Lab B1 – AWS Control Tower Deployment and Beyond

Overview

This lab gives you a high-level overview of the deployment of AWS Control Tower service. Let us walk through the implementation of the AWS Control Tower, and review some of the initial automated tasks that happen under the hood as part of the Control Tower initialization.

AWS Control Tower is a managed service, that automates the set-up of a baseline environment, or landing zone, that is a secure, well-architected multi-account AWS environment. You could initiate the AWS Control tower deployment from the AWS Management Console with few clicks and a form to fill.

It takes 60-90 minutes to launch an AWS Control Tower on a new AWS account. Hence we recommend to deploy the AWS Control Tower Section upfront before attending the class if possible.

Deploy the AWS Control Tower

In this section, we will deploy the AWS Control Tower service. Following tasks are performed on the successful launch of the service:

- Creates 2 organizational units, one for your shared accounts and other for user accounts.
- Provisions 2 additional accounts on top of master account. These are used for log archive, and security audit.

- 17 preventive guardrails to enforce policies and 8 detective guardrails to detect violations.
- A native cloud directory with preconfigured groups and single sign-on access.

We recommend performing this ahead of the session as the initial setup could take 60-90 minutes. If you are using an account which already got an AWS Control Tower installed by somebody else, still recommend going through the below steps to get familiar with installation:

1. Log in to the AWS Management Console of the account where you plan to deploy AWS Control Tower. This account will be referred to as Master account henceforth.
2. Select the service **Control Tower** under **Management & Governance**.
3. Make sure you are in one of the four supported regions (N. Virginia, Ohio, Oregon, Ireland) for GA.
4. On AWS Control Tower home page, select **Get Started** button.
5. Under Set up your AWS Control Tower, provide the email IDs which you plan to use for shared accounts.

Input	Description
Log archive account Email Address	The log archive account is a repository of immutable logs of API activities and resource configurations from all accounts
Audit Account Email Address	The audit account is a restricted account for your security and compliance teams to gain read and write access to all accounts

1. Expand **Learn more about permissions** under **Service permissions** to review the roles used to launch the AWS Control Tower service. Please note the two roles **AWSControlTowerAdmin** and **AWSControlTowerExecution** are

created as part of initialization. We will use these roles in the rest of our labs.

2. Checkbox **I grant AWS Control permissions to administer AWS resources and services** and click on **Launch your AWS Control Tower**.
3. You will be redirected to **AWS Control Tower Dashboard**. The launch progress is shown in the blue bar on top of the Dashboard.
4. Check your emails for account creation confirmation from [AWS Single Sign-On](https://aws.amazon.com/single-sign-on/).
5. In a few minutes, you will receive an email with subject **Invitation to join AWS Single Sign-On** to the master account email address. Make sure to open the email and click on **Accept invitation**.
6. The same email also contains **User portal URL**, recommend to bookmark this, we will use it to access the AWS environment throughout the labs.
7. On selecting **Accept Invitation**, you will be redirected to the **AWS Single Sign-On** page and from where you could set **New Password** to your master account. Repeat Password and Update User to proceed.
8. You will receive one more email with subject **AWS Organizations email verification request** to the master account email address. Click on **Verify your email address** to continue with inviting newly created accounts into AWS Organization.
9. Wait for the blue progress bar with **% complete** to disappear on top of the AWS Control Tower dashboard.

Note: It is normal to see the progress staying at 99% for 15-20 minutes

Exploring the Solution

AWS Control Tower uses AWS CloudFormation Stacksets to establish the baselines and create the guardrails across multiple accounts and regions. In this section we will walk through the Stacksets used under the hood.

1. Login in to **AWS SSO** Console using the bookmark and password that you setup in step 10 and 11.
2. Click on the Master account to expand. Select **Management console** next to **AWSAdministratorAccess** Role to login AWS Management console of the **master** account.
3. Select **CloudFormation** under **Management & Governance** and select **StackSets** under CloudFormation

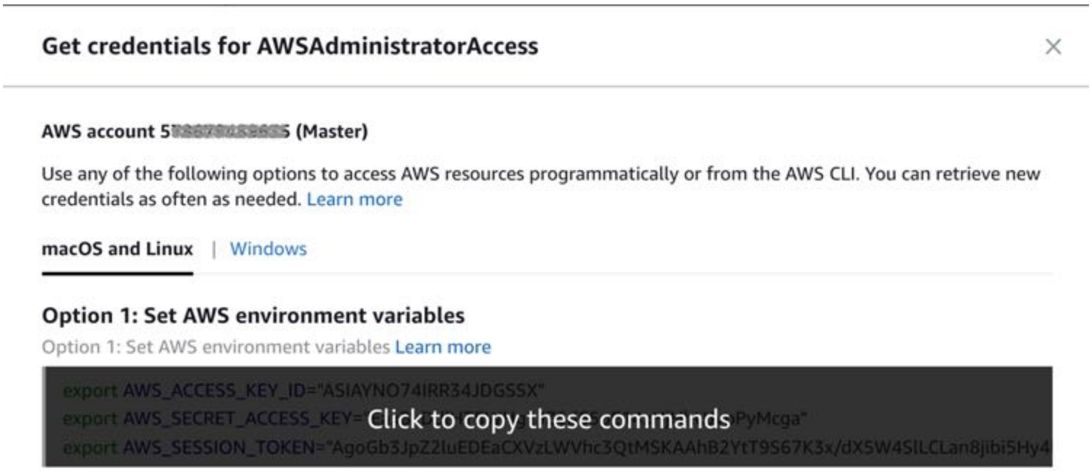
CloudFormation StackSets used as part of Control Tower Initialization

StackSet name	Description
AWSControlTowerBP-BASELINE-CLOUDTRAIL	Configure AWS CloudTrail on all accounts
AWSControlTowerBP-BASELINE-CLOUDWATCH	Configure Cloudwatch Rule, local SNS Topic, forwarding notifications from local SNS Topic to Security Topic
AWSControlTowerBP-BASELINE-CONFIG	Configure AWS Config on all accounts/regions
AWSControlTowerBP-BASELINE-ROLES	Creates all required baseline roles on all the accounts
AWSControlTowerBP-BASELINE-SERVICE-ROLES	Creates all required service roles on all the accounts for services (like AWS Config, SNS) used by CT
AWSControlTowerBP-SECURITY-TOPICS	Central monitoring and alerting using SNS and AWS CloudWatch
AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED	Configure AWS Config rules on core accounts to check that your S3 buckets do not allow public access
AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED	Configure AWS Config rules on core accounts to check that your S3 buckets do not allow public access
AWSControlTowerGuardrailAWS-GR-S3-BUCKET-PUBLIC-READ-PROHIBITED	StackSet for applying guardrail
AWSControlTowerGuardrailAWS-GR-S3-BUCKET-PUBLIC-WRITE-PROHIBITED	StackSet for applying guardrail
AWSControlTowerLoggingResources	StackSet to setup required resources on Log archive Account

You may see additional stacksets depending on the number of guardrails you enable on Control Tower.

Instructions on using CLI on AWS Control Tower environment

1. Log in to **AWS SSO** Console using the bookmark and password that you setup previously. Click on the account to expand, choose Command line or programmatic access. Select Option 1 for this lab.



Get credentials for AWSAdministratorAccess

AWS account 5[redacted]5 (Master)

Use any of the following options to access AWS resources programmatically or from the AWS CLI. You can retrieve new credentials as often as needed. Learn more

Option 1: Set AWS environment variables

Option 1: Set AWS environment variables Learn more

```
export AWS_ACCESS_KEY_ID="ASIAYNO74IRR34JDGSSX"
export AWS_SECRET_ACCESS_KEY=          PyMcga"
export AWS_SESSION_TOKEN="AgoGb3JpZ2luEDEaCXVzLWVhc3QtMSKAAhB2YtT9S67K3x/dX5W4SlLCLan8jibi5Hy4
```

2. Copy the credential information and follow the instructions from one of the first two options listed. On proper configuration the account will be able to run awscli commands. Plese

```
$ aws cloudformation list-stacks --query 'StackSummaries[?
StackStatus==`CREATE_COMPLETE`].StackName'
```

```
[
    "StackSet-AWSControlTowerBP-BASELINE-CONFIG-
f389a50e-4dc1-4528-8b32-18635ca6574f",
    "StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL-
d341f2b3-18b5-40cb-8c49-c3cc220c8df3",
    "StackSet-AWSControlTowerBP-BASELINE-
CLOUDWATCH-41be771b-1b42-422f-85d9-a75fc9c2e39e",
    "StackSet-AWSControlTowerBP-BASELINE-ROLES-00320288-ff98-4fb7-
a703-6bbcc97ac058",
    "StackSet-AWSControlTowerBP-BASELINE-SERVICE-
ROLES-4510cb1e-6d8e-4138-aaf6-f269b9327deb",
]
```

REFERENCES

- AWS Control Tower
- AWS Organizations
- AWS Single Sign On
- AWS Cloudformation Stacksets