

# Lab: mise en place de la landing Zone avec AWS Control Tower

## Scénario:

GlobalTech Inc. est une grande entreprise internationale fournissant des solutions financières et technologiques. Actuellement, elle utilise une infrastructure on-premises complexe avec plusieurs serveurs, applications, et bases de données critiques. Avec la montée en puissance du cloud et des exigences de conformité strictes, l'entreprise a décidé de migrer ses opérations vers AWS pour bénéficier de l'évolutivité, de la sécurité et des avantages financiers du cloud.

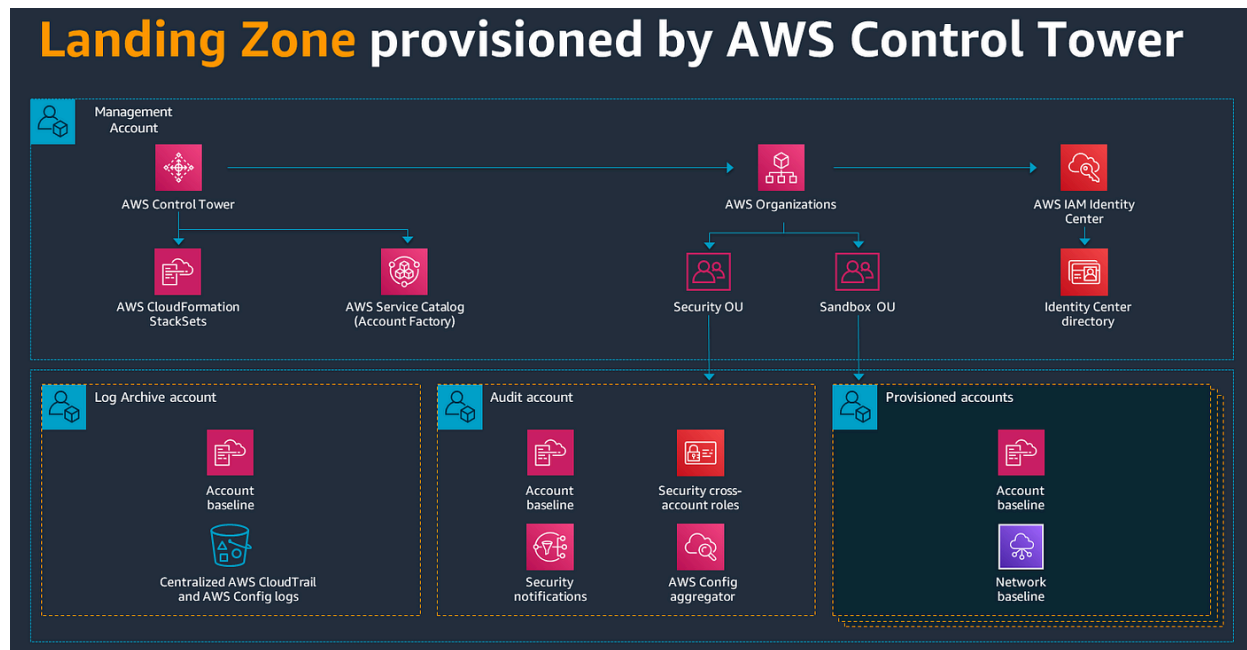
## Objectifs de Migration

1. **Sécurité et Conformité** : Assurer la conformité avec les réglementations financières et sécuritaires en place, telles que PCI-DSS et GDPR.
2. **Scalabilité** : Adapter facilement les ressources en fonction des besoins des différentes divisions de l'entreprise.
3. **Centralisation de la Gestion** : Mettre en place une gestion centralisée des comptes et des ressources AWS pour une meilleure visibilité et contrôle.
4. **Optimisation des coûts** : Optimiser les coûts en séparant les environnements de développement, de test et de production.

## Problématique

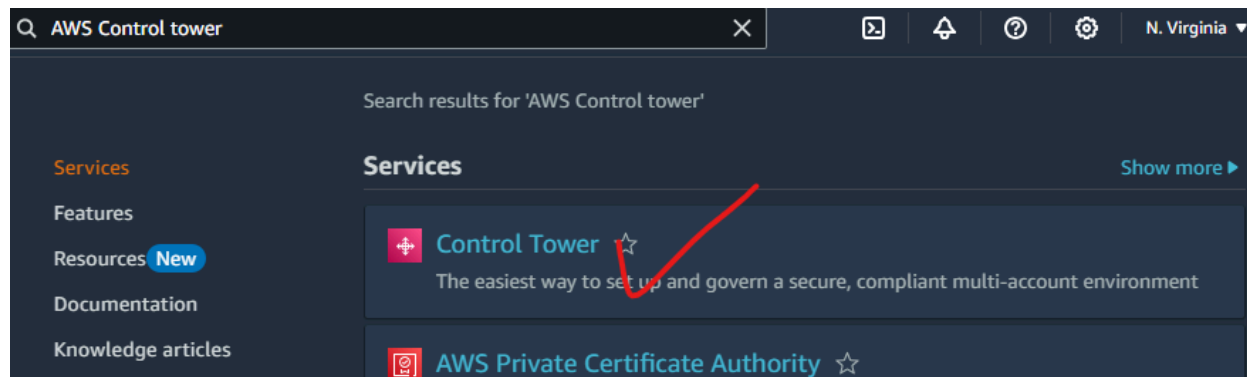
GlobalTech Inc. a besoin d'une solution pour configurer une infrastructure AWS multi-comptes sécurisée et conforme à ses politiques internes. Ils ont besoin d'une approche structurée pour créer une base solide sur laquelle leurs applications et services seront migrés. La configuration de cette infrastructure doit intégrer les meilleures pratiques de sécurité, de gouvernance et de gestion des coûts.

## Architecture:

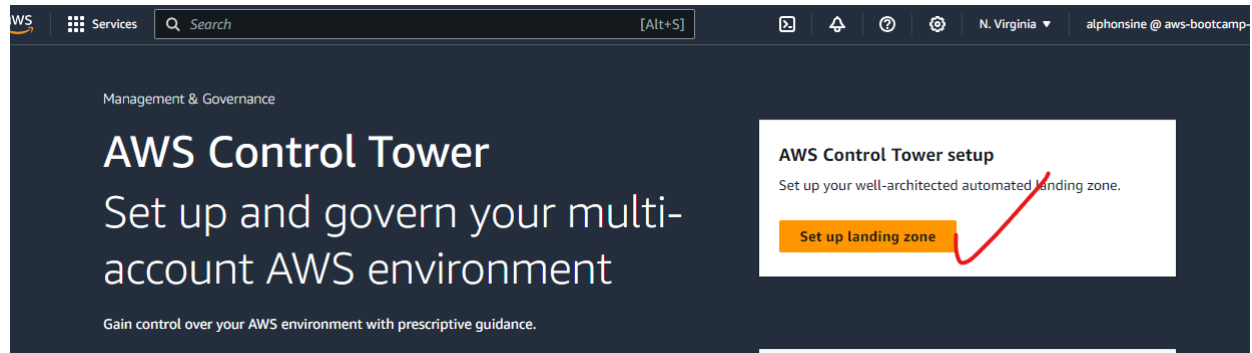


## Réalisation:

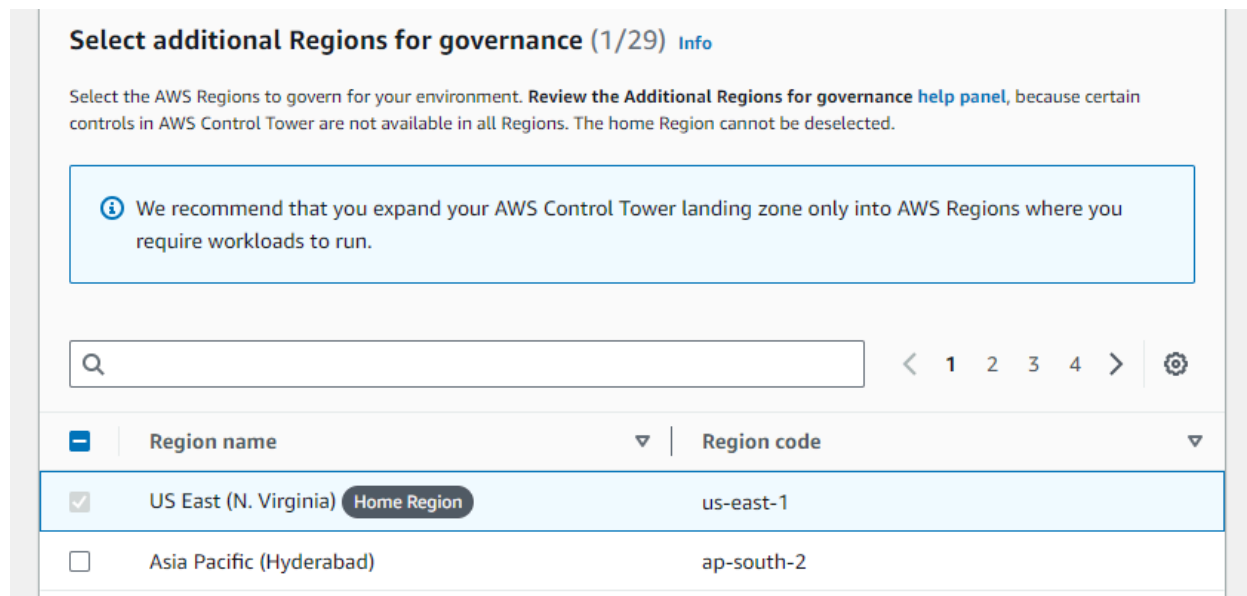
Au niveau de barre de recherche, entrez AWS Control Tower, cliquez-y dessus



Ensuite, cliquez le bouton “set up landing” comme sur l’image ci-dessous:




Faites le choix de la région de gouvernance



### Region deny setting [Info](#)

Select settings of the Region deny control for your landing zone. You cannot deny access to your home Region. This setting can be changed at a later time.

The Region deny setting enforces a control that prohibits access to AWS services and operations, by Region. It can be enabled for the landing zone and for individual OUs. For the landing zone, the configuration is based on the selections in the Additional Regions for governance table. It is enforced when you confirm your landing zone configurations. **Review the Region deny setting [help panel](#)** to understand how the Region deny control affects your landing zone and OUs.

 Before you enforce the Region deny control, be sure you do not have existing resources in Regions you want to deny, and Regions AWS Control Tower is not available in. You cannot access the resources in those Regions after the control is enforced.

☐ Enabled

☒ Not enabled

Cancel

Next

L'étape suivante consiste en la configuration des Unités d'Organisation ou Organizational Units (OU).

### Additional OU

To help set up a multi-account system, AWS Control Tower recommends you create a secondary OU when setting up your landing zone. This OU can be used to store any production or development accounts. You can create more OUs after setting up your landing zone.

Change OU name - *optional*  
"Sandbox" is the default OU name for your additional OU. OU names must be unique and can be edited after you set up your landing zone.

Sandbox

Cancel

Previous

Next

Configuration des comptes partagés

Step 1

[Review pricing and select Regions](#)

Step 2

[Configure organizational units \(OUs\)](#)

Step 3

**Configure shared accounts**

Step 4

Additional configurations

Step 5

Review and set up landing zone

## Configure shared accounts [Info](#)

### Management account

The management account provides billing and management of your accounts and your landing zone. It relies on your existing AWS account email address.

aws-bootcamp-eazytraining@eazytraining.fr

### Log archive account

The log archive account is a repository of immutable logs of API activities and resource configurations from all accounts.

☒ **Create new account**  
Create a new email address for the log archive account. This email address must not be in use for an existing AWS account.

☐ **Use existing account**  
Enter the account ID for a log archive account that exists in your organization

The log archive account email address must not be in use for an existing AWS account. It must be from 6 to 64 characters long.

### Change account name - *optional*

Keep your log archive account name unique from your other account names. **You cannot edit the name after setting up your landing zone.**

Log Archive

Configuration du compte d'audit:

### Audit account

The audit account is a restricted account. It allows your security and compliance teams to gain access to all accounts in the organization.

☒ **Create new account**  
Create a new email address for the audit account. This email address must not be in use for an existing AWS account.

☐ **Use existing account**  
Enter the account ID for an audit account that exists in your organization

Create account

The audit account email address must not be in use for an existing AWS account. It must be from 6 to 64 characters long.

Change account name - *optional*

Keep your audit account name unique from your other account names. You cannot edit the name after setting up your landing zone.

Cancel

Previous

Next

AWS Control Tower > Set up landing zone

Step 1

[Review pricing and select Regions](#)

Step 2

[Configure organizational units \(OUs\)](#)

Step 3

[Configure shared accounts](#)

Step 4

**Additional configurations**

Step 5

## Additional configurations

**AWS account access configuration** [Info](#)

Select how to manage access to your AWS accounts registered with AWS Control Tower. You can change this later.

☒ **AWS Control Tower sets up AWS account access with IAM Identity Center.**  
Best if you are just getting started with AWS or if your access management structure works with **AWS Control Tower groups and permission sets** [1]. You can connect your external identity provider (IdP) in IAM Identity Center later.


☐ **Self-managed AWS account access with IAM Identity Center or another method.**  
Best if you have custom requirements for managing AWS account access. AWS Control Tower will not manage account access. You must configure IAM Identity Center or another access method.


Configuration de CloudTrail

## AWS CloudTrail configuration [Info](#)

AWS CloudTrail captures actions for AWS Control Tower as events. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket.

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.


 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](#) 

☒ Enabled

☐ Not enabled

## KMS Encryption - optional [Info](#)

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](#) 

☐ Enable and customize encryption settings  
To disable encryption settings, uncheck this box.

Cancel

Previous

Next

Faites la revue et creer votre landing Zone

AWS Control Tower > Set up landing zone

Step 1  
[Review pricing and select Regions](#)

Step 2  
[Configure organizational units \(OUs\)](#)

Step 3  
[Configure shared accounts](#)

Step 4  
[Additional configurations](#)

Step 5  
**Review and set up landing zone**

## Review and set up landing zone

**Step 1: Review pricing and select Regions** Edit

Regions

Home Region US East (N. Virginia)	Additional Regions
Region deny <input type="radio"/> Not enabled	

**Step 2: Configure organizational units (OUs)** Edit

Foundational OU

## Step 5: Review and set up landing zone

**Service permissions**  
AWS Control Tower needs your permission to administer AWS resources and enforce rules on your behalf.

► [Learn more about permissions](#)

► [Learn more about guidance](#)

☒ I understand the permissions AWS Control Tower will use to administer AWS resources and enforce rules on my behalf. I also understand the guidance on the use of AWS Control Tower and the underlying AWS resources.

Cancel Previous **Set up landing zone**

Validez, et patientez 1h jusqu'à la création complète de votre landing zone



1

Setting up your landing zone

Estimated time remaining: 59 minutes.

Show status

You can safely close this browser tab.

3%

[AWS Control Tower](#) > [Dashboard](#)

Your landing zone is being set up

X

AWS Control Tower is setting up the following:

- 2 organizational units, one for your shared accounts and one for accounts that will be provisioned by your users.
- 3 shared accounts, which are the management account and isolated accounts for log archive and security audit.
- Your selected identity and access management configuration.
- 20 preventive controls to enforce policies and 3 detective controls to detect configuration violations.

Environment summary	Enabled control summary

Landing zone status

^

AWS Control Tower

X

Dashboard

Getting started

Organization

Account factory

Controls library

Categories

All controls

Users and access

Shared accounts

Management

Log archive

Audit

Landing zone settings

Find resources using properties

resource type

View all resources

6 matches

< 1 >

	Name	Baseline state	ID	Email	Organizational units registered	Accounts enrolled	Blue print ID
●	<div>Root</div>	✔ Succeeded	r-xfzf	-	✔ 2 of 2	✔ 3 of 3	-
○	<div>Sandbox</div>	✔ Succeeded	ou-xfzf-lo9bxxjg	-	⊖ 0 of 0	⊖ 0 of 0	-
●	<div>Security</div>	✔ Succeeded	ou-xfzf-j9wrz2iq	-	⊖ 0 of 0	✔ 2 of 2	-
○	<div>aws-bootcamp-eazytraining</div>	✔ Enrolled	010928200112	aws-bootcamp-eazytraining@eazytraining.fr	-	-	-

Registered organizational units

Find organizational units

< 1 >

Name	Parent organizational unit	State	Compliance
<a href="#">Root</a>	-	✔ Registered	✔ Compliant
<a href="#">Sandbox</a>	<a href="#">Root</a>	✔ Registered	✔ Compliant
<a href="#">Security</a>	<a href="#">Root</a>	✔ Registered	✔ Compliant

[View all organizational units](#)

Enrolled accounts					
<input type="text" value="Find accounts"/>				< 1 >	
Account name ▾	Account email ▾	Organizational unit ▾	Owner ▾	Compliance status	State ▾
<a href="#">aws-bootcamp-eazytraining</a>	aws-bootcamp-eazytraining@eazytraining.fr	<a href="#">Root</a>	AWS Control Tower	✔ Compliant	✔ Enrolled
<a href="#">Audit</a>	p9pq9nhf09@rfcdrive.com	<a href="#">Security</a>	AWS Control Tower	✔ Compliant	✔ Enrolled
<a href="#">Log Archive</a>	nikifen281@cetnob.com	<a href="#">Security</a>	AWS Control Tower	✔ Compliant	✔ Enrolled

1

---

<sup>1</sup> Lab proposed by Lahda Biassou Alphonsine