Tony Shen

AWS CONTROL TOWER

Contents

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

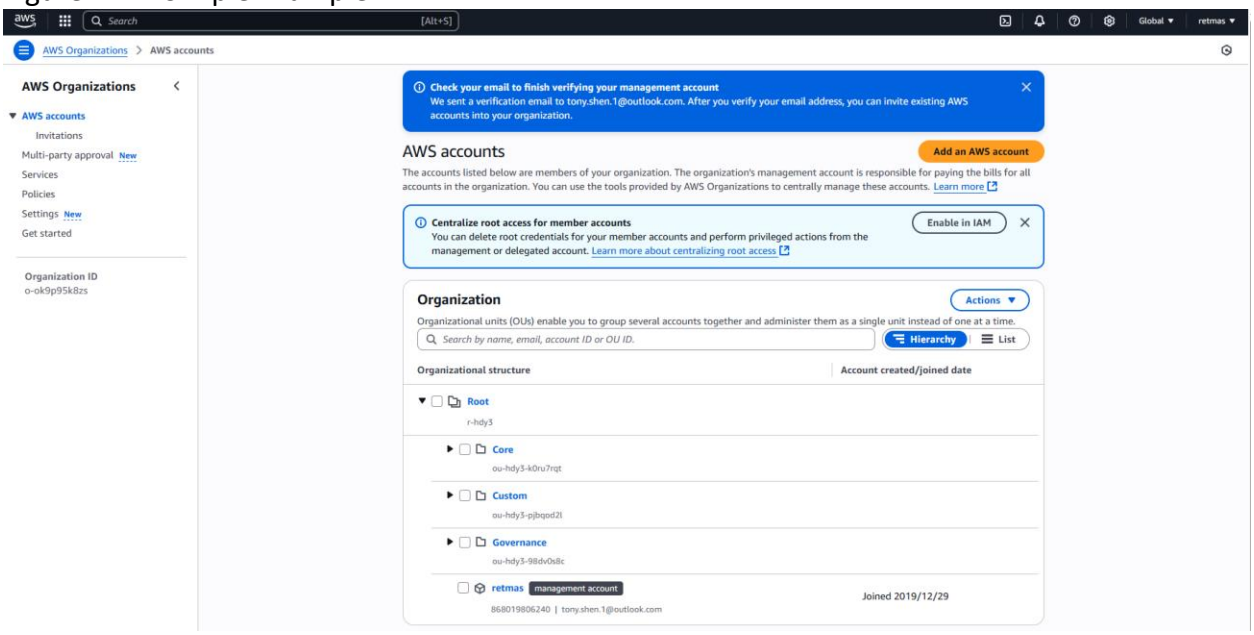
Control Tower is a service designed for creating and managing multi-account environments called AWS Organizations. Control Tower allows customer to organize multiple accounts into a logical entity Organization. Control Tower can create and manage multiple Organizations with each Organization having multiple 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.

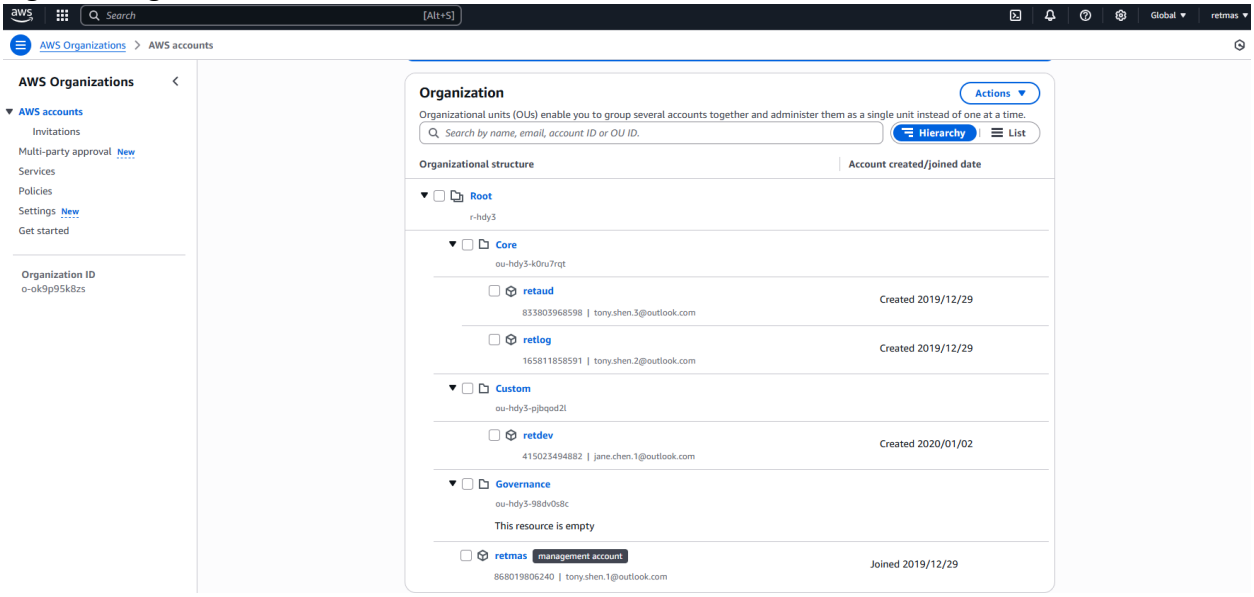
Parallel to Core, it created **Custom**, in there, reside user created AWS accounts. You can let CT create such an account for you. You can also import an existing AWS account. Those accounts are typically used to serve your business needs such as Accounting, Finance, HR, Sales, Inventory, Distribution,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

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.

Figure 3 – About Organizations

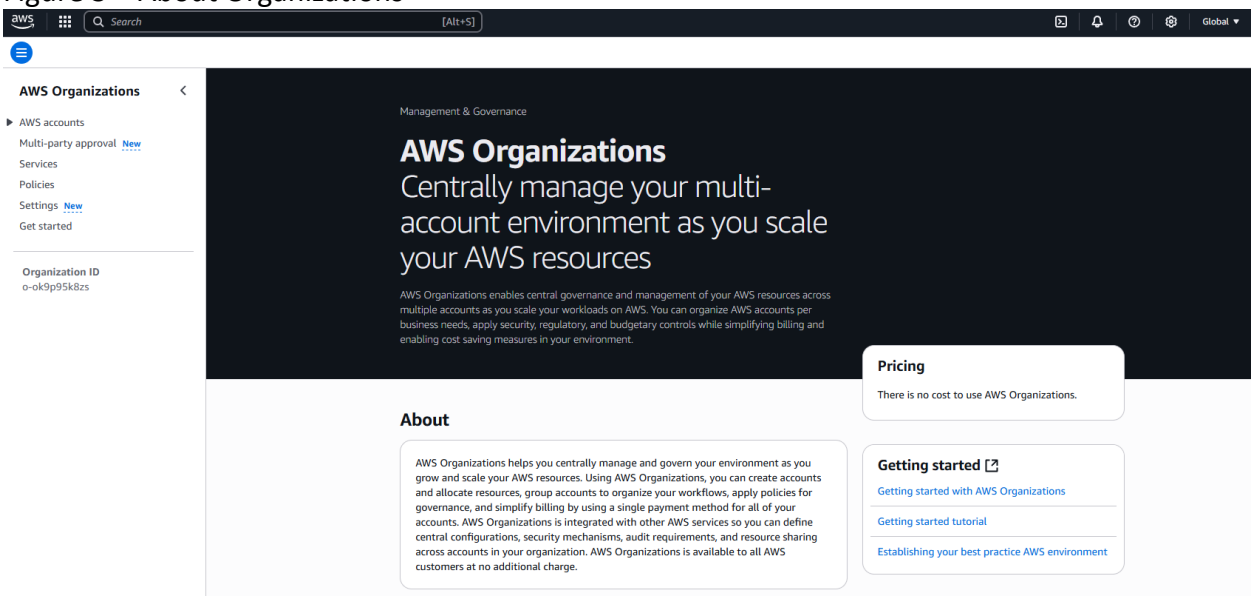


Figure 4 – How it works

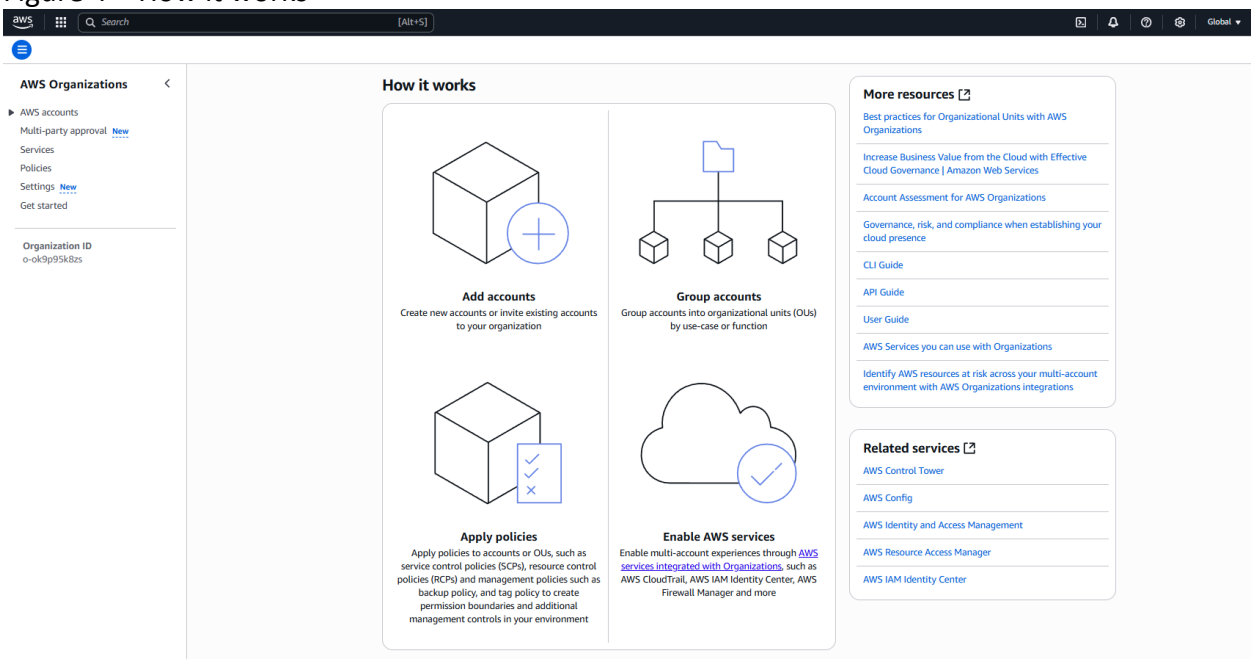


Figure 5 – Benefits and features

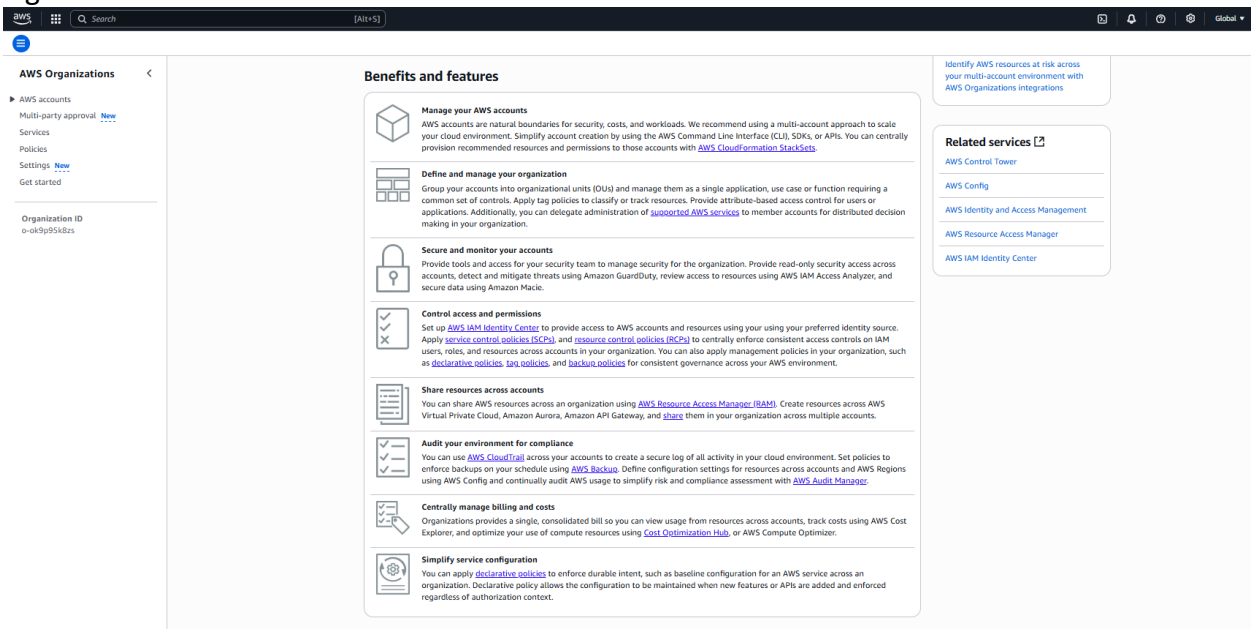


Figure 6 – Use Cases

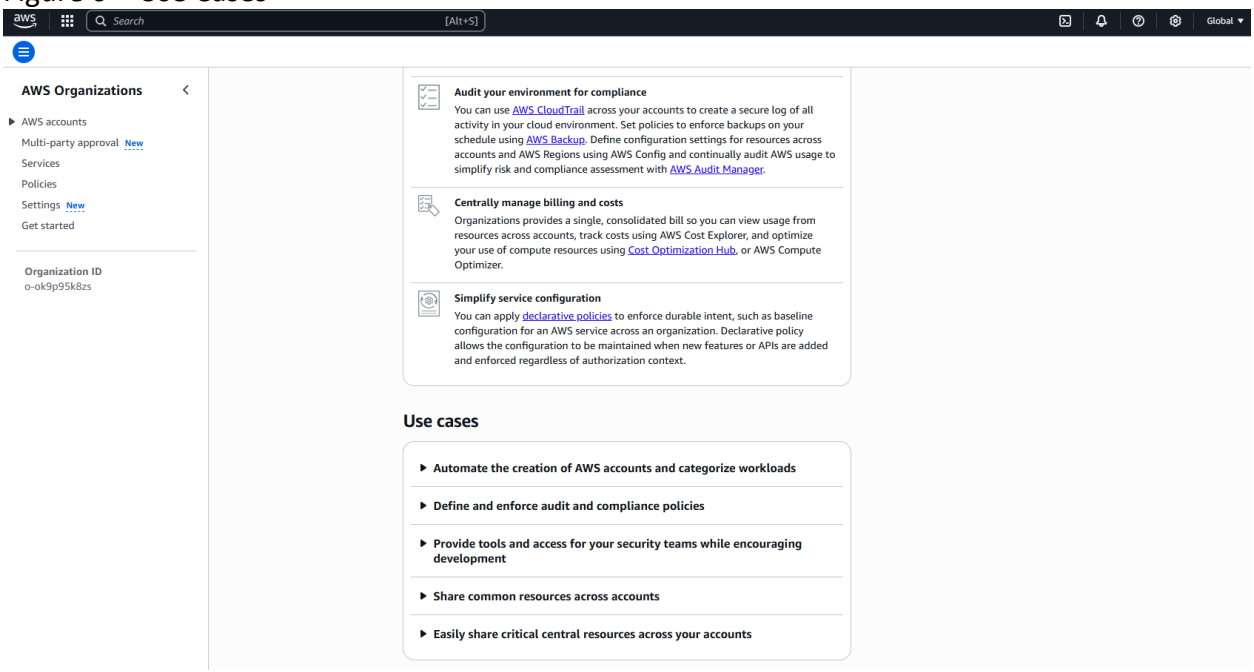


Figure 8 - Services

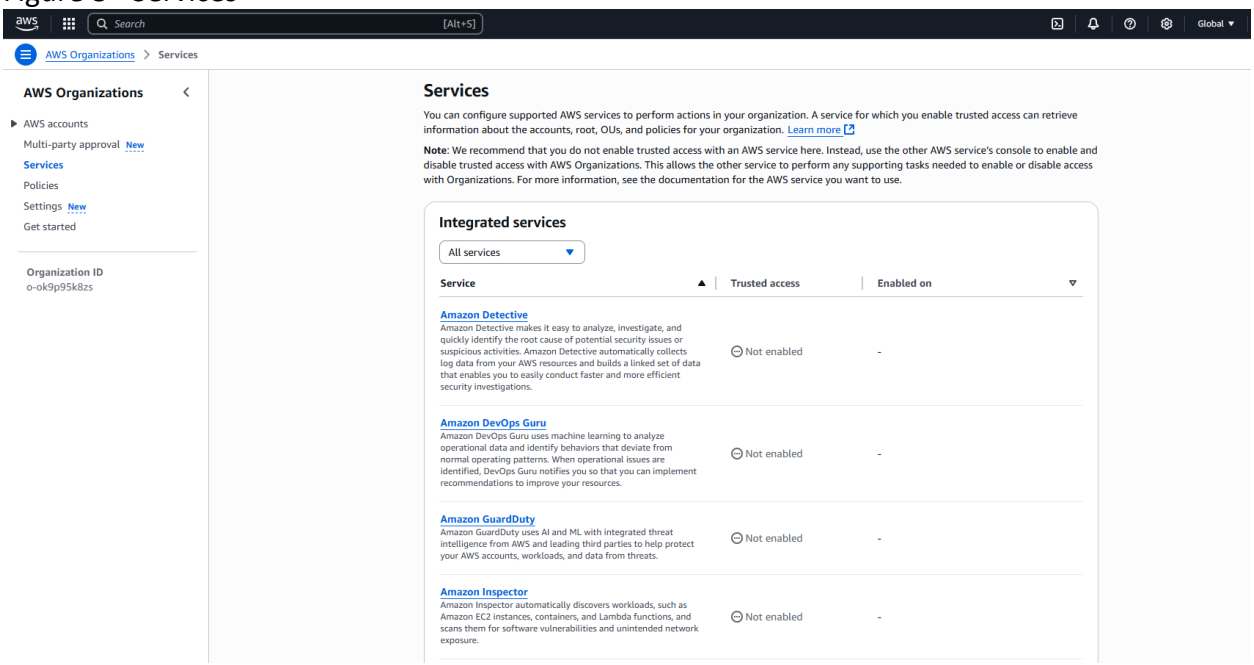


Figure 9 – Services (Continued)

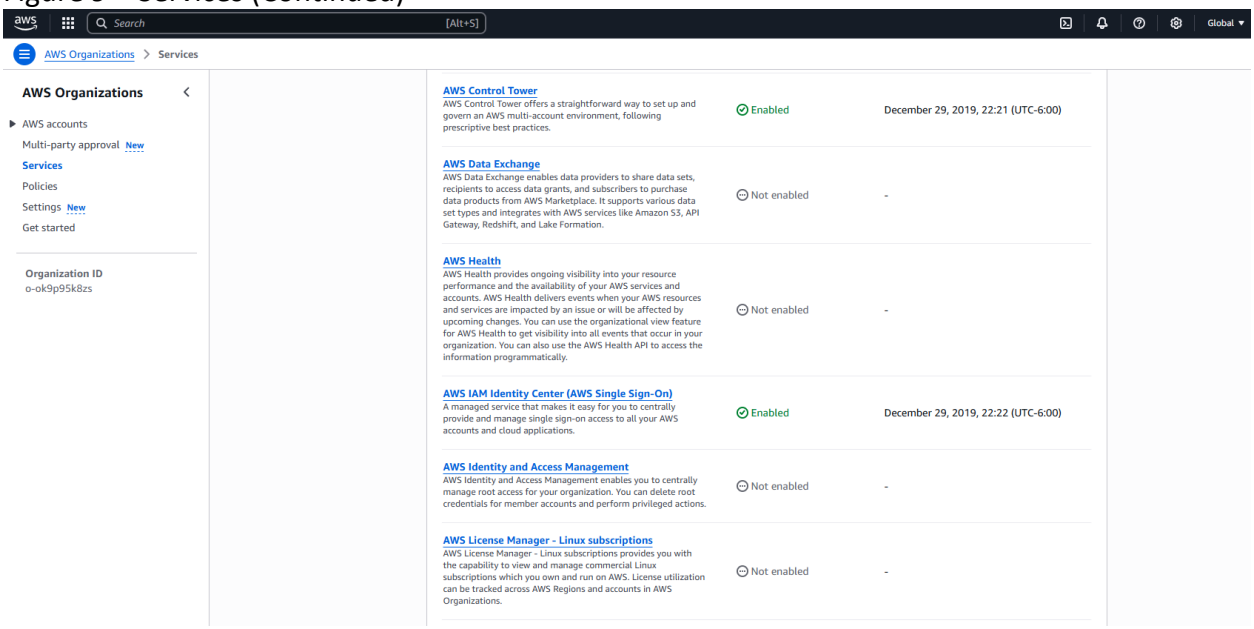


Figure 10 - Policies

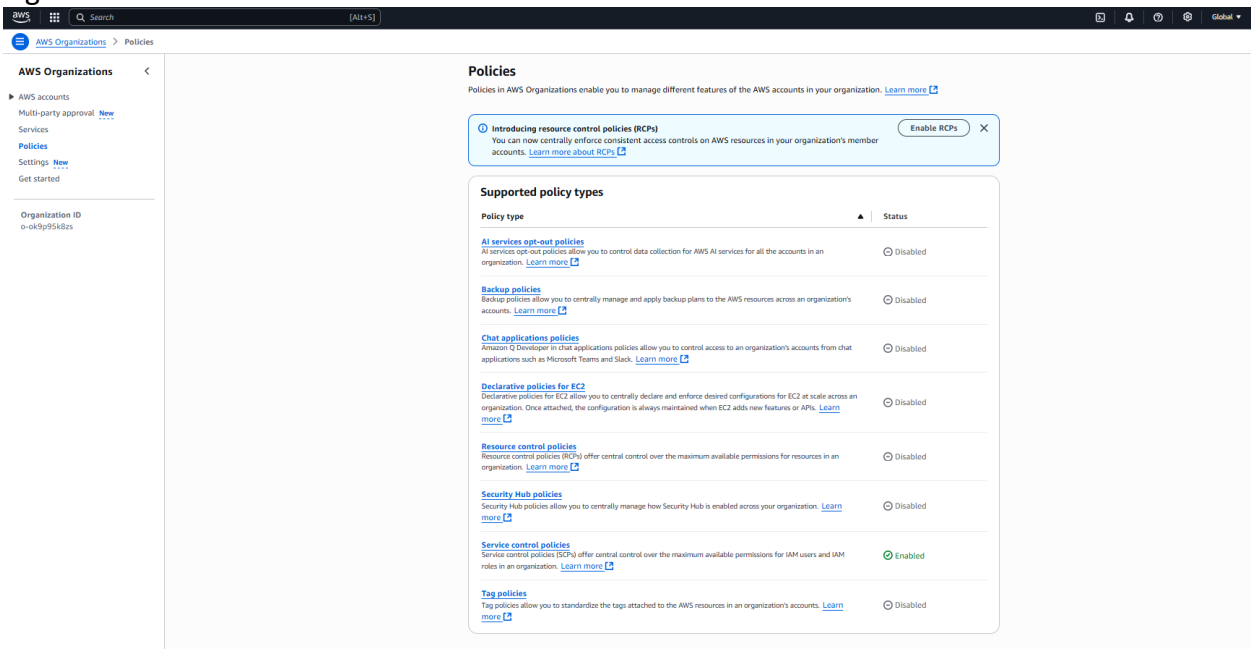


Figure 10 - Settings

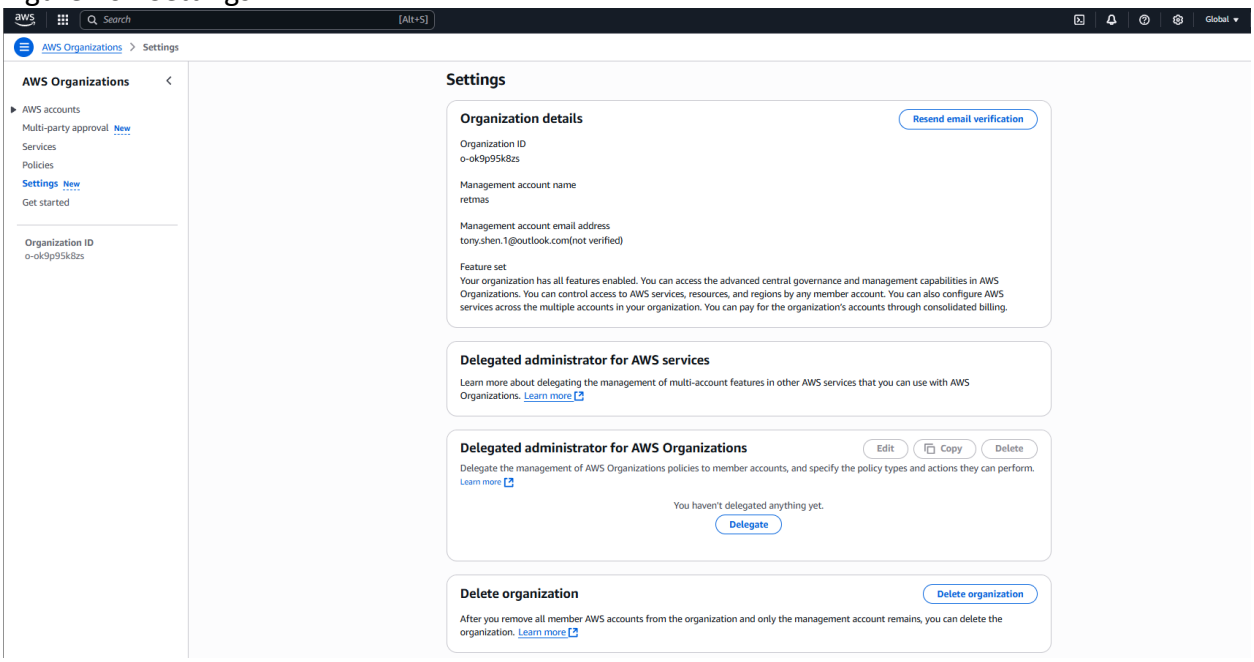
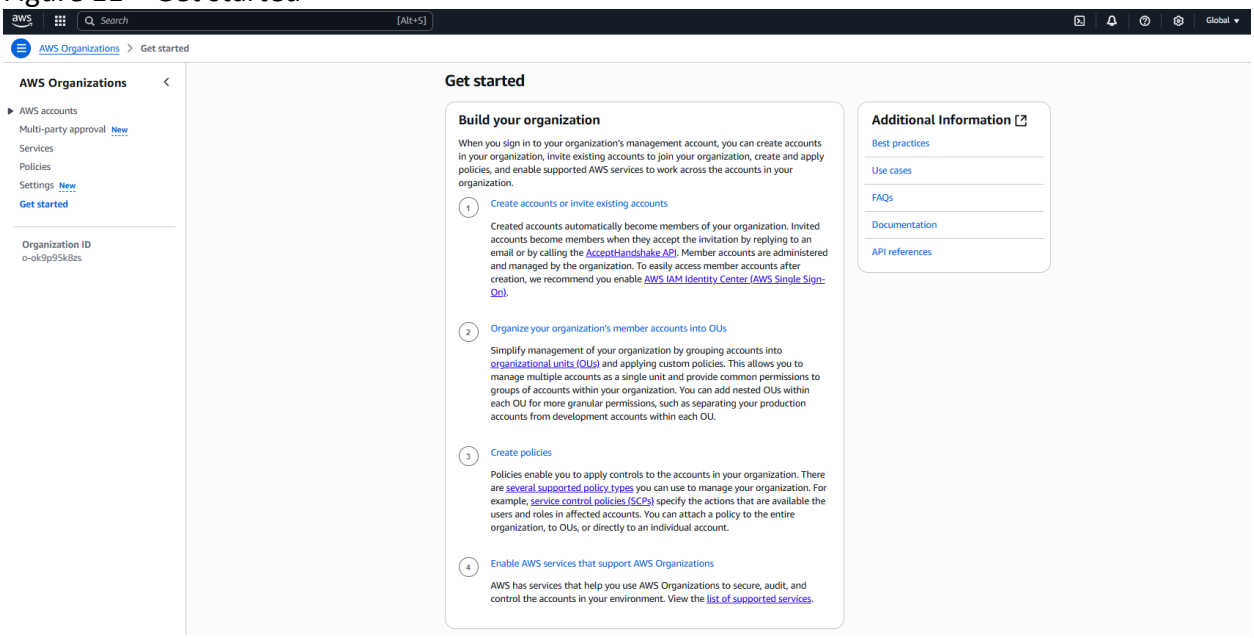


Figure 11 – Get started



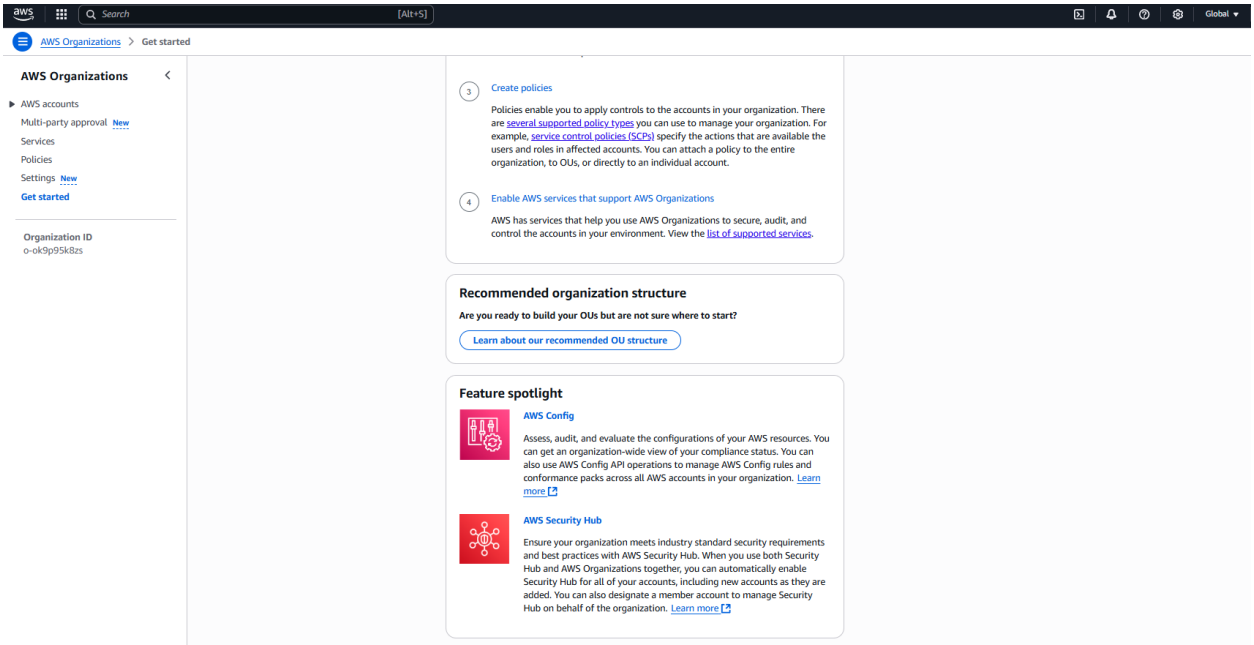
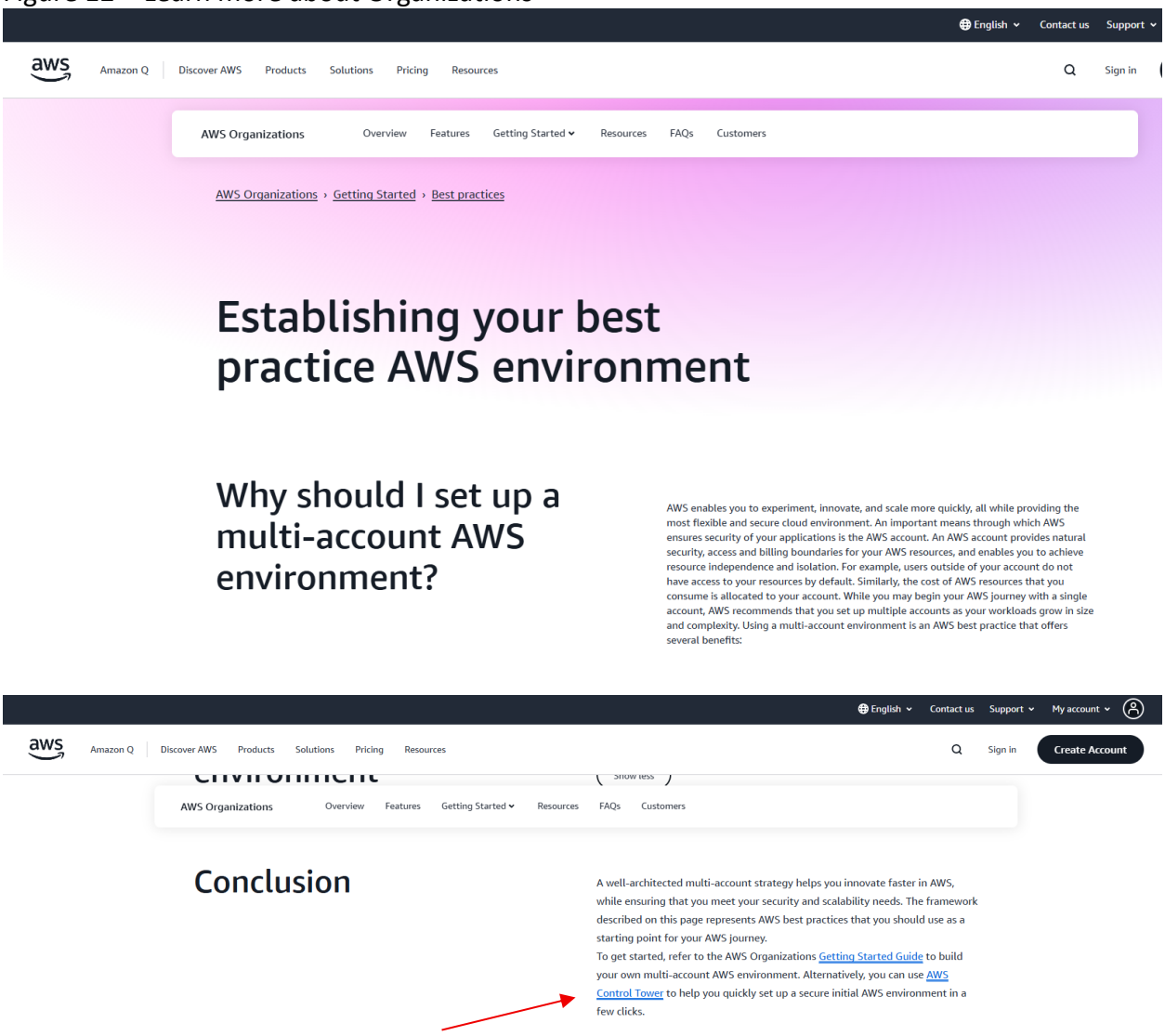


Figure 12 – Learn more about Organizations



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)

Figure 13 – Control Tower

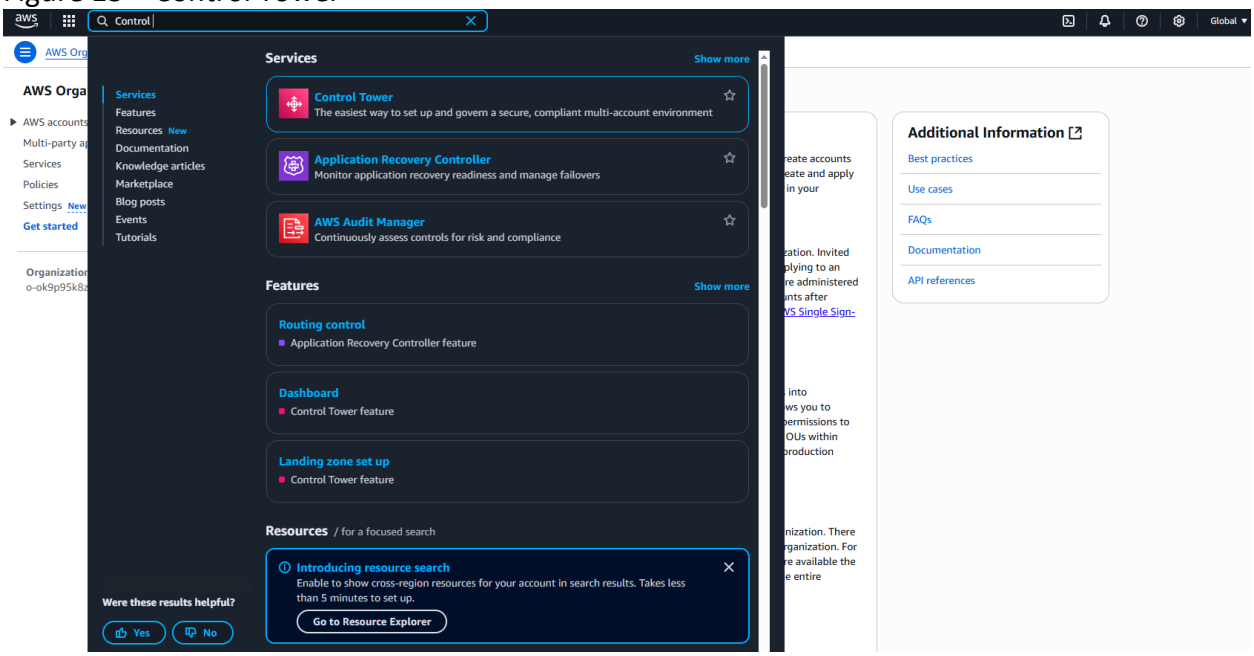


Figure 14 - Control Tower Dashboard

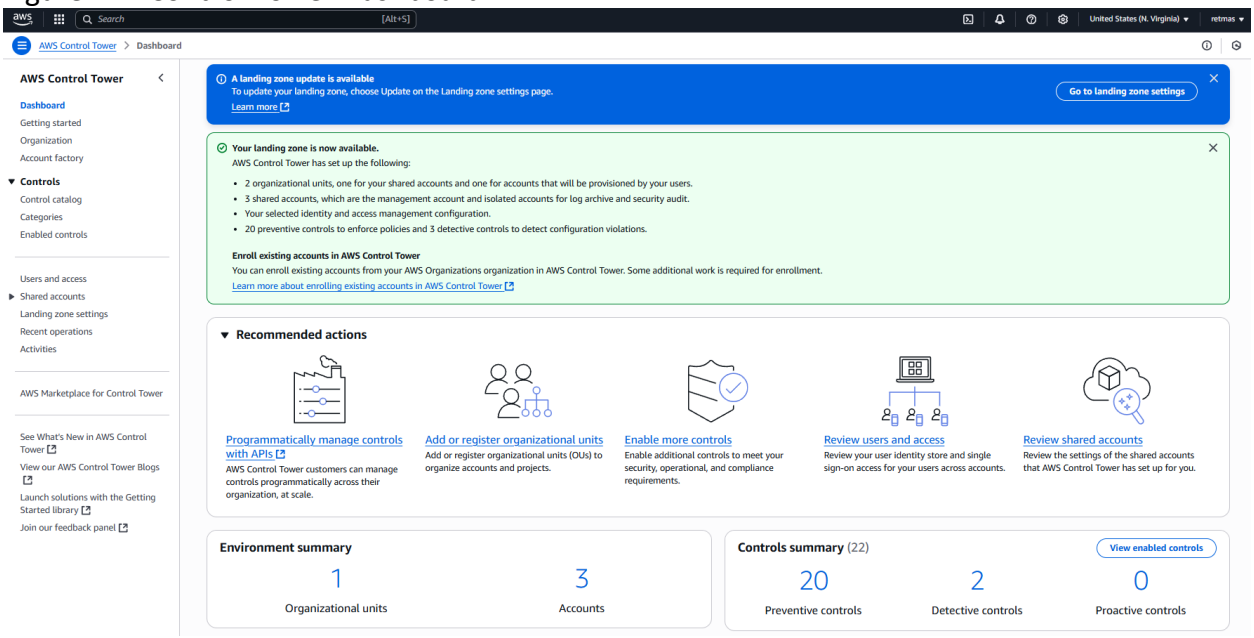


Figure 15 - Control Tower Dashboard (Continued)

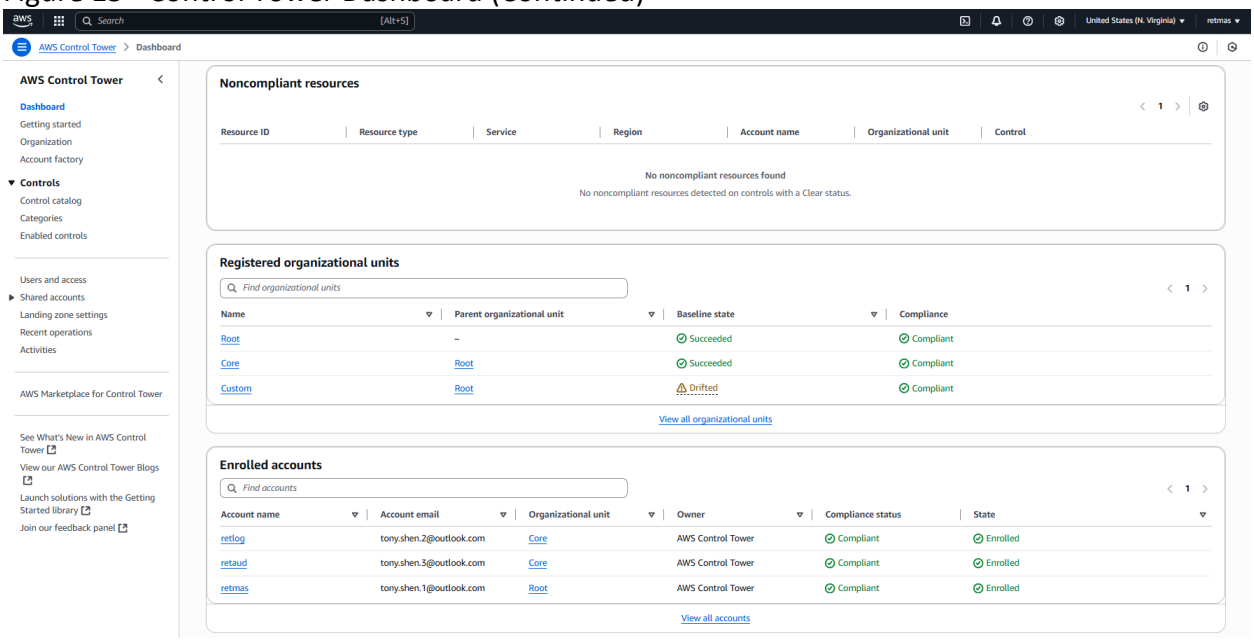
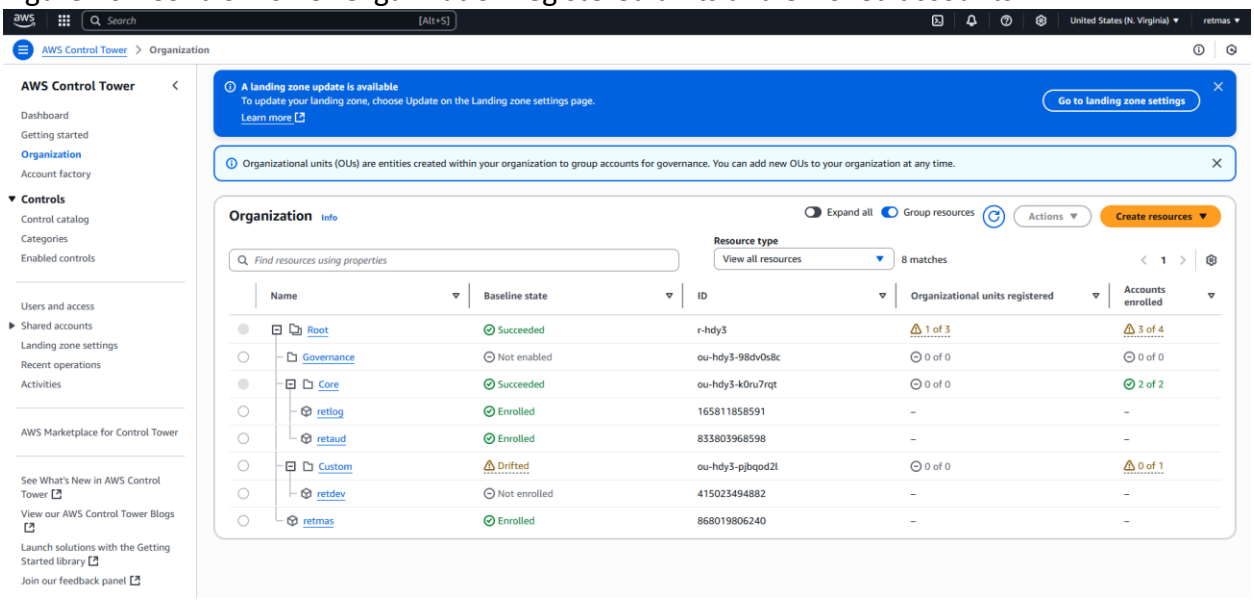


Figure 16 - Control Tower Organization registered units and enrolled accounts



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

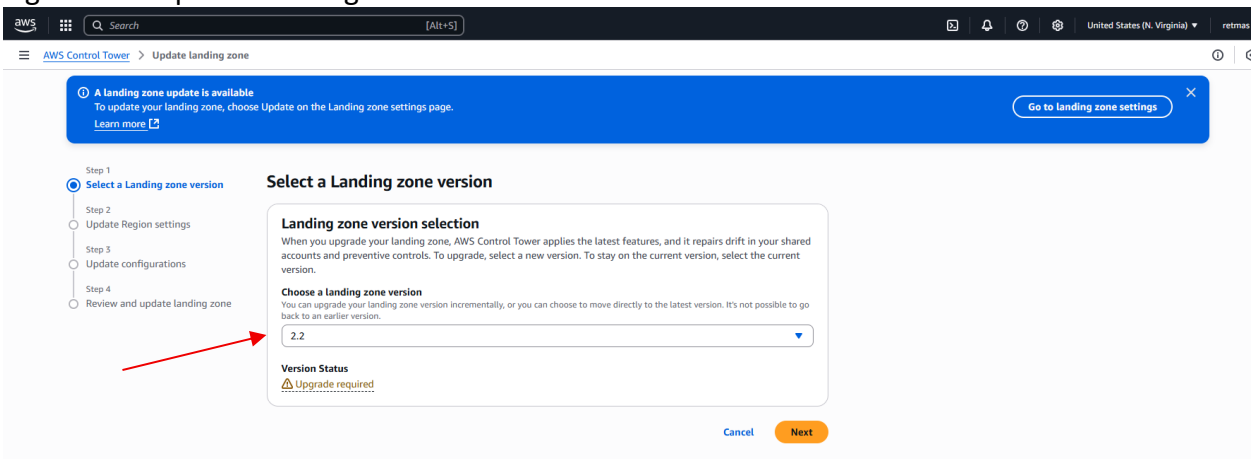
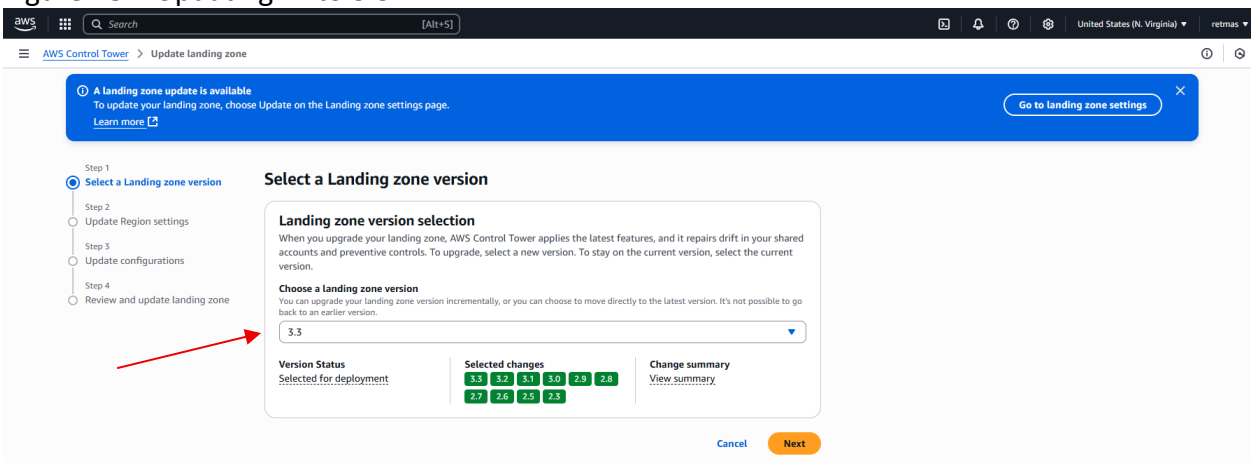


Figure 18 shows the lasted version of LZ available for you to update to.

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

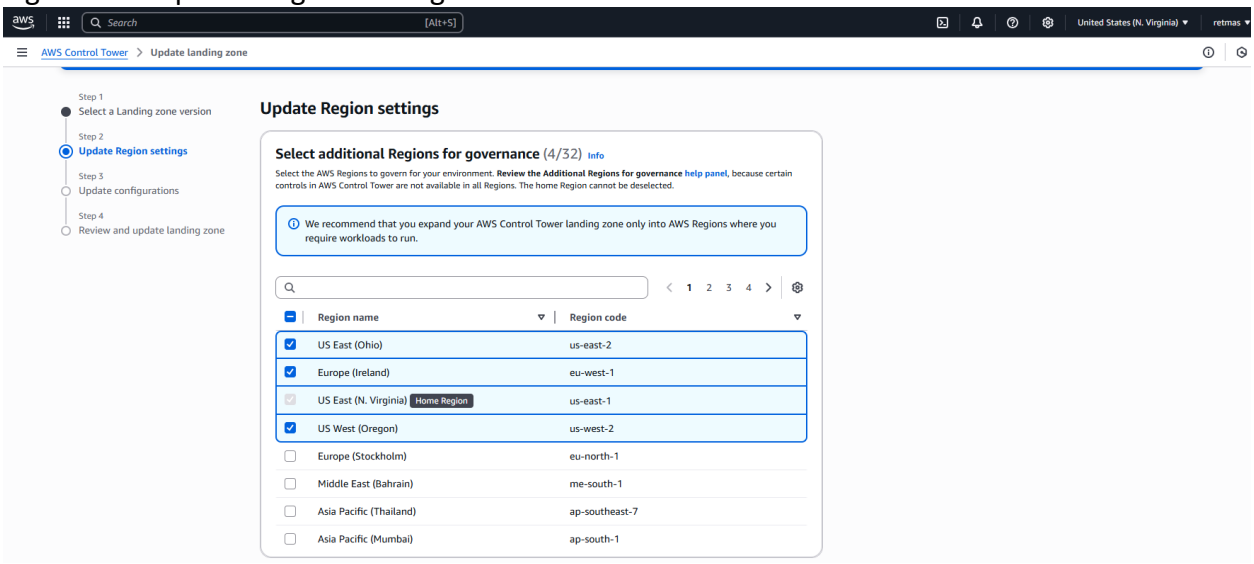


Figure 20 – Update configurations

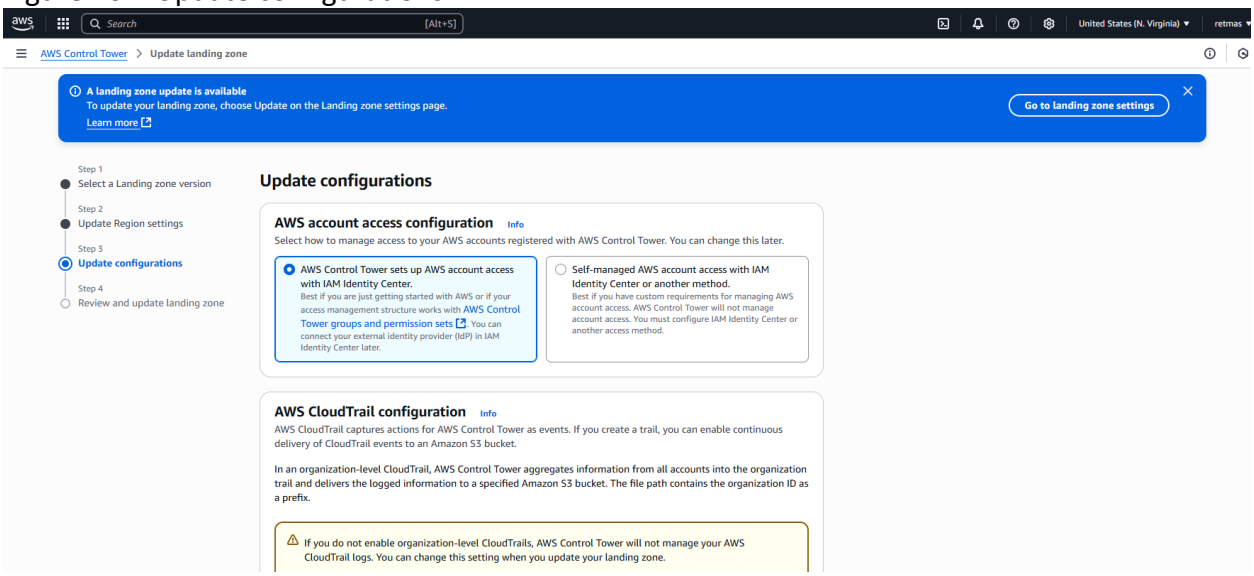


Figure 21 – Update configurations for CloudTrail

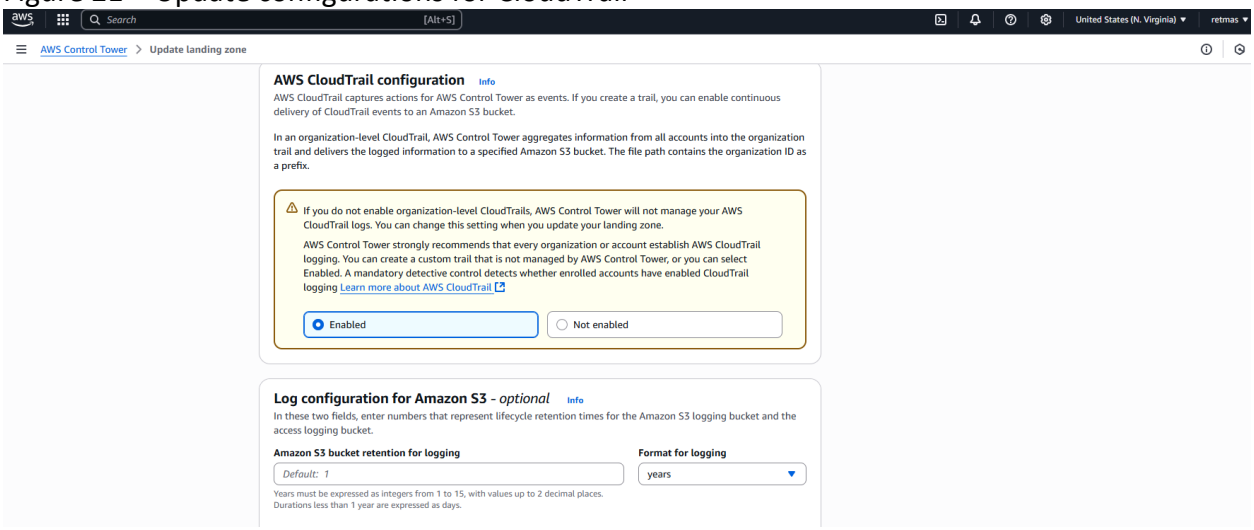


Figure 22 - Update configurations for CloudTrail (Continued)

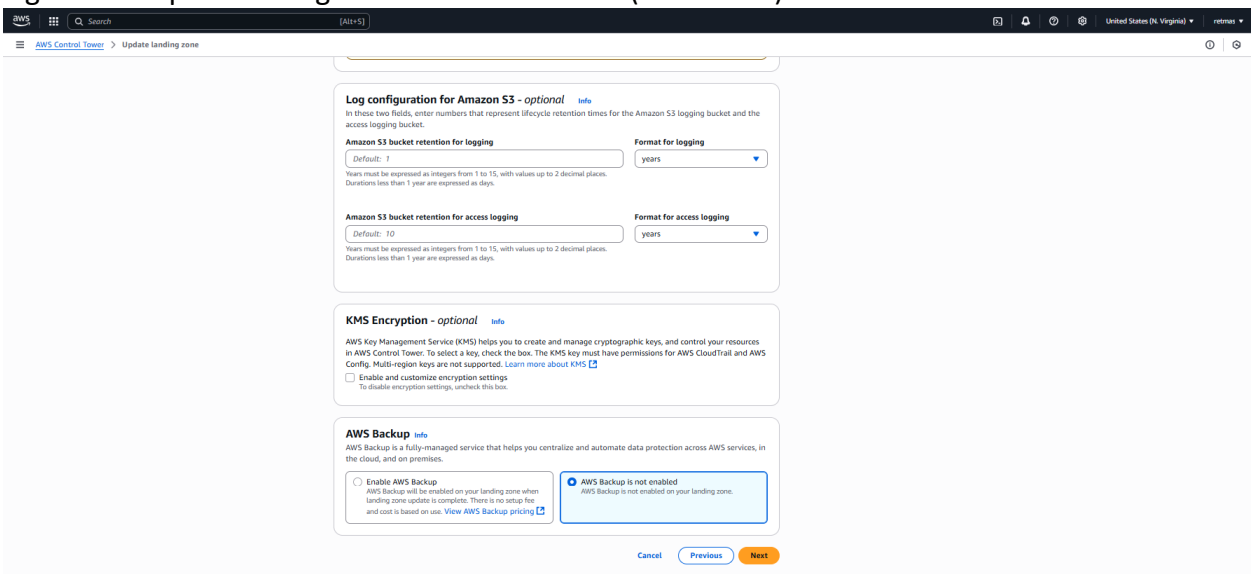


Figure 23 – Updating Landing Zone

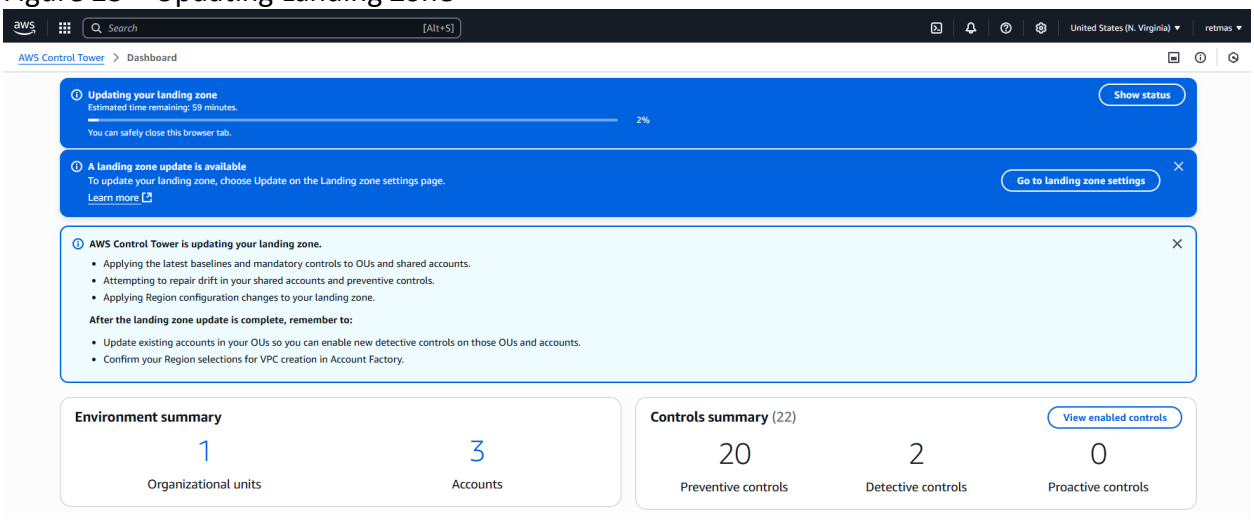


Figure 24 – Updating Landing Zone (Continued)

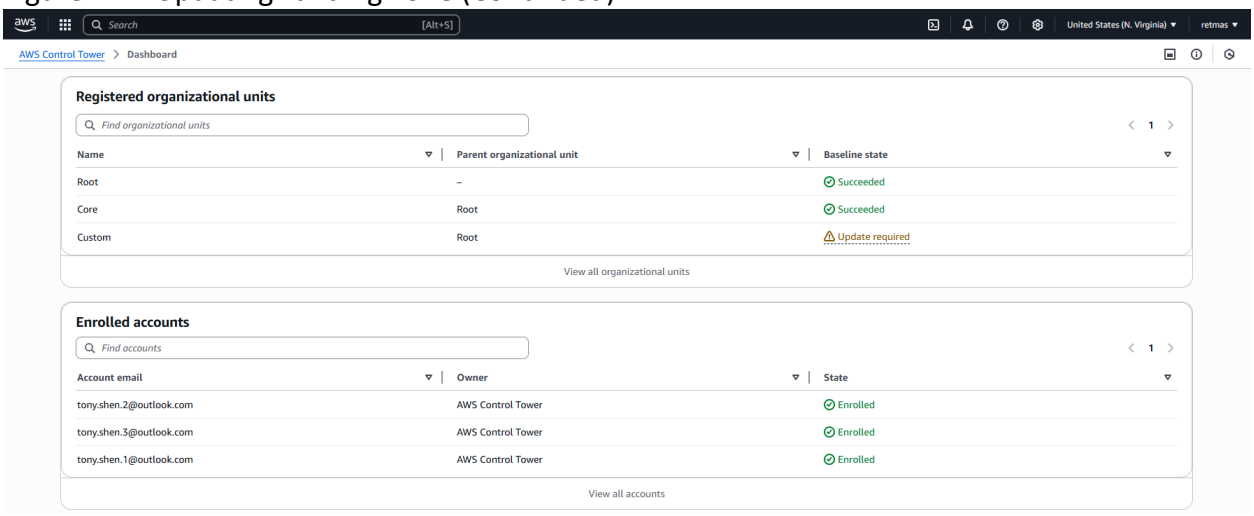


Figure 25 – Updating Landing Zone Status

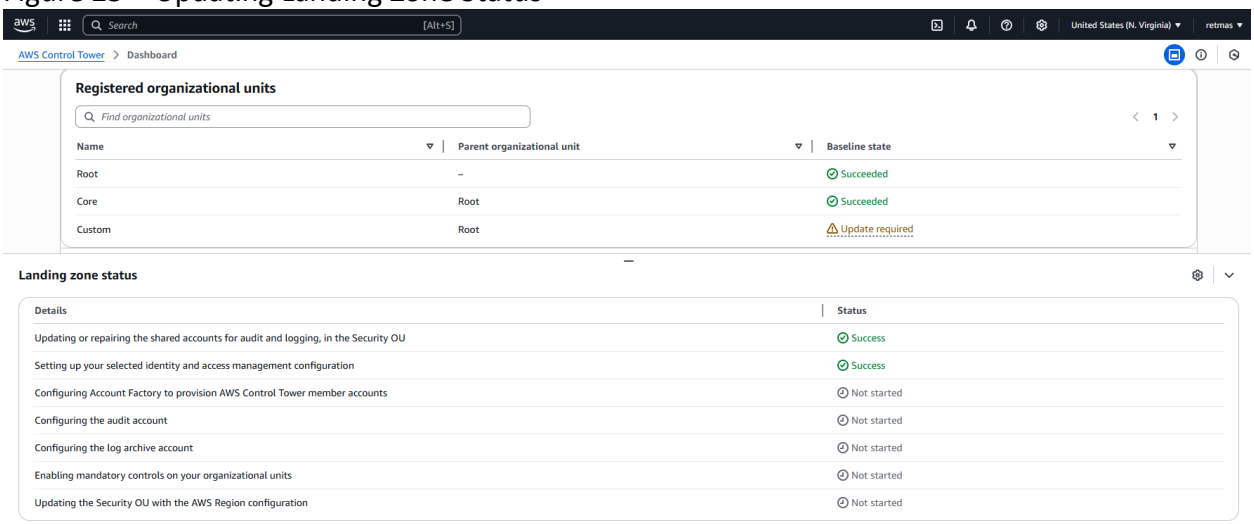


Figure 26 - Updating Landing Zone Status

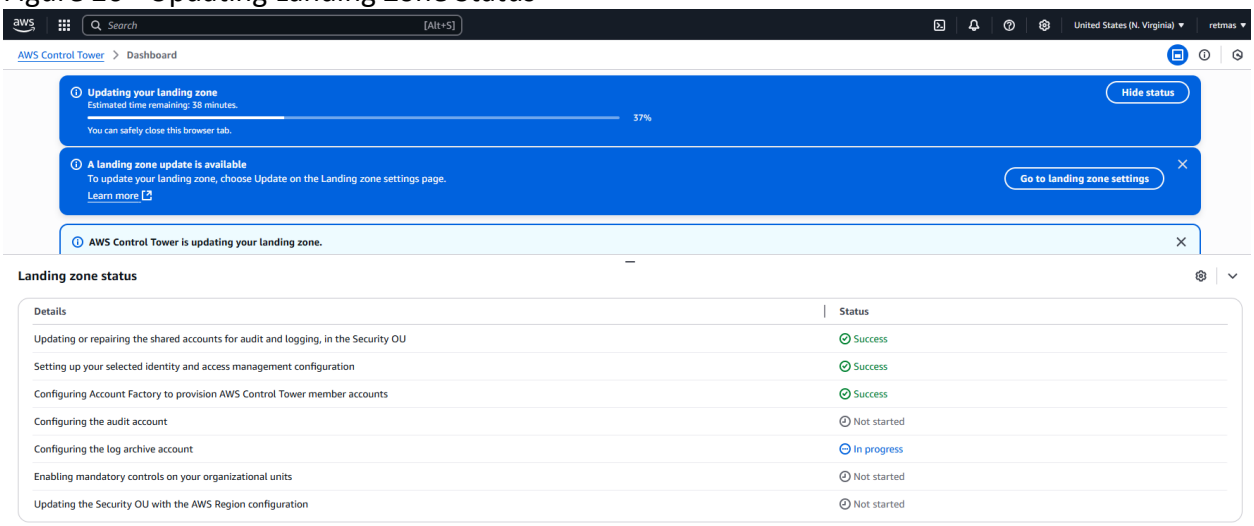
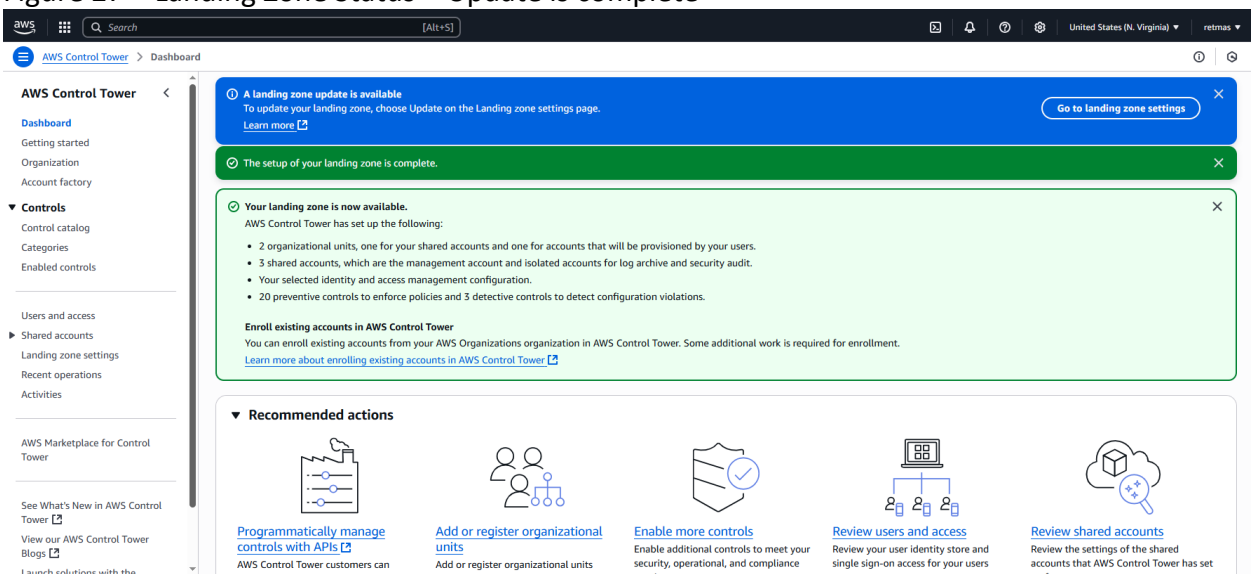


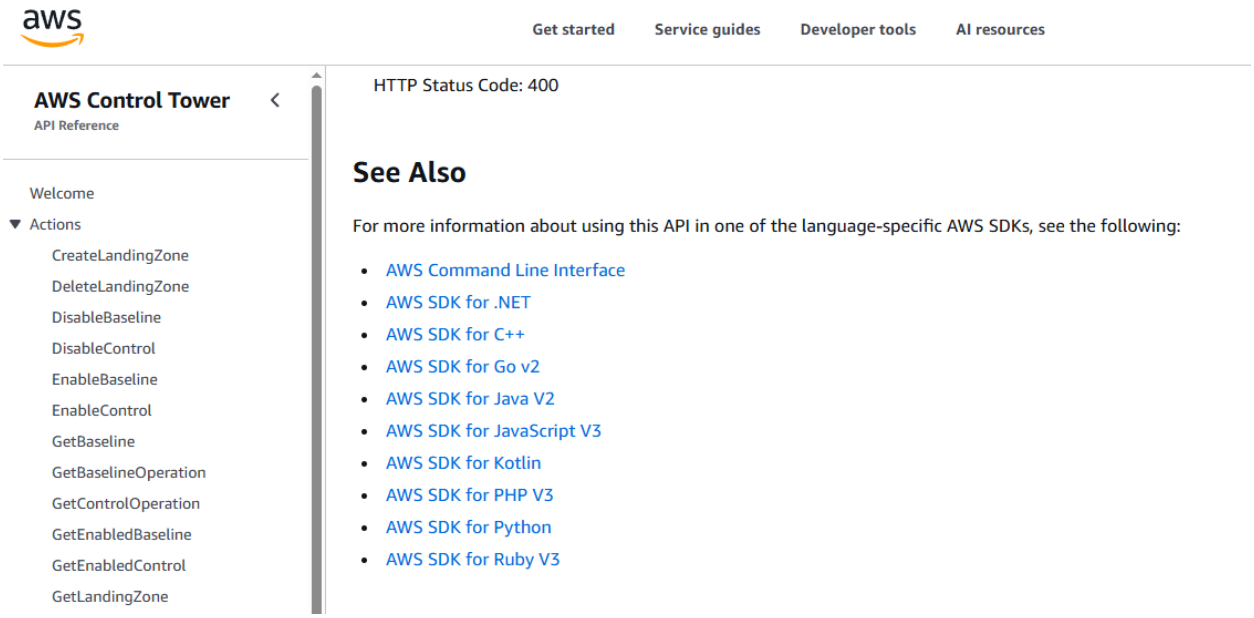
Figure 27 – Landing Zone Status – Update is complete



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.

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

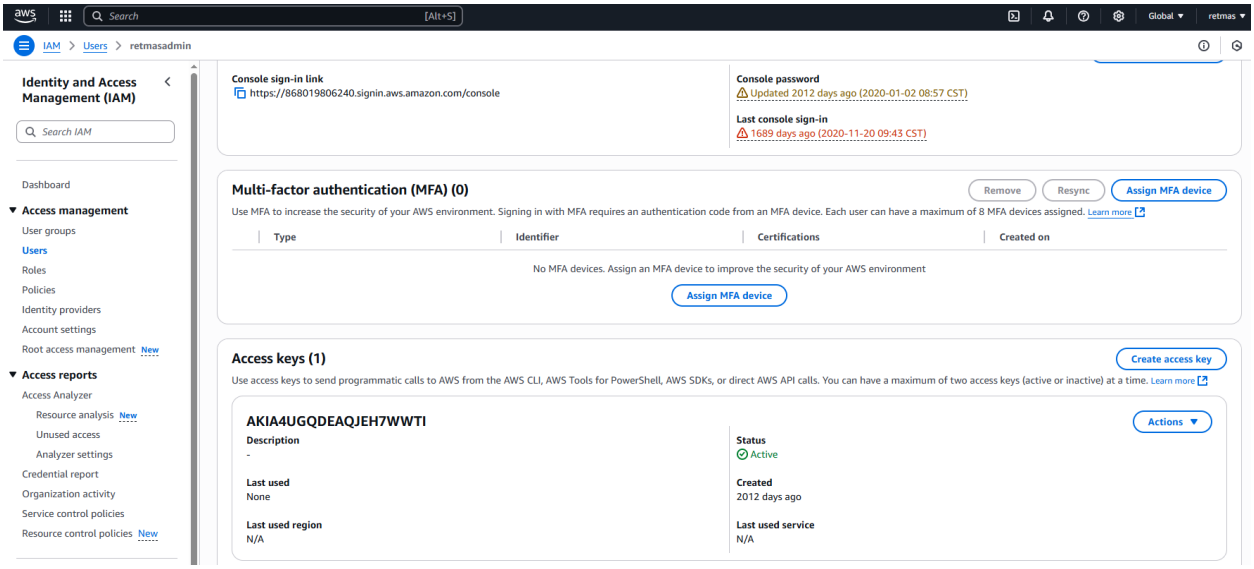


Figure 30 – Create Access Key (Continued)

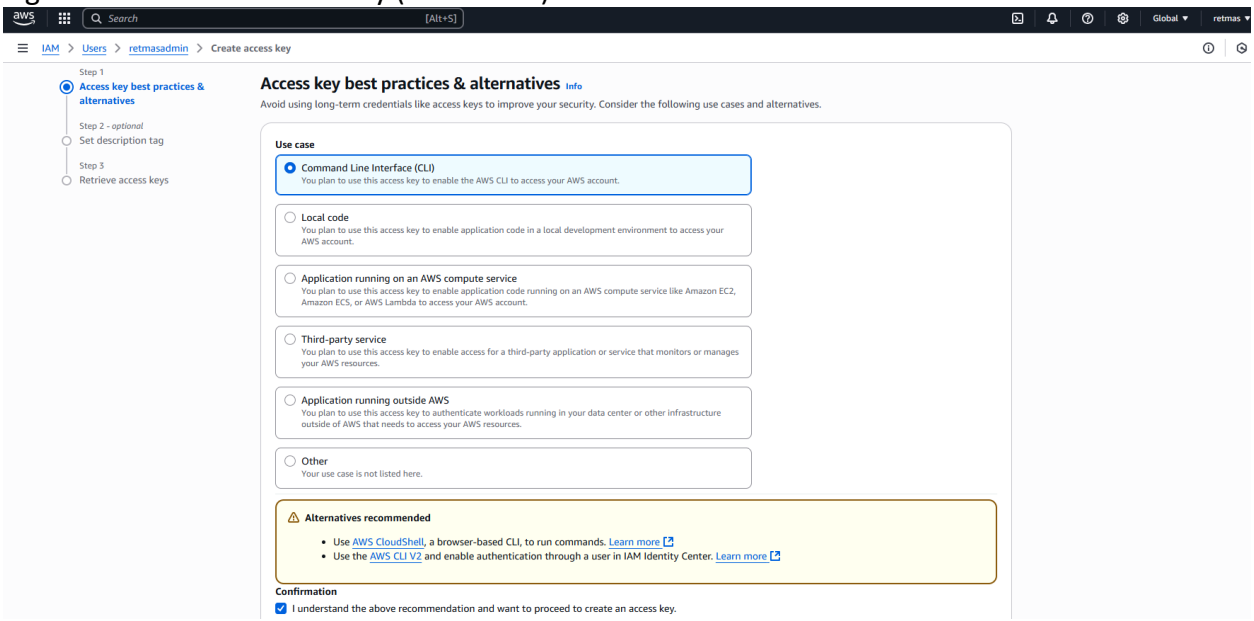


Figure 31 – Create Access Key (Continued)

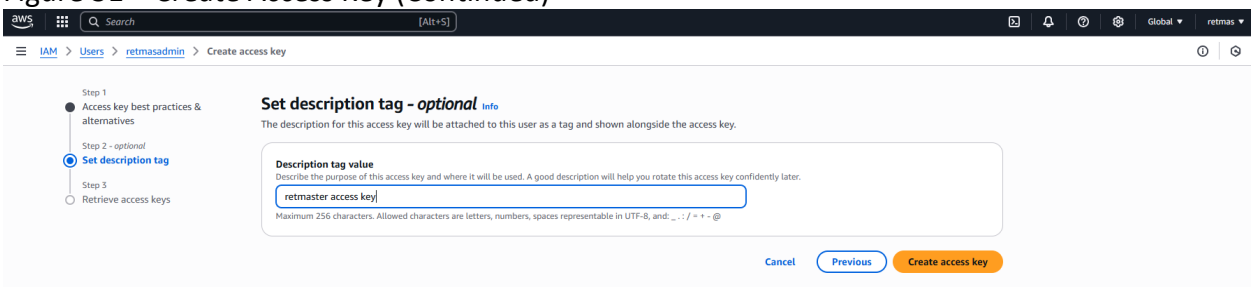
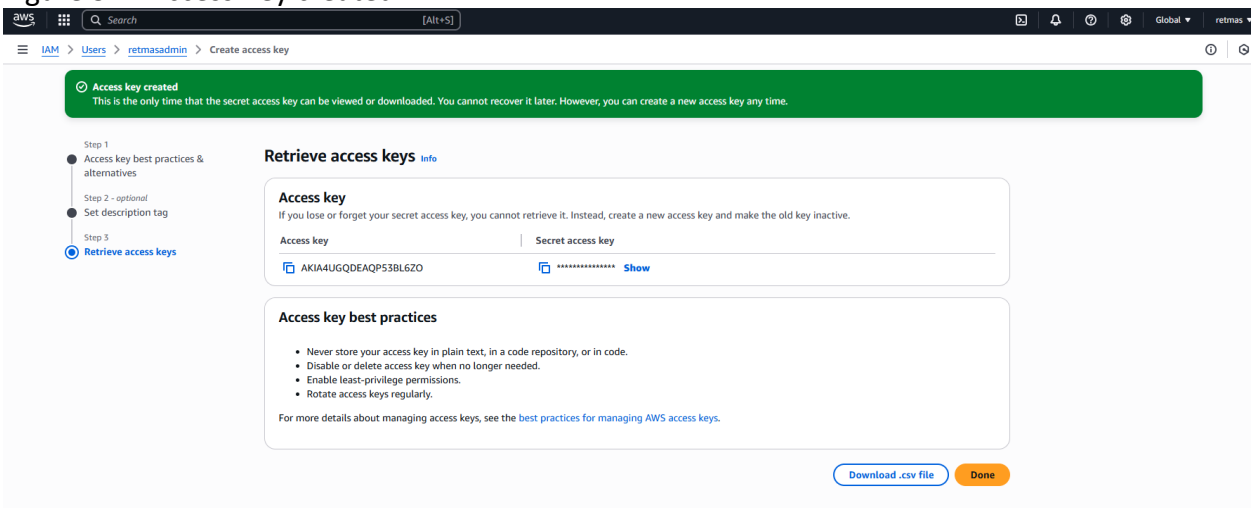


Figure 32 - Access Key created



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]: AKIA4UGQDEAQP53BL6ZO
```

Figure 34 – AWS CLI Access Configuration (Continued)

```
Start page | tshen@ubun221016: ~ | tshen@ubun221016: ~
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]: AKIA4UGQDEAQP53BL6ZO
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"
      },
      {
```

```
        "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/B10MNMYORNO6YM6N",
      "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/RWXUO4FAL209KVBE",
        "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/RWXUO49UCPXWJP0G",
        "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/1DMK6IYOFYKCVCPP",
        "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/1DMK6J0GLHXLFJTN",
      "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/B10MNMKG8RJDZYAL",
        "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/B10MNNR4ZTFBF0OQ",
      "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-
GR_SNS_SUBSCRIPTION_CHANGE_PROHIBITED",
      "driftStatusSummary": {
        "driftStatus": "NOT_CHECKING"
```

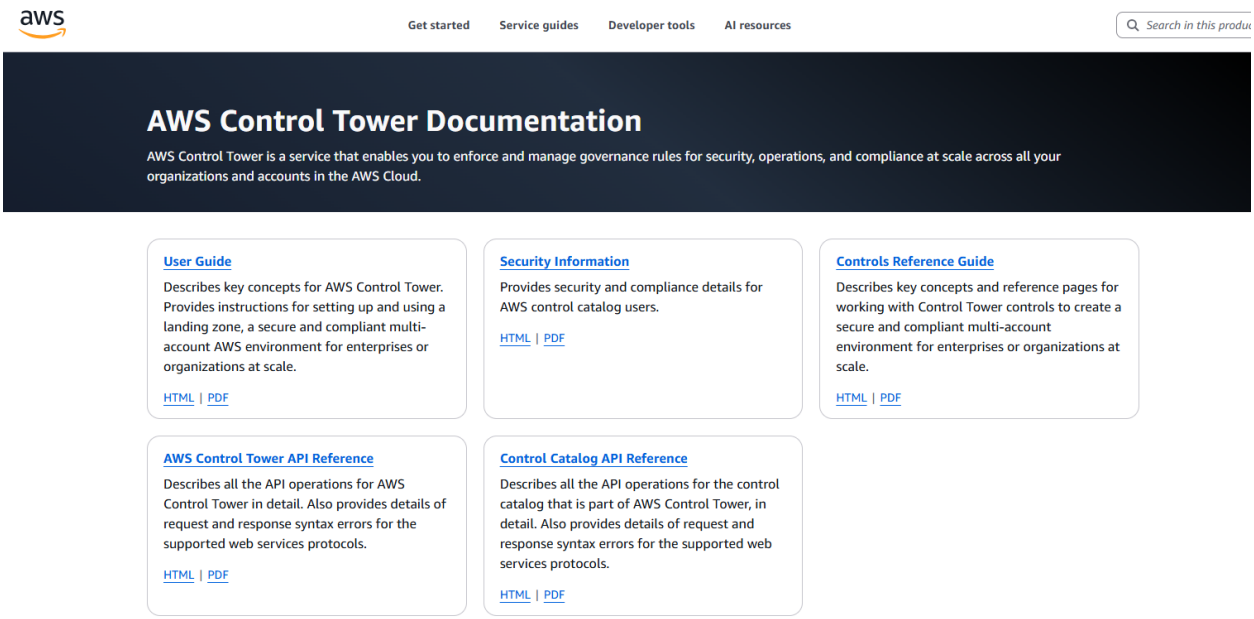
```
        },
        "statusSummary": {
          "status": "SUCCEEDED"
        }
      }
  ]
}
tshen@ubun221016:~$
```

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