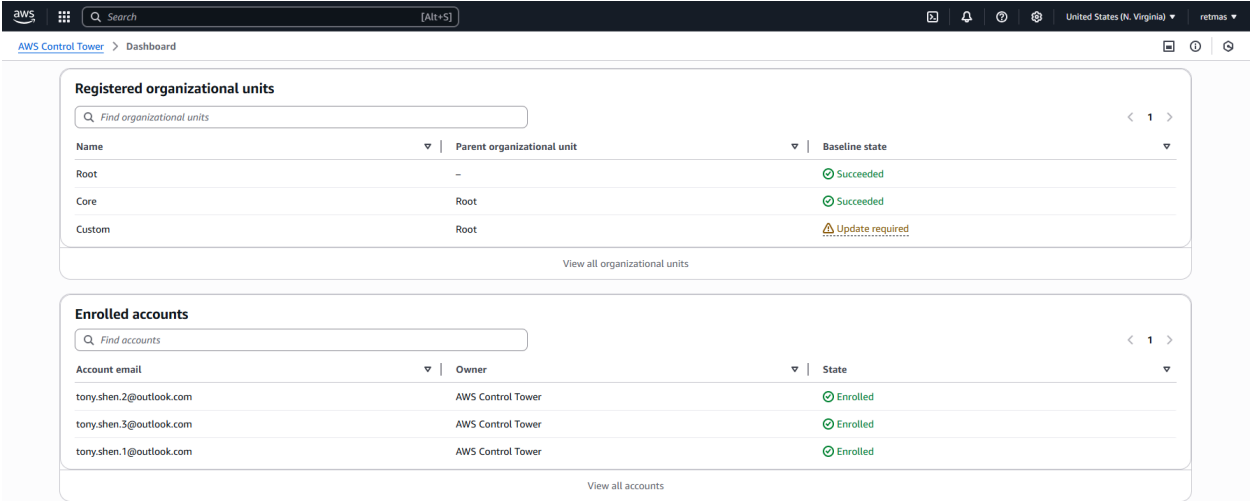


Figure 24 – Updating Landing Zone (Continued)



AWS Control Tower

Figure 25 – Updating Landing Zone Status

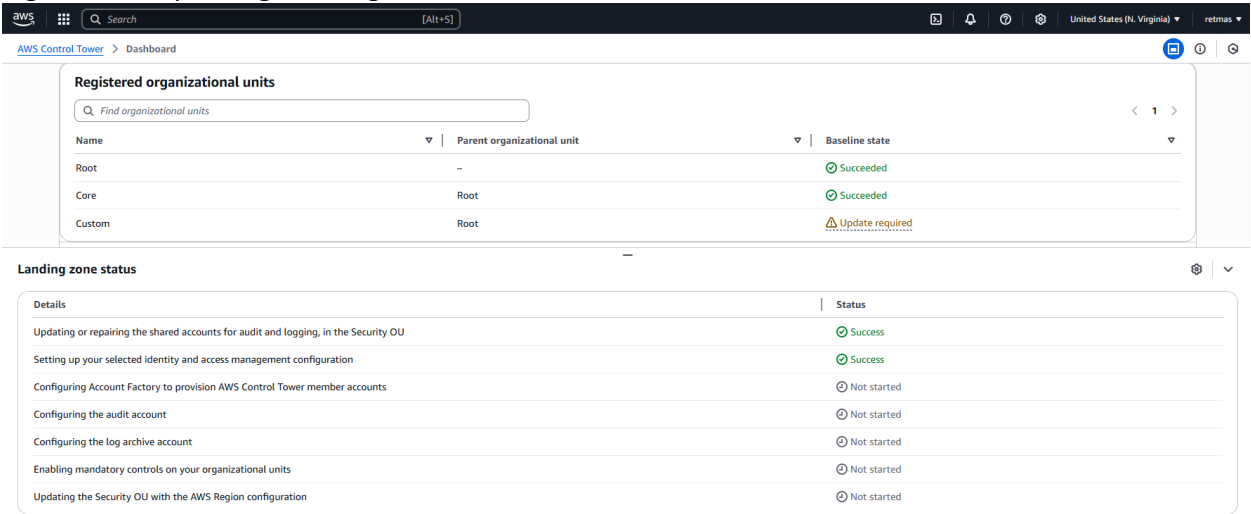
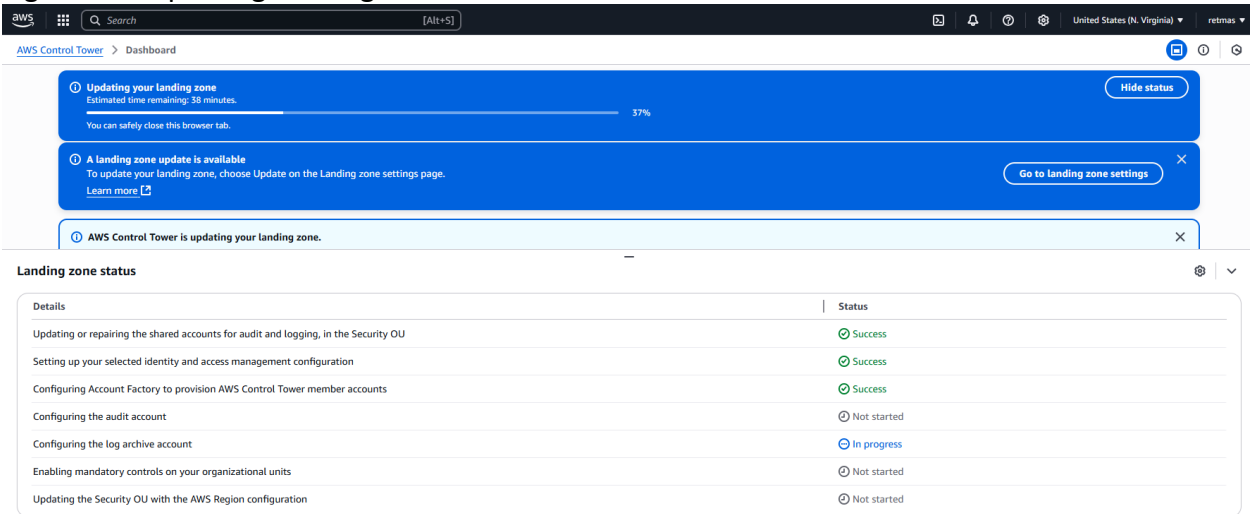
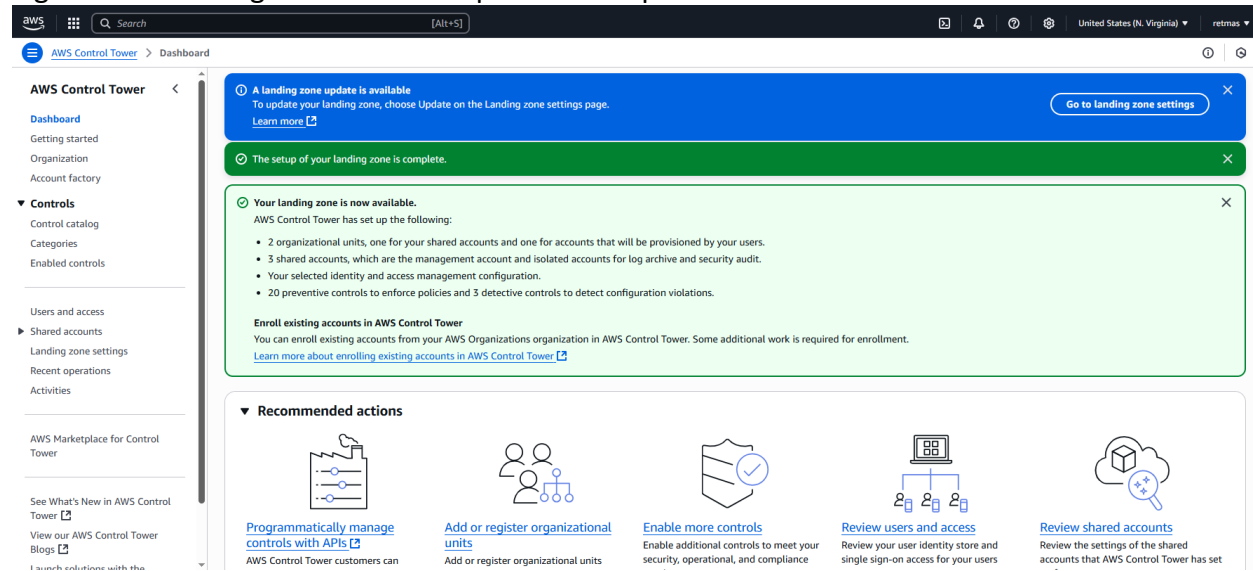


Figure 26 - Updating Landing Zone Status



AWS Control Tower

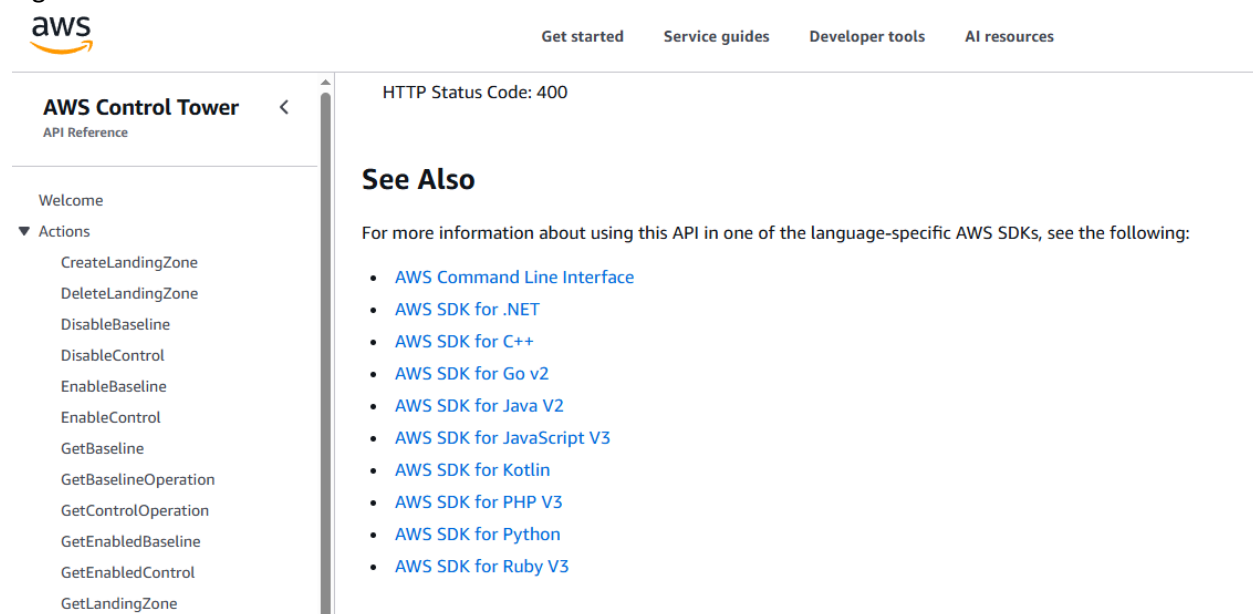
Figure 27 – Landing Zone Status – Update is complete



Control Tower API

Control Tower can be used by code with Control Tower API. Control Tower exposes its API in several forms, including Restful API calls and AWS Command Line Interface (CLI). See Figure 28 – Control Tower API below

Figure 28 – Control Tower API



Let's see how to work with Control Tower API by AWS CLI on a Linux host.

AWS Control Tower

Here below is an example of installing AWS CLI on a Ubuntu 22 host

Install and update AWS CLI on a Linux host

```
tshen@ubun221016:~$  
curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"  
unzip awscliv2.zip  
sudo ./aws/install --bin-dir /usr/local/bin --install-dir /usr/local/aws-cli --update  
...  
inflating: aws/dist/awscli/data/ac.index  
inflating: aws/dist/awscli/data/metadata.json  
You can now run: /usr/local/bin/aws --version  
tshen@ubun221016:~$ which aws  
/usr/local/bin/aws  
tshen@ubun221016:~$
```

Obtain Access Key and Secret Key for AWS CLI to access Control Tower

Sign in AWS with your Organization Root account credentials. Navigate to IAM to create Access Key and Secret Key of the user. See below Figure 28 through 31.

Figure 29 – Create Access Key

The screenshot shows the AWS IAM console interface. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, and Access reports. The main content area displays the 'Users' page for the user 'retmasadmin'. It includes sections for Console sign-in link, Console password, Last console sign-in, Multi-factor authentication (MFA) status, and Access keys. The Access keys section shows a single key with ID AKIA4UGQDEAQJEH7WWTI, which is active and was created 2012 days ago.

Type	Identifier	Certifications	Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment.			

Description	Status	Created	Last used service
AKIA4UGQDEAQJEH7WWTI	Active	2012 days ago	N/A

AWS Control Tower

Figure 30 – Create Access Key (Continued)

The screenshot shows the AWS IAM console interface for creating an access key. The breadcrumb trail is IAM > Users > retmasadmin > Create access key. A progress bar on the left indicates Step 1 (selected), Step 2 (optional), and Step 3. The main heading is 'Access key best practices & alternatives' with an 'Info' link. Below the heading is a warning: 'Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.' A 'Use case' section contains five radio buttons: 'Command Line Interface (CLI)' (selected), 'Local code', 'Application running on an AWS compute service', 'Third-party service', and 'Application running outside AWS'. Below this is a yellow box titled 'Alternatives recommended' with two bullet points: 'Use AWS CloudShell, a browser-based CLI, to run commands. Learn more' and 'Use the AWS CLI V2 and enable authentication through a user in IAM Identity Center. Learn more'. A 'Confirmation' section at the bottom has a checked checkbox: 'I understand the above recommendation and want to proceed to create an access key.'

Figure 31 – Create Access Key (Continued)

The screenshot shows the second step of the 'Create access key' process: 'Set description tag - optional'. The breadcrumb trail remains the same. The progress bar now highlights Step 2. The heading is 'Set description tag - optional' with an 'Info' link. A note states: 'The description for this access key will be attached to this user as a tag and shown alongside the access key.' Below this is a text input field labeled 'Description tag value' with the placeholder text 'retmaster access key'. A note below the field says: 'Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: _ . / ~ = + - @'. At the bottom are three buttons: 'Cancel', 'Previous', and 'Create access key'.

Figure 32 - Access Key created

The screenshot shows the third and final step: 'Retrieve access keys'. A green banner at the top states: 'Access key created. This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.' The breadcrumb trail is the same. The progress bar highlights Step 3. The heading is 'Retrieve access keys' with an 'Info' link. A note says: 'If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.' Below this is a table with two columns: 'Access key' and 'Secret access key'. The 'Access key' column contains the value 'AKIA4UGQDEAQP53BL6ZO'. The 'Secret access key' column contains a masked value '*****' with a 'Show' link. Below the table is a section titled 'Access key best practices' with four bullet points: 'Never store your access key in plain text, in a code repository, or in code.', 'Disable or delete access key when no longer needed.', 'Enable least-privilege permissions.', and 'Rotate access keys regularly.' A note at the bottom says: 'For more details about managing access keys, see the best practices for managing AWS access keys.' At the bottom right are two buttons: 'Download .csv file' and 'Done'.

Configure AWS CLI with acquired Access Key and Secret Key

Return to your AWS CLI Linux host to configure your access with your acquired Access Key and Secret Key. See below Figure 32 and 33

Figure 33 – AWS CLI Access Configuration

```
Using username "tshen".
tshen@192.168.0.18's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-57-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

113 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

New release '24.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

*** System restart required ***
Last login: Sun Jul  6 12:42:54 2025 from 192.168.0.4
tshen@ubun221016:~$ aws configure
AWS Access Key ID [None]: AKIA4UGQDEAQP53BL6ZC
```

Figure 34 – AWS CLI Access Configuration (Continued)

```
Start page X | tshen@ubun221016: ~ X | tshen@ubun221016: ~ X |
Using username "tshen".
tshen@192.168.0.18's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-57-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

113 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

New release '24.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

*** System restart required ***
Last login: Sun Jul  6 12:42:54 2025 from 192.168.0.4
tshen@ubun221016:~$ aws configure
AWS Access Key ID [None]: AKIA4UGQDEAQP53BL6ZC
AWS Secret Access Key [None]: 60[REDACTED]KF
```

Verify AWS CLI access by listing your Organization's accounts

List Organization accounts by AWS CLI

Figure 35 – List Organization Accounts

```
tshen@ubun221016:~$ aws organizations list-accounts
{
  "Accounts": [
    {
      "Id": "165811858591",
      "Arn": "arn:aws:organizations::868019806240:account/o-ok9p95k8zs/165811858591",
      "Email": "tony.shen.2@outlook.com",
      "Name": "retlog",
      "Status": "ACTIVE",
      "JoinedMethod": "CREATED",
      "JoinedTimestamp": "2019-12-29T22:21:51.278000-06:00"
    },
    {
      "Id": "415023494882",
      "Arn": "arn:aws:organizations::868019806240:account/o-ok9p95k8zs/415023494882",
      "Email": "jane.chen.1@outlook.com",
      "Name": "retdev",
      "Status": "ACTIVE",
      "JoinedMethod": "CREATED",
      "JoinedTimestamp": "2020-01-02T15:41:07.739000-06:00"
    },
    {
      "Id": "833803968598",
      "Arn": "arn:aws:organizations::868019806240:account/o-ok9p95k8zs/833803968598",
      "Email": "tony.shen.3@outlook.com",
      "Name": "retaud",
      "Status": "ACTIVE",
      "JoinedMethod": "CREATED",
      "JoinedTimestamp": "2019-12-29T22:22:22.548000-06:00"
    },
    {
      "Id": "868019806240",
      "Arn": "arn:aws:organizations::868019806240:account/o-ok9p95k8zs/868019806240",
      "Email": "tony.shen.1@outlook.com",
      "Name": "retmas",
      "Status": "ACTIVE",
      "JoinedMethod": "INVITED",
      "JoinedTimestamp": "2019-12-29T22:21:22.563000-06:00"
    }
  ]
}
tshen@ubun221016:~$ █
```

List Control Tower enabled baselines

```
tshen@ubun221016:~$ aws controltower list-enabled-baselines
```

```
{
  "enabledBaselines": [
    {
      "arn": "arn:aws:controltower:us-east-1:868019806240:enabledbaseline/XAOF4TXADTI3GOISH",
      "baselineIdentifier": "arn:aws:controltower:us-east-1::baseline/LN25R72TTG6IGPTQ",
      "statusSummary": {
        "status": "SUCCEEDED"
      },
      "targetIdentifier": "arn:aws:organizations::868019806240:account/o-ok9p95k8zs/868019806240"
    },
    {

```

AWS Control Tower

```
    "arn": "arn:aws:controltower:us-east-1:868019806240:enabledbaseline/XAN0EYP42BA3GOIVV",
    "baselineIdentifier": "arn:aws:controltower:us-east-1::baseline/4T4HA1KMO10S6311",
    "statusSummary": {
      "status": "SUCCEEDED"
    },
    "targetIdentifier": "arn:aws:organizations::868019806240:account/o-ok9p95k8zs/833803968598"
  },
  {
    "arn": "arn:aws:controltower:us-east-1:868019806240:enabledbaseline/XAFHJLGX98L3GOIU0",
    "baselineIdentifier": "arn:aws:controltower:us-east-1::baseline/J8HX46AHS5MIKQPD",
    "statusSummary": {
      "status": "SUCCEEDED"
    },
    "targetIdentifier": "arn:aws:organizations::868019806240:account/o-ok9p95k8zs/165811858591"
  },
  {
    "arn": "arn:aws:controltower:us-east-1:868019806240:enabledbaseline/XO60S75UJ2D3GOIS4",
    "baselineIdentifier": "arn:aws:controltower:us-east-1::baseline/17BSJV3IGJ2QSGA2",
    "baselineVersion": "1.0",
    "driftStatusSummary": {
      "types": {
        "inheritance": {
          "status": "DRIFTED"
        }
      }
    },
    "statusSummary": {
      "status": "SUCCEEDED"
    },
    "targetIdentifier": "arn:aws:organizations::868019806240:ou/o-ok9p95k8zs/ou-hdy3-pjbqod2l"
  }
]
```

List Control Tower enabled controls

```
tshen@ubun221016:~$ aws controltower list-enabled-controls
{
```

```
"enabledControls": [  
  {  
    "arn": "arn:aws:controltower:us-east-  
1:868019806240:enabledcontrol/RWXUO84XGVPQFJBK",  
    "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-  
GR_IAM_ROLE_CHANGE_PROHIBITED",  
    "driftStatusSummary": {  
      "driftStatus": "NOT_CHECKING"  
    },  
    "statusSummary": {  
      "status": "SUCCEEDED"  
    }  
  },  
  {  
    "arn": "arn:aws:controltower:us-east-  
1:868019806240:enabledcontrol/RWXUO6PUE7VZJUDT",  
    "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-  
GR_CLOUDWATCH_EVENTS_CHANGE_PROHIBITED",  
    "driftStatusSummary": {  
      "driftStatus": "NOT_CHECKING"  
    },  
    "statusSummary": {  
      "status": "SUCCEEDED"  
    }  
  },  
  {  
    "arn": "arn:aws:controltower:us-east-  
1:868019806240:enabledcontrol/1DMKTYDCJI7NRVLT",  
    "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-  
GR_CONFIG_AGGREGATION_CHANGE_PROHIBITED",  
    "driftStatusSummary": {  
      "driftStatus": "NOT_CHECKING"  
    },  
    "statusSummary": {  
      "status": "SUCCEEDED"  
    }  
  },  
  {  
    "arn": "arn:aws:controltower:us-east-  
1:868019806240:enabledcontrol/B10MNMYYORNO6YM6N",  
    "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-  
GR_CONFIG_ENABLED",  
    "driftStatusSummary": {  
      "driftStatus": "NOT_CHECKING"
```

```
    },
    "statusSummary": {
      "status": "SUCCEEDED"
    }
  },
  {
    "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/B10MNMYOQ5CQ57PS",
    "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_CONFIG_RULE_CHANGE_PROHIBITED",
    "driftStatusSummary": {
      "driftStatus": "NOT_CHECKING"
    },
    "statusSummary": {
      "status": "SUCCEEDED"
    }
  },
  {
    "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/1DMK6J0GJ4BOD4IM",
    "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_CONFIG_CHANGE_PROHIBITED",
    "driftStatusSummary": {
      "driftStatus": "NOT_CHECKING"
    },
    "statusSummary": {
      "status": "SUCCEEDED"
    }
  },
  {
    "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/RWXUO9ERFPGTXXAC",
    "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_SNS_CHANGE_PROHIBITED",
    "driftStatusSummary": {
      "driftStatus": "NOT_CHECKING"
    },
    "statusSummary": {
      "status": "SUCCEEDED"
    }
  },
  {
    "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/RWXUO6WXZITJLTWO",
```

```
    "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_CLOUDTRAIL_VALIDATION_ENABLED",
    "driftStatusSummary": {
      "driftStatus": "NOT_CHECKING"
    },
    "statusSummary": {
      "status": "SUCCEEDED"
    }
  },
  {
    "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/RWXUO5CFFNRPI6OJ",
    "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_CLOUDTRAIL_CLOUDWATCH_LOGS_ENABLED",
    "driftStatusSummary": {
      "driftStatus": "NOT_CHECKING"
    },
    "statusSummary": {
      "status": "SUCCEEDED"
    }
  },
  {
    "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/1DMKTY9S9ZAKPOQC",
    "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_CLOUDTRAIL_CHANGE_PROHIBITED",
    "driftStatusSummary": {
      "driftStatus": "NOT_CHECKING"
    },
    "statusSummary": {
      "status": "SUCCEEDED"
    }
  },
  {
    "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/RWY7UM5IXR05YK8Z",
    "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_IAM_ROLE_CHANGE_PROHIBITED",
    "driftStatusSummary": {
      "driftStatus": "NOT_CHECKING"
    },
    "statusSummary": {
      "status": "SUCCEEDED"
    }
  }
}
```

```
    },
    {
      "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/B10MNMYOQPRDHV0Q",
      "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_CONFIG_CHANGE_PROHIBITED",
      "driftStatusSummary": {
        "driftStatus": "NOT_CHECKING"
      },
      "statusSummary": {
        "status": "SUCCEEDED"
      }
    },
    {
      "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/1DMK6IWW5OGDEJQU",
      "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_AUDIT_BUCKET_RETENTION_POLICY",
      "driftStatusSummary": {
        "driftStatus": "NOT_CHECKING"
      },
      "statusSummary": {
        "status": "SUCCEEDED"
      }
    },
    {
      "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/1DMK6ITCZZAHITKZ",
      "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_AUDIT_BUCKET_DELETION_PROHIBITED",
      "driftStatusSummary": {
        "driftStatus": "NOT_CHECKING"
      },
      "statusSummary": {
        "status": "SUCCEEDED"
      }
    },
    {
      "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/B10HG6WWMHCCJ45Q",
      "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_AUDIT_BUCKET_POLICY_CHANGES_PROHIBITED",
      "driftStatusSummary": {
        "driftStatus": "NOT_CHECKING"
```

```
    },
    "statusSummary": {
      "status": "SUCCEEDED"
    }
  },
  {
    "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/RWXUO4FAL209KVB",
    "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIBITED",
    "driftStatusSummary": {
      "driftStatus": "NOT_CHECKING"
    },
    "statusSummary": {
      "status": "SUCCEEDED"
    }
  },
  {
    "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/67BITDSDPJWAOHIQ",
    "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_LAMBDA_CHANGE_PROHIBITED",
    "driftStatusSummary": {
      "driftStatus": "NOT_CHECKING"
    },
    "statusSummary": {
      "status": "SUCCEEDED"
    }
  },
  {
    "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/1DMK6J285BLA5DB1",
    "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_CONFIG_RULE_CHANGE_PROHIBITED",
    "driftStatusSummary": {
      "driftStatus": "NOT_CHECKING"
    },
    "statusSummary": {
      "status": "SUCCEEDED"
    }
  },
  {
    "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/B10MNNCWVJYMAR6H",
```

```
    "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_LAMBDA_CHANGE_PROHIBITED",
    "driftStatusSummary": {
      "driftStatus": "NOT_CHECKING"
    },
    "statusSummary": {
      "status": "SUCCEEDED"
    }
  },
  {
    "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/RWXUO49UCPXWJPOG",
    "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED",
    "driftStatusSummary": {
      "driftStatus": "NOT_CHECKING"
    },
    "statusSummary": {
      "status": "SUCCEEDED"
    }
  },
  {
    "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/1DMK6IYOFYKVCVCP",
    "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_CLOUDTRAIL_ENABLED",
    "driftStatusSummary": {
      "driftStatus": "NOT_CHECKING"
    },
    "statusSummary": {
      "status": "SUCCEEDED"
    }
  },
  {
    "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/1DMK6ITCT9GP2ZME",
    "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_AUDIT_BUCKET_ENCRYPTION_ENABLED",
    "driftStatusSummary": {
      "driftStatus": "NOT_CHECKING"
    },
    "statusSummary": {
      "status": "SUCCEEDED"
    }
  }
}
```

```
    },
    {
      "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/B10HG8W0VYDQJAAB",
      "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_LOG_GROUP_POLICY",
      "driftStatusSummary": {
        "driftStatus": "NOT_CHECKING"
      },
      "statusSummary": {
        "status": "SUCCEEDED"
      }
    },
    {
      "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/1DMK6J0GLHXLFTN",
      "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_CONFIG_AGGREGATION_CHANGE_PROHIBITED",
      "driftStatusSummary": {
        "driftStatus": "NOT_CHECKING"
      },
      "statusSummary": {
        "status": "SUCCEEDED"
      }
    },
    {
      "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/67BLQS8HEGMHAGAY",
      "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_CLOUDTRAIL_ENABLED",
      "driftStatusSummary": {
        "driftStatus": "NOT_CHECKING"
      },
      "statusSummary": {
        "status": "SUCCEEDED"
      }
    },
    {
      "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/RWY7UJLRM3CX2F0D",
      "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_CLOUDTRAIL_CLOUDWATCH_LOGS_ENABLED",
      "driftStatusSummary": {
        "driftStatus": "NOT_CHECKING"
```

```
    },
    "statusSummary": {
      "status": "SUCCEEDED"
    }
  },
  {
    "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/67BITDKTWSSAAQJO",
    "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_CONFIG_AGGREGATION_AUTHORIZATION_POLICY",
    "driftStatusSummary": {
      "driftStatus": "NOT_CHECKING"
    },
    "statusSummary": {
      "status": "SUCCEEDED"
    }
  },
  {
    "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/67BLQSGXJ6GOD58R",
    "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_CONFIG_AGGREGATION_AUTHORIZATION_POLICY",
    "driftStatusSummary": {
      "driftStatus": "NOT_CHECKING"
    },
    "statusSummary": {
      "status": "SUCCEEDED"
    }
  },
  {
    "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/B10MNMKG8RJDZYL",
    "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_CLOUDTRAIL_VALIDATION_ENABLED",
    "driftStatusSummary": {
      "driftStatus": "NOT_CHECKING"
    },
    "statusSummary": {
      "status": "SUCCEEDED"
    }
  },
  {
    "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/RWY7UKBBU0YKCGAC",
```

```
    "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_CLOUDWATCH_EVENTS_CHANGE_PROHIBITED",
    "driftStatusSummary": {
      "driftStatus": "NOT_CHECKING"
    },
    "statusSummary": {
      "status": "SUCCEEDED"
    }
  },
  {
    "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/67BLQT4OMTD3EUVH",
    "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_SNS_CHANGE_PROHIBITED",
    "driftStatusSummary": {
      "driftStatus": "NOT_CHECKING"
    },
    "statusSummary": {
      "status": "SUCCEEDED"
    }
  },
  {
    "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/1DMKTYF485VWDY4B",
    "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_LOG_GROUP_POLICY",
    "driftStatusSummary": {
      "driftStatus": "NOT_CHECKING"
    },
    "statusSummary": {
      "status": "SUCCEEDED"
    }
  },
  {
    "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/67BITDSPDX8OMRQ5",
    "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_CONFIG_ENABLED",
    "driftStatusSummary": {
      "driftStatus": "NOT_CHECKING"
    },
    "statusSummary": {
      "status": "SUCCEEDED"
    }
  }
}
```

```
    },
    {
      "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/B10HG7B4O0FQECGI",
      "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_CLOUDTRAIL_CHANGE_PROHIBITED",
      "driftStatusSummary": {
        "driftStatus": "NOT_CHECKING"
      },
      "statusSummary": {
        "status": "SUCCEEDED"
      }
    },
    {
      "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/RWXUO3CC34JI8JES",
      "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_AUDIT_BUCKET_LOGGING_ENABLED",
      "driftStatusSummary": {
        "driftStatus": "NOT_CHECKING"
      },
      "statusSummary": {
        "status": "SUCCEEDED"
      }
    },
    {
      "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/B10HG8W0MECVBAQ6",
      "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_SNS_SUBSCRIPTION_CHANGE_PROHIBITED",
      "driftStatusSummary": {
        "driftStatus": "NOT_CHECKING"
      },
      "statusSummary": {
        "status": "SUCCEEDED"
      }
    },
    {
      "arn": "arn:aws:controltower:us-east-1:868019806240:enabledcontrol/B10MNNR4ZTFBF00Q",
      "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-GR_SNS_SUBSCRIPTION_CHANGE_PROHIBITED",
      "driftStatusSummary": {
        "driftStatus": "NOT_CHECKING"
```

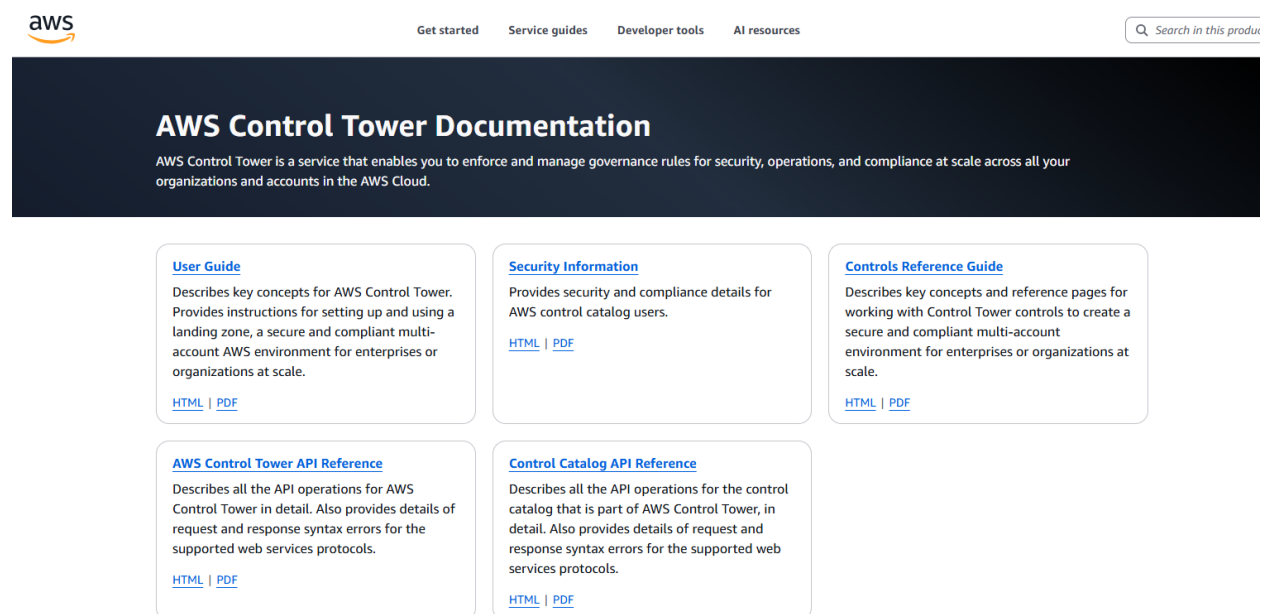
```
    },
    "statusSummary": {
      "status": "SUCCEEDED"
    }
  }
}
]
}
tshen@ubun221016:~$
```

At this point, you are fully in control over your Control Tower and your Organization, and you are ready to standardize, enhance, and fine-tune your AWS multi-account environments using Control Tower by Control Tower API as well as AWS Management Console, the GUI interface. Your choice of API, in this article, is AWS CLI for Linux, commonly used by AWS administrators and other IT professionals.

Control Tower Documentation

Control Tower Documentation consists of five documents. See Figure 35 below

Figure 36 – Control Tower Documentation



<https://docs.aws.amazon.com/controltower/>

Summary

When an enterprise or a large organization leverages AWS for its IT operations, it always has multiple AWS accounts to meet its various needs. AWS Organizations, Landing Zones, and Control Tower are all AWS services designed to help AWS customer to best manage its multi-account environments.

AWS Organizations is a service that helps centrally manage and govern multiple AWS accounts. It enables you to create a hierarchy of accounts, apply policies for security and compliance, and share resources efficiently.

AWS Landing Zone is a solution (now part of AWS Control Tower) that provides a pre-configured, secure, multi-account AWS environment based on best practices. It automates the setup of a baseline environment, helping organizations scale quickly while maintaining security and compliance.

AWS Control Tower is a service that simplifies the setup and governance of a secure, multi-account AWS environment, building on Landing Zones. It provides an orchestrated way to deploy and manage a landing zone with best practices.

In this article, we quickly toured a simple Organization that Control Tower created. We also showed how to make Control Tower API calls with AWS CLI on a Linux host, a tool commonly used by AWS administrators and other IT professionals. Please send your comments and suggestions to tshen@datacommlab.com and your feedback will be very much appreciated.

References

[AWS Control Tower User Guide](#)
[AWS Control Tower Control Catalog API](#)
[AWS Control Tower API Reference](#)
[AWS Control Tower Controls Reference Guide](#)
[AWS Control Tower Security Catalog Controls](#)