Guide de l’utilisateur

AWS Control Tower

AWS Control Tower: Guide de l’utilisateur

Table of Contents

Qu'est-ce qu'AWS Control Tower ?

AWS Control Tower offre un moyen simple de configurer et de gérer un environnement AWS multi-comptes, en suivant les meilleures pratiques prescriptives. AWS Control Tower orchestre les capacités de plusieurs autres AWS services, notamment AWS Organizations, et AWS Service Catalog AWS IAM Identity Center, pour créer une zone d'atterrissage en moins d'une heure. Les ressources sont configurées et gérées en votre nom.

L'orchestration d'AWS Control Tower étend les fonctionnalités de. AWS OrganizationsPour protéger vos organisations et vos comptes contre la dérive, qui constitue une divergence par rapport aux meilleures pratiques, AWS Control Tower applique des contrôles (parfois appelés barrières de sécurité). Par exemple, vous pouvez utiliser des contrôles pour garantir que les journaux de sécurité et les autorisations d'accès entre comptes nécessaires sont créés, et non modifiés.

Si vous hébergez plusieurs comptes, il est avantageux de disposer d'une couche d'orchestration qui facilite le déploiement et la gouvernance des comptes. Vous pouvez adopter AWS Control Tower comme principal moyen de provisionner des comptes et une infrastructure. Avec AWS Control Tower, vous pouvez plus facilement adhérer aux normes de l'entreprise, satisfaire aux exigences réglementaires et suivre les meilleures pratiques.

AWS Control Tower permet aux utilisateurs finaux de vos équipes distribuées de créer rapidement de nouveaux AWS comptes, au moyen de modèles de comptes configurables dans Account Factory. Dans le même temps, vos administrateurs cloud centraux peuvent vérifier que tous les comptes sont conformes aux politiques de conformité établies à l'échelle de l'entreprise.

En bref, AWS Control Tower offre le moyen le plus simple de configurer et de gérer un AWS environnement multi-comptes sécurisé et conforme, basé sur les meilleures pratiques établies en collaboration avec des milliers d'entreprises. Pour plus d'informations sur l'utilisation d'AWS Control Tower et sur les meilleures pratiques décrites dans la stratégie AWS multi-comptes, consultezAWS stratégie multi-comptes : guide des meilleures pratiques.

Fonctionnalités

AWS Control Tower possède les fonctionnalités suivantes :

- Zone d'atterrissage — Une zone d'atterrissage est un environnement multi-comptes bien conçu, basé sur les meilleures pratiques en matière de sécurité et de conformité. Il s'agit du conteneur à l'échelle de l'entreprise qui contient toutes vos unités organisationnelles (UO), comptes, utilisateurs

et autres ressources que vous souhaitez soumettre à la réglementation de conformité. Une zone de destination peut être mise à l'échelle pour s'adapter aux besoins de l'entreprise, quelle que soit sa taille.

- Contrôles — Un contrôle (parfois appelé garde-fou) est une règle de haut niveau qui fournit une gouvernance continue de votre environnement global AWS . Elle est exprimée en langage simple. Il existe trois types de contrôles : les contrôles préventifs, les contrôles de détection et les contrôles proactifs. Trois catégories de directives s'appliquent aux contrôles : obligatoires, fortement recommandés ou facultatifs. Pour plus d'informations sur les contrôles, consultezComment fonctionnent les commandes.
- Account Factory — An Account Factory est un modèle de compte configurable qui permet de normaliser le provisionnement de nouveaux comptes grâce à des configurations de compte préapprouvées. AWS Control Tower propose une Account Factory intégrée qui permet d'automatiser le flux de travail de provisionnement des comptes dans votre organisation. Pour de plus amples informations, veuillez consulter Provisionner et gérer des comptes avec Account Factory.
- Tableau de bord : le tableau de bord permet à votre équipe d'administrateurs cloud centraux de superviser en permanence votre zone d'atterrissage. Utilisez le tableau de bord pour voir les comptes provisionnés au sein de votre entreprise, les contrôles activés pour l'application des politiques, les contrôles activés pour la détection continue des non-conformités aux politiques et les ressources non conformes organisées par comptes et unités d'organisation.

Comment AWS Control Tower interagit avec les autres services AWS

AWS Control Tower repose sur des AWS services fiables et fiables AWS Service Catalog, notamment AWS IAM Identity Center, et AWS Organizations. Pour de plus amples informations, veuillez consulter Services intégrés.

Vous pouvez intégrer AWS Control Tower à d'autres AWS services dans une solution qui vous aide à migrer vos charges de travail existantes. AWSPour plus d'informations, consultez Comment tirer parti d'AWS Control Tower et CloudEndure migrer les charges de travail vers. AWS

Configuration, gouvernance et extensibilité

- Configuration automatisée des comptes : AWS Control Tower automatise le déploiement et l'inscription des comptes au moyen d'un Account Factory (ou « distributeur automatique »), qui est

conçu comme une abstraction au-dessus des produits fournis. AWS Service CatalogThe Account Factory peut créer et inscrire AWS des comptes, et automatise le processus d'application de contrôles et de politiques à ces comptes.

- Gouvernance centralisée : en utilisant les fonctionnalités d'AWS Control Tower AWS Organizations, elle met en place un cadre garantissant une conformité et une gouvernance cohérentes dans votre environnement multi-comptes. Le AWS Organizations service fournit des fonctionnalités essentielles pour gérer un environnement multi-comptes, notamment la gouvernance et la gestion centralisées des comptes, la création de comptes à partir d' AWS Organizations API et les politiques de contrôle des services (SCP).

- Extensibilité : vous pouvez créer ou étendre votre propre environnement AWS Control Tower en travaillant directement dans AWS Organizationsou dans la console AWS Control Tower. Vous pouvez voir vos modifications reflétées dans AWS Control Tower après avoir enregistré vos organisations existantes et inscrit vos comptes existants dans AWS Control Tower. Vous pouvez mettre à jour la zone de landing de votre AWS Control Tower en fonction de vos modifications. Si vos charges de travail nécessitent des fonctionnalités avancées supplémentaires, vous pouvez tirer parti des solutions d'autres AWS partenaires, ainsi que d'AWS Control Tower.

Utilisez-vous AWS Control Tower pour la première fois ?

Si c'est la première fois que vous utilisez ce service, nous vous recommandons de lire ce qui suit :

1. Si vous avez besoin de plus d'informations sur la façon de planifier et d'organiser votre zone d'atterrissage, consultez Planifiez la zone de landing de votre AWS Control Tower etAWS stratégie multi-comptes pour votre zone de landing zone AWS Control Tower.
2. Si vous êtes prêt à créer votre première zone de destination, veuillez consulter Commencer à utiliser AWS Control Tower.
3. Pour de plus amples informations sur la prévention et la détection de la dérive, veuillez consulter Détectez et corrigez les dérives dans AWS Control Tower.
4. Pour les détails de sécurité, veuillez consulter Sécurité dans AWS Control Tower.
5. Pour plus d'informations sur la mise à jour de votre zone de landing zone et de vos comptes membres, consultezGestion des mises à jour de configuration dans AWS Control Tower.

Comment fonctionne AWS Control Tower

Cette section décrit de manière détaillée le fonctionnement d'AWS Control Tower. Votre zone de landing zone est un environnement multi-comptes bien conçu pour toutes vos ressources. AWS Vous pouvez utiliser cet environnement pour appliquer les réglementations de conformité à tous vos AWS comptes.

Structure d'une zone d'atterrissage d'une tour de contrôle AWS

La structure d'une zone d'atterrissage dans AWS Control Tower est la suivante :

- Root : le parent qui contient toutes les autres unités d'organisation de votre zone de landing zone.
- UO de sécurité — Cette UO contient les comptes d'archive des journaux et d'audit. Ces comptes sont souvent appelés comptes partagés. Lorsque vous lancez votre zone de landing zone, vous pouvez choisir des noms personnalisés pour ces comptes partagés, et vous avez la possibilité d'intégrer des AWS comptes existants dans AWS Control Tower pour des raisons de sécurité et de journalisation. Toutefois, ils ne peuvent pas être renommés ultérieurement, et les comptes existants ne peuvent pas être ajoutés pour des raisons de sécurité et de journalisation après le lancement initial.
- Unité d'organisation Sandbox : l'unité d'organisation Sandbox est créée lorsque vous lancez votre zone d'atterrissage, si vous l'activez. Cette unité d'organisation enregistrée, ainsi que d'autres, contiennent les comptes inscrits avec lesquels vos utilisateurs travaillent pour exécuter leurs charges de travail AWS.
- Répertoire du centre d'identité IAM : ce répertoire héberge les utilisateurs de votre centre d'identité IAM. Il définit l'étendue des autorisations pour chaque utilisateur de l'IAM Identity Center.
- Utilisateurs de l'IAM Identity Center : il s'agit des identités que vos utilisateurs peuvent adopter pour exécuter leurs AWS charges de travail dans votre zone de landing zone.

Que se passe-t-il lorsque vous configurez une zone d'atterrissage

Lorsque vous configurez une zone de landing zone, AWS Control Tower effectue les actions suivantes sur votre compte de gestion en votre nom :

- Crée deux unités AWS Organizations organisationnelles (UO) : Security et Sandbox (facultatif), contenues dans la structure racine de l'organisation.
- Crée ou ajoute deux comptes partagés dans l'unité d'organisation de sécurité : le compte Log Archive et le compte Audit.

- Crée un annuaire cloud natif dans IAM Identity Center, avec des groupes préconfigurés et un accès par authentification unique, si vous choisissez la configuration par défaut d'AWS Control Tower, ou si cela vous permet de gérer vous-même votre fournisseur d'identité.
- Applique tous les contrôles préventifs obligatoires pour appliquer les politiques.
- Applique tous les contrôles de détection obligatoires pour détecter les violations de configuration.
- Les contrôles préventifs ne sont pas appliqués au compte de gestion.
- À l'exception du compte de gestion, les contrôles sont appliqués à l'ensemble de l'organisation.

Gestion sécurisée des ressources au sein de votre zone d'atterrissage et de vos comptes AWS Control Tower

- Lorsque vous créez votre zone de landing zone, un certain nombre de AWS ressources sont créées. Pour utiliser AWS Control Tower, vous ne devez pas modifier ou supprimer ces ressources gérées par AWS Control Tower en dehors des méthodes prises en charge décrites dans ce guide. La suppression ou la modification de ces ressources fera entrer votre zone d'atterrissage dans un état inconnu. Pour plus d'informations, consultez Conseils pour créer et modifier les ressources AWS Control Tower.
- Lorsque vous activez les contrôles facultatifs (ceux qui sont fortement recommandés ou facultatifs), AWS Control Tower crée AWS des ressources qu'elle gère dans vos comptes. Ne modifiez ni ne supprimez les ressources créées par AWS Control Tower. Cela peut entraîner l'entrée des commandes dans un état inconnu.

Quels sont les comptes partagés ?

Dans AWS Control Tower, les comptes partagés de votre zone de landing zone sont provisionnés lors de la configuration : le compte de gestion, le compte d'archivage des journaux et le compte d'audit.

Qu'est-ce que le compte de gestion ?

Il s'agit du compte que vous avez créé spécifiquement pour votre zone de landing zone. Ce compte est utilisé pour facturer tout ce qui se trouve dans votre zone de landing zone. Il est également utilisé pour le provisionnement des comptes par Account Factory, ainsi que pour gérer les unités d'organisation et les contrôles.

> **Note**
>
> Il n'est pas recommandé d'exécuter des charges de travail de production à partir d'un compte de gestion AWS Control Tower. Créez un compte AWS Control Tower distinct pour exécuter vos charges de travail.

Pour plus d'informations, consultez Compte de gestion.

Qu'est-ce que le compte d'archivage des journaux ?

Ce compte fonctionne comme un référentiel pour les journaux des activités de l'API et des configurations de ressources de tous les comptes de la zone de landing zone.

Pour plus d'informations, consultez Compte d'archivage des journaux.

Qu'est-ce que le compte d'audit ?

Le compte d'audit est un compte restreint conçu pour donner à vos équipes de sécurité et de conformité un accès en lecture et en écriture à tous les comptes de votre zone de landing zone. Depuis le compte d'audit, vous disposez d'un accès par programmation pour passer en revue les comptes, au moyen d'un rôle qui est accordé uniquement aux fonctions Lambda. Le compte d'audit ne vous permet pas de vous connecter manuellement à d'autres comptes. Pour plus d'informations sur les fonctions et les rôles Lambda, voir Configurer une fonction Lambda pour qu'elle assume le rôle d'une autre. Compte AWS

Pour plus d'informations, consultez Compte d'audit.

Comment fonctionnent les commandes

Un contrôle est une règle de haut niveau qui fournit une gouvernance continue de votre AWS environnement global. Chaque contrôle applique une règle unique, exprimée en langage clair. Vous pouvez modifier les contrôles facultatifs ou fortement recommandés qui sont en vigueur à tout moment depuis la console AWS Control Tower ou les API AWS Control Tower. Les contrôles obligatoires sont toujours appliqués et ne peuvent pas être modifiés.

Les contrôles préventifs empêchent les actions de se produire. Par exemple, le contrôle électif appelé Interdire les modifications apportées à la politique de compartiment pour les compartiments Amazon S3 (précédemment appelé Interdire les modifications de politique aux archives de journaux) empêche

toute modification de la politique IAM au sein du compte partagé d'archives de journaux. Toute tentative d'exécution d'une action empêchée est refusée et connectée CloudTrail. La ressource est également connectée AWS Config.

Les contrôles Detective détectent des événements spécifiques lorsqu'ils se produisent et enregistrent l'actionCloudTrail. Par exemple, le contrôle fortement recommandé appelé Detect Whether Encryption is Enabled for Amazon EBS Volumes Attached to Amazon EC2 Instances détecte si un volume Amazon EBS non chiffré est attaché à une instance EC2 dans votre zone de landing zone.

Des contrôles proactifs vérifient si les ressources sont conformes aux politiques et aux objectifs de votre entreprise, avant qu'elles ne soient provisionnées dans vos comptes. Si les ressources ne sont pas conformes, elles ne sont pas provisionnées. Les contrôles proactifs surveillent les ressources qui seraient déployées dans vos comptes au moyen de AWS CloudFormation modèles.

Pour ceux qui connaissent AWS : Dans AWS Control Tower, les contrôles préventifs sont mis en œuvre à l'aide de politiques de contrôle des services (SCP). Les contrôles Detective sont mis en œuvre avec AWS Config des règles. Les contrôles proactifs sont mis en œuvre à l'aide de AWS CloudFormation crochets.

Rubriques connexes

- Détectez et corrigez les dérives dans AWS Control Tower

Comment fonctionne AWS Control Tower avec StackSets

AWS Control Tower permet AWS CloudFormation StackSets de configurer les ressources de vos comptes. Chaque ensemble de piles StackInstances correspond à des comptes et à Régions AWS par compte. AWS Control Tower déploie une instance de stack set par compte et par région.

AWS Control Tower applique des mises à jour à certains comptes de Régions AWS manière sélective, en fonction AWS CloudFormation des paramètres. Lorsque les mises à jour sont appliquées à certaines instances de pile, d'autres instances de pile peuvent être laissées à l'état Outdated (Obsolète). Ce comportement est attendu et normal.

Lorsqu'une instance de pile passe à l'état Outdated (Obsolète) cela signifie généralement que la pile correspondant à cette instance de pile n'est pas alignée avec le dernier modèle de l'ensemble de piles. La pile reste dans l'ancien modèle, de sorte qu'elle peut ne pas inclure les dernières ressources ou derniers paramètres. La pile est encore complètement utilisable.

Voici un bref résumé du comportement auquel vous pouvez vous attendre, en fonction des AWS CloudFormation paramètres spécifiés lors d'une mise à jour :

Si la mise à jour de l'ensemble de piles inclut des modifications du modèle (c'est-à-dire si les `TemplateURL` propriétés `TemplateBody` ou sont spécifiées), ou si la `Parameters` propriété est spécifiée, AWS CloudFormation marque toutes les instances de pile avec le statut Obsolète avant de mettre à jour les instances de pile dans les comptes spécifiés et Régions AWS. Si la mise à jour de l'ensemble de piles n'inclut aucune modification du modèle ou des paramètres, AWS CloudFormation met à jour les instances de pile dans les comptes et régions spécifiés, tout en conservant le statut d'instance de pile existant pour toutes les autres instances de pile. Pour mettre à jour toutes les instances de pile associées à un jeu de piles, ne spécifiez pas les propriétés `Regions` ou `Accounts`.

Pour plus d'informations, voir Mettre à jour votre ensemble de piles dans le guide de AWS CloudFormation l'utilisateur.

Terminologie

Voici un bref aperçu de certains termes que vous trouverez dans la documentation d'AWS Control Tower.

Tout d'abord, il est bon de savoir qu'AWS Control Tower partage une grande partie de la terminologie avec le AWS Organizations service, notamment les termes organisation et unité organisationnelle (OU), qui apparaissent tout au long de ce document.

- Pour plus d'informations sur les organisations et les unités d'organisation, consultez AWS Organizations la section Terminologie et concepts. Si vous utilisez AWS Control Tower pour la première fois, cette terminologie est un bon point de départ.
- AWS Organizationsest un AWS service qui vous aide à gérer votre environnement de manière centralisée au fur et à mesure que vous développez et adaptez vos charges de travail. AWS AWS Control Tower s'appuie sur la création AWS Organizations de comptes, l'application de contrôles préventifs au niveau de l'unité organisationnelle et la fourniture d'une facturation centralisée.
- Un AWS compte Account Factory est un AWS compte provisionné à l'aide de Account Factory dans AWS Control Tower. Account Factory est parfois désigné de manière informelle comme un « distributeur automatique » de comptes.
- La région d'origine de votre AWS Control Tower est la AWS région dans laquelle votre zone d'atterrissage AWS Control Tower a été déployée. Vous pouvez voir votre région d'origine dans les paramètres de votre zone d'atterrissage.
- AWS Service Catalogvous permet de gérer de manière centralisée les services informatiques couramment déployés. Dans le contexte de ce document, Account Factory utilise Account Factory AWS Service Catalog pour approvisionner de nouveaux AWS comptes, y compris des comptes à partir de plans personnalisés.
- AWS CloudFormation StackSetssont un type de ressource qui étend les fonctionnalités des piles afin que vous puissiez créer, mettre à jour ou supprimer des piles sur plusieurs comptes et régions à l'aide d'une seule opération et d'un seul CloudFormation modèle.
- Une instance de pile est une référence à une pile dans un compte cible au sein d'une région.
- Une pile est un ensemble de AWS ressources que vous pouvez gérer comme une seule unité.
- Un agrégateur est un type de AWS Config ressource qui collecte des données de AWS Config configuration et de conformité à partir de plusieurs comptes et régions au sein de l'organisation, ce qui vous permet de consulter et d'interroger ces données de conformité au sein d'un seul compte.

- Un pack de conformité est un ensemble de AWS Config règles et d'actions correctives qui peuvent être déployées en tant qu'entité unique dans un compte et une région, ou au sein d'une organisation dans. AWS Organizations Vous pouvez utiliser un pack de conformité pour personnaliser votre environnement AWS Control Tower. Pour les blogs techniques fournissant plus de détails, consultez la section Informations connexes.
- Dans AWS Control Tower, une référence est un groupe de ressources et de configurations spécifiques que vous pouvez appliquer à une cible. L'objectif de référence le plus courant peut être une unité organisationnelle (UO). Par exemple, la ligne de base appelée `AWSControlTowerBaseline` est disponible pour vous aider à enregistrer vos unités d'organisation auprès d'AWS Control Tower. Lors de la configuration et de la mise à jour de la zone d'atterrissage, la cible de référence peut être un compte partagé ou un paramètre spécifique pour la zone d'atterrissage dans son ensemble.
- Plan : un plan est un artefact qui encapsule certaines métadonnées, qui décrivent les composants de l'infrastructure déployés au sein d'un compte. Par exemple, un AWS CloudFormation modèle peut servir de modèle pour un compte AWS Control Tower.
- Dérive : modification d'une ressource installée et configurée par AWS Control Tower. L'absence de dérive des ressources permet à AWS Control Tower de fonctionner correctement.
- Ressource non conforme : ressource qui enfreint une AWS Config règle définissant un contrôle de détection particulier.
- Compte partagé : l'un des trois comptes qu'AWS Control Tower crée automatiquement lorsque vous configurez votre zone de landing zone : le compte de gestion, le compte d'archivage des journaux et le compte d'audit. Vous pouvez choisir des noms personnalisés pour le compte d'archivage du journal et le compte d'audit lors de la configuration.
- Compte membre : un compte membre appartient à l'organisation AWS Control Tower. Le compte de membre peut être inscrit ou désinscrit dans AWS Control Tower. Lorsqu'une unité d'organisation enregistrée contient un mélange de comptes inscrits et non inscrits :
  - Les contrôles préventifs activés sur l'unité d'organisation s'appliquent à tous les comptes qu'elle contient, y compris les comptes non inscrits. Cela est vrai car les contrôles préventifs sont appliqués avec les SCP au niveau de l'unité d'organisation, et non au niveau du compte. Pour plus d'informations, consultez la section Héritage pour les politiques de contrôle des services dans la AWS Organizations documentation.
  - Les contrôles Detective activés sur l'unité d'organisation ne s'appliquent pas aux comptes non inscrits.

Un compte ne peut être membre que d'une seule organisation à la fois, et ses frais sont facturés au compte de gestion de cette organisation. Un compte membre peut être déplacé vers le conteneur racine d'une organisation.

- AWS compte : un AWS compte fait office de conteneur de ressources et de limite d'isolation des ressources. Un AWS compte peut être associé à la facturation et au paiement. Un AWS compte est différent d'un compte utilisateur (parfois appelé compte utilisateur IAM) dans AWS Control Tower. Les comptes créés dans le cadre du processus de provisionnement d'Account Factory sont des AWS comptes. AWS des comptes peuvent également être ajoutés à AWS Control Tower par le biais du processus d'inscription au compte ou d'enregistrement de l'unité d'organisation.
- Contrôle : un contrôle (également connu sous le nom de garde-corps) est une règle de haut niveau qui fournit une gouvernance continue pour l'ensemble de votre environnement AWS Control Tower. Chaque contrôle applique une seule règle. Des contrôles préventifs sont mis en œuvre avec des SCP. Les contrôles Detective sont mis en œuvre avec AWS Config des règles. Les contrôles proactifs sont mis en œuvre à l'aide de AWS CloudFormation crochets. Pour plus d'informations, consultez Comment fonctionnent les commandes.
- Zone d'atterrissage : une zone de destination est un environnement cloud qui propose un point de départ recommandé, notamment les comptes par défaut, la structure des comptes, les configurations réseau et de sécurité, etc. À partir d'une zone de landing zone, vous pouvez déployer des charges de travail qui utilisent vos solutions et applications.
- UO imbriquée : une UO imbriquée dans AWS Control Tower est une UO contenue dans une autre UO. Une unité d'organisation imbriquée peut avoir exactement une unité d'organisation parent, et chaque compte peut être membre d'une seule unité d'organisation. Les unités d'organisation imbriquées créent une hiérarchie. Lorsque vous associez une politique à l'une des unités d'organisation de la hiérarchie, elle s'applique à toutes les unités d'organisation et à tous les comptes situés en dessous. Une hiérarchie d'unités d'organisation imbriquée dans AWS Control Tower peut avoir une profondeur maximale de cinq niveaux.
- UO parent : UO située juste au-dessus de l'UO actuelle dans la hiérarchie. Chaque unité d'organisation peut avoir exactement une unité d'organisation parent.
- UO enfant : toute UO située en dessous de l'UO actuelle dans la hiérarchie. Une UO peut avoir plusieurs UO enfants.
- Hiérarchie des unités d'organisation : dans AWS Control Tower, la hiérarchie des unités d'organisation imbriquées peut comporter jusqu'à cinq niveaux. L'ordre d'imbrication est appelé niveaux. Le sommet de la hiérarchie est désigné comme niveau 1.

- UO de haut niveau : une UO de haut niveau est toute unité d'organisation située directement sous la racine, et non la racine elle-même. La racine n'est pas considérée comme une unité d'organisation.

Tarification

L'utilisation d'AWS Control Tower n'entraîne aucun frais supplémentaire. Vous ne payez que pour les AWS services activés par AWS Control Tower et les services que vous utilisez dans votre zone de landing zone. Par exemple, vous payez pour Service Catalog pour l'approvisionnement de comptes auprès d'Account Factory et AWS CloudTrail pour les événements suivis dans votre zone de landing zone. Pour plus d'informations sur les tarifs et les frais associés à AWS Control Tower, consultez la section Tarification d'AWS Control Tower.

Si vous exécutez des charges de travail éphémères à partir de comptes dans AWS Control Tower, vous constaterez peut-être une augmentation des coûts associés à. AWS ConfigPour de plus amples informations, veuillez consulter TarificationAWS Config. Contactez le représentant de votre AWS compte pour obtenir des informations plus spécifiques sur la gestion de ces coûts. Pour en savoir plus sur le AWS Config fonctionnement d'AWS Control Tower, consultezSurveillez l'évolution des ressources avec AWS Config.

Si vous implémentez des AWS CloudTrail sentiers en dehors d'AWS Control Tower, vous pouvez les utiliser avec AWS Control Tower. Toutefois, des frais supplémentaires peuvent vous être facturés si vous optez également pour des parcours gérés par AWS Control Tower. Nous vous déconseillons de créer des sentiers extérieurs, sauf si vous avez des exigences spécifiques. Si vous choisissez de vous inscrire lors de la configuration ou de la mise à jour de la zone d'atterrissage, AWS Control Tower met en place et active un suivi au niveau de l'organisation CloudTrail pour vous dans le compte de gestion. Pour plus d'informations sur la gestion des CloudTrail coûts, consultez la section Gestion des CloudTrail coûts.

Configuration

Avant de l'utiliser AWS Control Tower pour la première fois, suivez les étapes décrites dans cette section pour créer un AWS compte et protéger votre compte AWS Control Tower de gestion. Pour plus d'informations sur les tâches de configuration supplémentaires spécifiquement destinées à AWS Control Tower, voirCommencer à utiliser AWS Control Tower.

Inscrivez-vous pour AWS

Lorsque vous vous inscrivez à Amazon Web Services (AWS), votre AWS compte est automatiquement inscrit à tous les services AWS, y compris AWS Control Tower. Si vous avez déjà un AWS compte, passez à la tâche suivante. Si vous n'avez pas de AWS compte, suivez la procédure ci-dessous pour en créer un.

Notez votre numéro de AWS compte, car vous en avez besoin pour d'autres tâches.

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. La meilleure pratique en matière de sécurité consiste à attribuer un accès administratif à un utilisateur et à n'utiliser que l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Une fois que vous vous êtes inscrit à un utilisateur administratif Compte AWS, que vous Utilisateur racine d'un compte AWS l'avez sécurisé AWS IAM Identity Center, que vous l'avez activé et que vous en avez créé un, afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, consultez la section Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, accordez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connectez-vous en tant qu'utilisateur disposant d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribuer l'accès à des utilisateurs supplémentaires

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme aux meilleures pratiques en matière d'application des autorisations du moindre privilège.

   Pour obtenir des instructions, voir Création d'un ensemble d'autorisations dans le guide de AWS IAM Identity Center l'utilisateur.
2. Affectez des utilisateurs à un groupe, puis attribuez un accès d'authentification unique au groupe.

   Pour obtenir des instructions, consultez la section Ajouter des groupes dans le guide de AWS IAM Identity Center l'utilisateur.

> **Sécurité de vos comptes**
>
> Vous trouverez des conseils supplémentaires sur la manière de mettre en place les meilleures pratiques qui protègent la sécurité de vos AWS Control Tower comptes dans la AWS Organizations documentation.
>
> - Bonnes pratiques pour le compte de gestion
> - Bonnes pratiques pour les comptes des membres

Étape suivante

Commencer à utiliser AWS Control Tower

Commencer à utiliser AWS Control Tower

Cette procédure de mise en route est destinée aux administrateurs d'AWS Control Tower. Suivez cette procédure lorsque vous êtes prêt à configurer votre zone d'atterrissage à l'aide de la console ou des API AWS Control Tower.

Si vous êtes actuellement AWS client, mais que vous utilisez AWS Control Tower pour la première fois, vous souhaiterez peut-être consulter la section intitulée «Planifiez la zone de landing de votre AWS Control Tower, avant de continuer.

Rubriques

Guide de démarrage rapide d'AWS Control Tower

Si vous êtes nouveau dans ce AWSdomaine, vous pouvez suivre les étapes décrites dans cette section pour démarrer rapidement avec AWS Control Tower. Si vous préférez personnaliser immédiatement votre environnement AWS Control Tower, consultez Étape 2. Configurez et lancez votre zone d'atterrissage .

> **Note**
>
> AWS Control Tower met en place des services payants AWS CloudTrail AWS Config, tels que Amazon CloudWatch, Amazon S3 et Amazon VPC. Lorsqu'ils sont utilisés, ces services peuvent entraîner des coûts, comme indiqué sur la page de tarification. La console AWS de gestion vous indique l'utilisation de tous les services payants et les coûts engagés. Aucun coût supplémentaire n'est créé par AWS Control Tower elle-même.

Avant de commencer

La décision la plus importante à prendre avant de commencer le processus de configuration est de choisir votre région d'origine. Votre région d'origine est la AWS région dans laquelle vous exécuterez la plupart de vos charges de travail ou stockerez la plupart de vos données. Il ne peut pas être modifié une fois que vous avez configuré votre zone de landing AWS Control Tower. Pour plus d'informations sur le choix d'une région d'origine, consultez Conseils administratifs pour la configuration de la zone d'atterrissage .

> **Note**
>
> Par défaut, AWS Control Tower choisit la région dans laquelle votre compte fonctionne actuellement comme région d'origine. Vous pouvez voir votre région actuelle dans le coin supérieur droit de l'écran de votre console de AWS gestion.

La procédure de démarrage rapide suppose que vous accepterez les valeurs par défaut pour les ressources de votre environnement AWS Control Tower. Bon nombre de ces choix peuvent être modifiés ultérieurement. Quelques choix ponctuels sont répertoriés dans la section intitulée Attentes relatives à la configuration de la zone d'atterrissage .

Si vous avez créé un nouveau AWS compte, il répond automatiquement aux conditions requises pour configurer AWS Control Tower. Vous pouvez suivre les étapes suivantes.

Étapes de démarrage rapide

1. Connectez-vous à la console de AWS gestion à l'aide de vos informations d'identification d'administrateur.
2. Accédez à la console AWS Control Tower à l'adresse https://console.aws.amazon.com/controltower.
3. Vérifiez que vous travaillez dans la région d'origine de votre choix.
4. Choisissez Configurer la zone d'atterrissage.
5. Suivez les instructions de la console en acceptant toutes les valeurs par défaut. Vous devrez saisir l'adresse e-mail de votre compte, d'un compte d'archivage des journaux et d'un compte d'audit.
6. Confirmez vos choix et choisissez Configurer la zone d'atterrissage.
7. AWS Control Tower met environ 30 minutes pour configurer toutes les ressources de votre zone de landing zone.

Pour obtenir une version plus détaillée de la configuration d'AWS Control Tower, notamment des méthodes de personnalisation de votre environnement, lisez et suivez les procédures décrites dans les rubriques suivantes.

> **Note**
>
> Si vous êtes client pour la première fois et que vous rencontrez un problème de configuration, contactez le AWS Support pour obtenir une assistance diagnostique.

Prérequis : vérifications automatisées avant le lancement de votre compte de gestion

Avant qu'AWS Control Tower ne configure la zone de landing zone, elle exécute automatiquement une série de vérifications préalables au lancement sur votre compte. Aucune action de votre part n'est requise pour effectuer ces vérifications, qui garantissent que votre compte de gestion est prêt à faire face aux modifications établissant votre zone de landing zone. Voici les vérifications effectuées par AWS Control Tower avant de configurer une zone de landing zone :

- Les limites de service existantes Compte AWS doivent être suffisantes pour permettre le lancement d'AWS Control Tower. Pour de plus amples informations, veuillez consulter Limitations et quotas dans AWS Control Tower.
- Vous Compte AWS devez être abonné aux AWS services suivants :
  - Amazon Simple Storage Service (Amazon S3)
  - Amazon Elastic Compute Cloud (Amazon EC2)
  - Amazon SNS
  - Amazon Virtual Private Cloud (Amazon VPC)
  - AWS CloudFormation
  - AWS CloudTrail
  - Amazon CloudWatch
  - AWS Config
  - AWS Identity and Access Management (JE SUIS)
  - AWS Lambda

> **Note**
>
> Par défaut, tous les comptes sont abonnés à ces services.

Considérations pour les AWS IAM Identity Center clients (IAM Identity Center)

- Si AWS IAM Identity Center (IAM Identity Center) est déjà configuré, la région d'origine d'AWS Control Tower doit être identique à la région du centre d'identité IAM.
- IAM Identity Center ne peut être installé que dans le compte de gestion d'une organisation.
- Trois options s'appliquent à votre répertoire IAM Identity Center, en fonction de la source d'identité que vous choisissez :
  - Boutique d'utilisateurs d'IAM Identity Center : si AWS Control Tower est configuré avec IAM Identity Center, AWS Control Tower crée des groupes dans le répertoire IAM Identity Center et fournit l'accès à ces groupes, pour l'utilisateur que vous sélectionnez, pour les comptes des membres.
  - Active Directory : si IAM Identity Center pour AWS Control Tower est configuré avec Active Directory, AWS Control Tower ne gère pas le répertoire IAM Identity Center. Il n'affecte pas d'utilisateurs ou de groupes à de nouveaux AWS comptes.
  - Fournisseur d'identité externe : si le centre d'identité IAM pour AWS Control Tower est configuré avec un fournisseur d'identité externe (IdP), AWS Control Tower crée des groupes dans le répertoire du centre d'identité IAM et fournit l'accès à ces groupes à l'utilisateur que vous sélectionnez pour les comptes de membre. Vous pouvez spécifier un utilisateur existant à partir de votre IdP externe dans Account Factory lors de la création du compte, et AWS Control Tower donne à cet utilisateur l'accès au nouveau compte lorsqu'elle synchronise les utilisateurs du même nom entre IAM Identity Center et l'IdP externe. Vous pouvez également créer des groupes dans votre IdP externe pour qu'ils correspondent aux noms des groupes par défaut dans AWS Control Tower. Lorsque vous affectez des utilisateurs à ces groupes, ces utilisateurs auront accès à vos comptes inscrits.

Pour plus d'informations sur l'utilisation d'IAM Identity Center et d'AWS Control Tower, consultez Ce qu'il faut savoir sur les comptes IAM Identity Center et AWS Control Tower

Considérations pour AWS Config et pour AWS CloudTrail les clients

- L'accès sécurisé Compte AWS ne peut pas être activé dans le compte de gestion de l'organisation pour AWS Config ou CloudTrail. Pour plus d'informations sur la désactivation de l'accès sécurisé, consultez la AWS Organizations documentation sur l'activation ou la désactivation de l'accès sécurisé.
- Si vous disposez d'un AWS Config enregistreur, d'un canal de diffusion ou d'une configuration d'agrégation dans l'un des comptes existants que vous envisagez d'inscrire dans AWS Control Tower, vous devez modifier ou supprimer ces configurations avant de commencer à inscrire les comptes, une fois votre zone de landing zone configurée. Cette vérification préalable ne s'applique pas au compte de gestion AWS Control Tower lors du lancement de la zone de landing zone. Pour de plus amples informations, veuillez consulter Inscrire des comptes disposant de ressources existantes AWS Config.
- Si vous exécutez des charges de travail éphémères à partir de comptes dans AWS Control Tower, vous constaterez peut-être une augmentation des coûts associés à Config. AWS Contactez le représentant de votre AWS compte pour obtenir des informations plus spécifiques sur la gestion de ces coûts.
- Lorsque vous créez un compte dans AWS Control Tower, celui-ci est régi par le AWS CloudTrail parcours de l'organisation AWS Control Tower. Si vous avez déjà déployé un essai dans CloudTrail le compte, des frais supplémentaires peuvent être facturés, sauf si vous supprimez le journal existant pour le compte avant de l'inscrire dans AWS Control Tower. Pour plus d'informations sur les sentiers au niveau de l'organisation et sur AWS Control Tower, consultez. Tarification

> **Note**
>
> Lors du lancement, les points de terminaison du AWS Security Token Service (STS) doivent être activés dans le compte de gestion, pour toutes les régions régies par AWS Control Tower. Sinon, le lancement peut échouer au milieu du processus de configuration.

Commencer à utiliser AWS Control Tower depuis la console

Cette procédure de démarrage est destinée aux administrateurs d'AWS Control Tower. Suivez cette procédure lorsque vous êtes prêt à configurer votre zone d'atterrissage à l'aide de la console AWS Control Tower. Du début à la fin, cela devrait prendre environ une demi-heure. Cette procédure nécessite quelques prérequis et trois étapes principales.

Si vous êtes actuellement AWS client, mais que vous utilisez AWS Control Tower pour la première fois, vous souhaiterez peut-être consulter la section intitulée «Planifiez la zone de landing de votre AWS Control Tower, avant de continuer.

Rubriques

Étape 1 : Créez les adresses e-mail de votre compte partagé

Si vous configurez votre zone d'atterrissage dans une nouvelle zone Compte AWS, consultezConfiguration.

- Pour configurer votre zone de landing zone avec de nouveaux comptes partagés, AWS Control Tower a besoin de deux adresses e-mail uniques qui ne sont pas encore associées à un Compte AWS. Chacune de ces adresses e-mail servira de boîte de réception collaborative (un compte e-mail partagé) destinée aux différents utilisateurs de votre entreprise chargés de tâches spécifiques liées à AWS Control Tower.
- Si vous configurez AWS Control Tower pour la première fois, et si vous intégrez des comptes de sécurité et d'archivage de journaux existants dans AWS Control Tower, vous pouvez saisir les adresses e-mail actuelles des AWS comptes existants.

Les adresses e-mail sont obligatoires pour :

- Compte d'audit : ce compte est destiné à votre équipe d'utilisateurs qui ont besoin d'accéder aux informations d'audit mises à disposition par AWS Control Tower. Vous pouvez également utiliser ce compte en tant que point d'accès pour les outils tiers qui effectuent l'audit par programmation de votre environnement pour vous aider à effectuer l'audit à des fins de conformité.
- Compte d'archivage des journaux : ce compte est destiné à votre équipe d'utilisateurs qui ont besoin d'accéder à toutes les informations de connexion de tous vos comptes inscrits au sein des unités d'organisation enregistrées dans votre zone de landing zone.

Ces comptes sont configurés dans l'unité d'organisation de sécurité lorsque vous créez votre zone de landing zone. À titre de bonne pratique, nous vous recommandons, lorsque vous effectuez des actions sur ces comptes, d'utiliser un utilisateur IAM Identity Center disposant des autorisations appropriées.

> **Note**
>
> Si vous spécifiez AWS des comptes existants comme comptes d'audit et d'archivage des journaux, les comptes existants doivent passer certains contrôles avant le lancement afin de garantir qu'aucune ressource n'est en conflit avec les exigences d'AWS Control Tower. Si ces vérifications échouent, il se peut que la configuration de votre zone d'atterrissage échoue. En particulier, les comptes ne doivent pas disposer de AWS Config ressources existantes. Pour plus d'informations, consultez Considérations relatives à l'ajout de comptes de sécurité ou de journalisation existants.

Dans un souci de clarté, le présent guide de l'utilisateur fait toujours référence aux comptes partagés par leurs noms par défaut : archivage des journaux et audit. Lorsque vous lisez ce document, n'oubliez pas de remplacer les noms personnalisés que vous donnez initialement à ces comptes, si vous choisissez de les personnaliser. Vous pouvez consulter vos comptes avec leurs noms personnalisés sur la page Détails du compte.

> **Note**
>
> Nous sommes en train de modifier notre terminologie concernant les noms par défaut de certaines unités organisationnelles (UO) d'AWS Control Tower afin de nous aligner sur la stratégie AWS multi-comptes. Vous remarquerez peut-être certaines incohérences lors de la transition visant à améliorer la clarté de ces noms. L'unité d'organisation de sécurité était auparavant appelée unité d'organisation principale. L'unité d'organisation Sandbox était auparavant appelée unité d'organisation personnalisée.

Attentes relatives à la configuration de la zone d'atterrissage

Le processus de configuration de votre zone de landing AWS Control Tower comporte plusieurs étapes. Certains aspects de votre zone de landing zone AWS Control Tower sont configurables. Les autres choix ne peuvent pas être modifiés après la configuration.

Éléments clés à configurer lors de l'installation

- Vous pouvez sélectionner les noms de vos unités d'organisation de premier niveau lors de la configuration, et vous pouvez également modifier les noms de vos unités d'organisation après avoir configuré votre zone de landing zone. Par défaut, les unités d'organisation de niveau supérieur sont nommées Security et Sandbox. Pour plus d'informations, consultez Directives pour la mise en place d'un environnement bien conçu.
- Lors de la configuration, vous pouvez sélectionner des noms personnalisés pour les comptes partagés créés par AWS Control Tower, appelés archive de journaux et audit par défaut, mais vous ne pouvez pas modifier ces noms après la configuration. (Il s'agit d'une sélection unique.)
- Lors de la configuration, vous pouvez éventuellement spécifier AWS des comptes existants pour AWS Control Tower à utiliser comme comptes d'audit et d'archivage des journaux. Si vous prévoyez de spécifier AWS des comptes existants, et si ces comptes disposent de AWS Config ressources existantes, vous devez supprimer les AWS Config ressources existantes avant de pouvoir les inscrire dans AWS Control Tower. (Il s'agit d'une sélection unique.)
- Si vous effectuez la configuration pour la première fois ou si vous passez à la version 3.0 de landing zone, vous pouvez choisir d'autoriser AWS Control Tower à configurer un AWS CloudTrail parcours au niveau de l'organisation pour votre organisation, ou de vous désinscrire des sentiers gérés par AWS Control Tower et de gérer vos propres CloudTrail sentiers. Vous pouvez accepter ou refuser les pistes au niveau de l'organisation qui sont gérées par AWS Control Tower chaque fois que vous mettez à jour votre zone de landing zone.
- Vous pouvez éventuellement définir une politique de rétention personnalisée pour votre bucket de log et votre bucket d'accès aux logs Amazon S3, lorsque vous configurez ou mettez à jour votre zone de landing zone.
- Vous pouvez éventuellement spécifier un plan prédéfini à utiliser pour le provisionnement de comptes membres personnalisés à partir de la console AWS Control Tower. Vous pourrez personnaliser les comptes ultérieurement si aucun plan n'est disponible. veuillez consulter Personnalisez les comptes avec Account Factory Customization (AFC).

Choix de configuration qui ne peuvent pas être annulés

- Vous ne pouvez pas modifier votre région d'origine une fois que vous avez configuré votre zone de landing zone.
- Si vous approvisionnez des comptes Account Factory avec des VPC, les CIDR VPC ne peuvent pas être modifiés une fois qu'ils ont été créés.

Étape 2. Configurez et lancez votre zone d'atterrissage

Avant de lancer votre zone de landing zone AWS Control Tower, déterminez la région d'origine la plus appropriée. Pour plus d'informations, consultez Conseils administratifs pour la configuration de la zone d'atterrissage .

> **Important**
>
> Le changement de région d'origine après le déploiement de la zone de landing de votre AWS Control Tower nécessite une mise hors service ainsi que l'assistance du Support AWS . Cette pratique n'est pas recommandée.

Découvrez comment configurer et lancer votre zone d'atterrissage à l'aide de AWS CLI l'entréeCommencer à utiliser AWS Control Tower à l'aide des API.

Pour configurer et lancer votre zone d'atterrissage dans la console, effectuez les étapes suivantes.

Préparation : accédez à la console AWS Control Tower

1. Ouvrez un navigateur Web et accédez à la console AWS Control Tower à l'adresse https://console.aws.amazon.com/controltower.
2. Dans la console, vérifiez que vous travaillez dans la région d'origine de votre choix pour AWS Control Tower. Choisissez ensuite Configurer votre zone de landing zone.

Étape 2a. Passez en revue et sélectionnez vos AWS régions

Assurez-vous d'avoir correctement désigné la AWS région que vous sélectionnez pour votre région d'origine. Une fois que vous avez déployé AWS Control Tower, vous ne pouvez pas modifier la région d'origine.

Dans cette section du processus de configuration, vous pouvez ajouter les AWS régions supplémentaires dont vous avez besoin. Vous pouvez ajouter d'autres régions ultérieurement, si nécessaire, et vous pouvez supprimer des régions de la gouvernance.

Pour sélectionner d'autres AWS régions à gouverner

1. Le panneau affiche les sélections de régions actuelles. Ouvrez le menu déroulant pour voir la liste des régions supplémentaires disponibles pour la gouvernance.

2. Cochez la case à côté de chaque région à intégrer à la gouvernance par AWS Control Tower. La région que vous avez sélectionnée n'est pas modifiable.

Pour refuser l'accès à certaines régions

Pour refuser l'accès aux AWS ressources et aux charges de travail dans certaines AWS régions, sélectionnez Activé dans la section relative au refus de contrôle de la région. Par défaut, le paramètre de ce contrôle est Non activé.

Étape 2b. Configurez vos unités organisationnelles (UO)

Si vous acceptez les noms par défaut de ces unités d'organisation, vous n'avez aucune action à effectuer pour que la configuration continue. Pour modifier le nom des unités d'organisation, entrez les nouveaux noms directement dans le champ du formulaire.

- UO de base — AWS Control Tower s'appuie sur une unité d'organisation de base initialement nommée unité d'organisation de sécurité. Vous pouvez modifier le nom de cette unité d'organisation lors de la configuration initiale et par la suite, à partir de la page de détails de l'unité d'organisation. Cette unité d'organisation de sécurité contient vos deux comptes partagés, appelés par défaut compte d'archivage du journal et compte d'audit.
- UO supplémentaire — AWS Control Tower peut configurer une ou plusieurs UO supplémentaires pour vous. Nous vous recommandons de prévoir au moins une unité d'organisation supplémentaire dans votre zone de landing, en plus de l'unité d'organisation de sécurité. Si cette unité d'organisation supplémentaire est destinée à des projets de développement, nous vous recommandons de la nommer unité d'organisation Sandbox, comme indiqué dans leDirectives pour la mise en place d'un environnement bien conçu. Si vous avez déjà une unité d'organisation existante dans AWS Organizations, vous pouvez voir s'afficher l'option permettant d'ignorer la configuration d'une unité d'organisation supplémentaire dans AWS Control Tower.

Étape 2c. Configuration de vos comptes partagés, de la journalisation et du chiffrement

Dans cette section du processus de configuration, le panneau affiche les sélections par défaut pour les noms de vos comptes AWS Control Tower partagés. Ces comptes constituent un élément essentiel de votre zone de landing zone. Ne déplacez ni ne supprimez ces comptes partagés. Vous pouvez choisir des noms personnalisés pour les comptes d'audit et d'archivage des journaux lors de la configuration. Vous pouvez également choisir une seule fois de définir les AWS comptes existants comme comptes partagés.

Vous devez fournir des adresses e-mail uniques pour vos comptes d'archivage de journaux et d'audit, et vous pouvez vérifier l'adresse e-mail que vous avez précédemment fournie pour votre compte de gestion. Cliquez sur le bouton Modifier pour modifier les valeurs par défaut modifiables.

À propos des comptes partagés

- Le compte de gestion — Le compte de gestion AWS Control Tower fait partie du niveau root. Le compte de gestion permet de facturer AWS Control Tower. Le compte dispose également d'autorisations d'administrateur pour votre zone de landing zone. Vous ne pouvez pas créer de comptes distincts pour la facturation et pour les autorisations d'administrateur dans AWS Control Tower.

  L'adresse e-mail indiquée pour le compte de gestion n'est pas modifiable pendant cette phase de configuration. Il s'affiche comme une confirmation, afin que vous puissiez vérifier que vous modifiez le bon compte de gestion, au cas où vous auriez plusieurs comptes.
- Les deux comptes partagés — Vous pouvez choisir des noms personnalisés pour ces deux comptes ou créer vos propres comptes, et vous devez fournir une adresse e-mail unique pour chaque compte, qu'il soit nouveau ou existant. Si vous choisissez qu'AWS Control Tower crée de nouveaux comptes partagés pour vous, les adresses e-mail ne doivent pas déjà être associées à AWS des comptes.

Pour configurer les comptes partagés, renseignez les informations demandées.

1. Sur la console, entrez le nom du compte initialement appelé compte d'archive du journal. De nombreux clients décident de conserver le nom par défaut de ce compte.
2. Fournissez une adresse e-mail unique pour ce compte.
3. Entrez un nom pour le compte initialement appelé compte d'audit. De nombreux clients choisissent de l'appeler le compte Security.
4. Fournissez une adresse e-mail unique pour ce compte.

Configurez éventuellement la conservation des journaux

Au cours de cette phase de configuration, vous pouvez personnaliser la politique de conservation des journaux pour les compartiments Amazon S3 qui stockent vos AWS CloudTrail journaux dans AWS Control Tower, par tranches de jours ou d'années, jusqu'à un maximum de 15 ans. Si vous choisissez de ne pas personnaliser la conservation de vos journaux, les paramètres par défaut sont d'un an pour la journalisation standard du compte et de 10 ans pour la journalisation des accès.

Cette fonctionnalité est également disponible lorsque vous mettez à jour ou réinitialisez votre zone d'atterrissage.

Gestion automatique de l'accès en Compte AWS option

Vous pouvez choisir si AWS Control Tower configure l' Compte AWS accès avec AWS Identity and Access Management (IAM) ou si vous souhaitez gérer vous-même l' Compte AWS accès, soit avec les utilisateurs, les rôles et les autorisations d' AWS IAM Identity Center que vous pouvez configurer et personnaliser vous-même, soit avec une autre méthode telle qu'un IdP externe, soit pour la fédération directe de comptes, soit pour la fédération à plusieurs comptes via IAM Identity Center. Vous pourrez modifier cette sélection ultérieurement.

Par défaut, AWS Control Tower configure l' AWS IAM Identity Center pour votre zone de landing zone, conformément aux recommandations relatives aux meilleures pratiques définies dans la section Organisation de votre AWS environnement à l'aide de plusieurs comptes. La plupart des clients choisissent la valeur par défaut. D'autres méthodes d'accès sont parfois nécessaires, pour des raisons de conformité réglementaire dans des secteurs ou des pays spécifiques, ou dans les pays Régions AWS où AWS IAM Identity Center n'est pas disponible.

La sélection de fournisseurs d'identité au niveau du compte n'est pas prise en charge. Cette option s'applique uniquement à la zone d'atterrissage dans son ensemble.

Pour plus d'informations, consultez Conseils relatifs à l'IAM Identity Center.

Configurez éventuellement AWS CloudTrail des sentiers

En tant que bonne pratique, nous vous recommandons de configurer la journalisation. Si vous souhaitez autoriser AWS Control Tower à configurer un suivi au niveau de l'organisation et à CloudTrail le gérer pour vous, choisissez Opt in. Si vous souhaitez gérer la journalisation à l'aide de vos propres CloudTrail sentiers ou d'un outil de journalisation tiers, choisissez Se désinscrire. Confirmez votre sélection lorsque cela est demandé dans la console. Vous pouvez modifier votre sélection et choisir d'accéder ou de refuser des parcours au niveau de l'organisation lorsque vous mettez à jour votre zone de landing zone.

Vous pouvez configurer et gérer vos propres CloudTrail sentiers à tout moment, y compris les sentiers au niveau de l'organisation et au niveau du compte. Si vous configurez des CloudTrail parcours dupliqués, vous risquez d'encourir des coûts supplémentaires lorsque les CloudTrail événements sont enregistrés.

Configurez éventuellement AWS KMS keys

Si vous souhaitez chiffrer et déchiffrer vos ressources à l'aide d'une clé de AWS KMS chiffrement, cochez la case. Si vous avez des clés existantes, vous pourrez les sélectionner parmi les identifiants affichés dans un menu déroulant. Vous pouvez générer une nouvelle clé en choisissant Créer une clé. Vous pouvez ajouter ou modifier une clé KMS à chaque fois que vous mettez à jour votre zone de landing zone.

Lorsque vous sélectionnez Set up landing zone, AWS Control Tower effectue une pré-vérification pour valider votre clé KMS. La clé doit répondre aux exigences suivantes :

- Activées
- Symétrique
- Il ne s'agit pas d'une clé multirégionale
- Les autorisations correctes ont été ajoutées à la politique
- La clé se trouve dans le compte de gestion

Une bannière d'erreur peut s'afficher si la clé ne répond pas à ces exigences. Dans ce cas, choisissez une autre clé ou générez une clé. Veillez à modifier la politique d'autorisation de la clé, comme décrit dans la section suivante.

Mettre à jour la politique relative aux clés KMS

Avant de pouvoir mettre à jour une politique de clé KMS, vous devez créer une clé KMS. Pour plus d'informations, consultez Création d'une stratégie de clé dans le Guide du développeur AWS Key Management Service .

Pour utiliser une clé KMS avec AWS Control Tower, vous devez mettre à jour la politique de clé KMS par défaut en ajoutant les autorisations minimales requises pour AWS Config et AWS CloudTrail. À titre de bonne pratique, nous vous recommandons d'inclure les autorisations minimales requises dans toute politique. Lorsque vous mettez à jour une politique de clé KMS, vous pouvez ajouter des autorisations en tant que groupe dans une seule instruction JSON ou ligne par ligne.

La procédure décrit comment mettre à jour la politique de clé KMS par défaut dans la AWS KMS console en ajoutant des instructions de politique autorisant AWS Config et CloudTrail à utiliser AWS KMS pour le chiffrement. Les déclarations de politique exigent que vous incluiez les informations suivantes :

- **YOUR-MANAGEMENT-ACCOUNT-ID**— l'ID du compte de gestion sur lequel AWS Control Tower sera configuré.
- **YOUR-HOME-REGION**— la région d'origine que vous allez sélectionner lors de la configuration d'AWS Control Tower.
- **YOUR-KMS-KEY-ID**— l'ID de clé KMS qui sera utilisé avec la politique.

Pour mettre à jour la politique relative aux clés KMS

1. Ouvrez la AWS KMS console à https://console.aws.amazon.com/kms
2. Dans le volet de navigation, sélectionnez Clés gérées par le client.
3. Dans le tableau, sélectionnez la clé que vous souhaitez modifier.
4. Dans l'onglet Stratégie clé, assurez-vous que vous pouvez consulter la politique clé. Si vous ne pouvez pas consulter la politique clé, choisissez Basculer vers l'affichage des politiques.
5. Choisissez Modifier, puis mettez à jour la politique de clé KMS par défaut en ajoutant les déclarations de stratégie suivantes pour AWS Config et CloudTrail.

   AWS Config déclaration de politique

```
{
    "Sid": "Allow Config to use KMS for encryption",
    "Effect": "Allow",
    "Principal": {
        "Service": "config.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": "arn:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:key/YOUR-KMS-KEY-ID"
}
```

   CloudTrail déclaration de politique

```
{
    "Sid": "Allow CloudTrail to use KMS for encryption",
    "Effect": "Allow",
    "Principal": {
```

```
            "Service": "cloudtrail.amazonaws.com"
        },
        "Action": [
            "kms:GenerateDataKey*",
            "kms:Decrypt"
        ],
        "Resource": "arn:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:key/YOUR-
KMS-KEY-ID",
        "Condition": {
            "StringEquals": {
                "aws:SourceArn": "arn:aws:cloudtrail:YOUR-HOME-REGION:YOUR-MANAGEMENT-
ACCOUNT-ID:trail/aws-controltower-BaselineCloudTrail"
            },
            "StringLike": {
                "kms:EncryptionContext:aws:cloudtrail:arn": "arn:aws:cloudtrail:*:YOUR-
MANAGEMENT-ACCOUNT-ID:trail/*"
            }
        }
}
```

6. Sélectionnez Enregistrer les modifications.

Exemple de politique relative aux clés KMS

L'exemple de politique suivant montre à quoi pourrait ressembler votre politique de clé KMS une fois que vous aurez ajouté les déclarations de politique qui accordent AWS Config CloudTrail les autorisations minimales requises. L'exemple de politique n'inclut pas votre politique de clé KMS par défaut.

```
{
    "Version": "2012-10-17",
    "Id": "CustomKMSPolicy",
    "Statement": [
        {
        ... YOUR-EXISTING-POLICIES ...
        },
        {
            "Sid": "Allow Config to use KMS for encryption",
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": [
```

```
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID"
        },
        {
            "Sid": "Allow CloudTrail to use KMS for encryption",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
              ],
            "Resource": "arn:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": "arn:aws:cloudtrail:YOUR-HOME-REGION:YOUR-
MANAGEMENT-ACCOUNT-ID:trail/aws-controltower-BaselineCloudTrail"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:YOUR-MANAGEMENT-ACCOUNT-ID:trail/*"
                }
            }
        }
    ]
}
```

Pour consulter d'autres exemples de politiques, consultez les pages suivantes :

- Octroi d'autorisations de chiffrement dans le guide de AWS CloudTrail l'utilisateur.
- Autorisations requises pour la clé KMS lors de l'utilisation de rôles liés à un service (livraison de compartiments S3) dans le guide du développeur.AWS Config

Protégez-vous contre les attaquants

En ajoutant certaines conditions à vos politiques, vous pouvez contribuer à empêcher un type d'attaque spécifique, connu sous le nom d'attaque adjointe confuse, qui se produit lorsqu'une entité contraint une entité plus privilégiée à effectuer une action, par exemple dans le cas d'une usurpation d'identité interservices. Pour des informations générales sur les conditions du contrat, voir égalementSpécification de conditions dans une politique.

Le AWS Key Management Service (AWS KMS) vous permet de créer des clés KMS multirégionales et des clés asymétriques ; cependant, AWS Control Tower ne prend pas en charge les clés multirégionales ou asymétriques. AWS Control Tower effectue une pré-vérification de vos clés existantes. Un message d'erreur peut s'afficher si vous sélectionnez une clé multirégionale ou une clé asymétrique. Dans ce cas, générez une autre clé à utiliser avec les ressources AWS Control Tower.

Pour plus d'informations AWS KMS, consultez le guide du AWS KMS développeur.

Notez que les données des clients dans AWS Control Tower sont chiffrées au repos, par défaut, à l'aide de SSE-S3.

Configurez et créez éventuellement des comptes de membres personnalisés

Lorsque vous suivez le flux de travail de création de compte pour ajouter vos comptes membres, vous pouvez éventuellement spécifier un plan défini au préalable à utiliser pour le provisionnement de comptes membres personnalisés depuis la console AWS Control Tower. Vous pourrez personnaliser les comptes ultérieurement si aucun plan n'est disponible. veuillez consulter Personnalisez les comptes avec Account Factory Customization (AFC).

Étape 3. Vérifiez et configurez la zone d'atterrissage

La section suivante de la configuration indique les autorisations dont AWS Control Tower a besoin pour votre zone de landing zone. Cochez une case pour développer chaque sujet. Il vous sera demandé d'accepter ces autorisations, qui peuvent affecter plusieurs comptes, et d'accepter les conditions générales d'utilisation.

Pour finaliser

1. Sur la console, passez en revue les autorisations du service et, lorsque vous serez prêt, choisissez Je comprends les autorisations qu'AWS Control Tower utilisera pour administrer les AWS ressources et appliquer les règles en mon nom.

2. Pour finaliser vos sélections et initialiser le lancement, choisissez Configurer la zone d'atterrissage.

Cette série d'étapes lance le processus de configuration de votre zone d'atterrissage, qui peut prendre environ trente minutes. Lors de la configuration, AWS Control Tower crée votre niveau racine, l'unité d'organisation de sécurité et les comptes partagés. D'autres AWS ressources sont créées, modifiées ou supprimées.

> ⚠ Confirmer les abonnements SNS
>
> L'adresse e-mail que vous avez fournie pour le compte d'audit recevra des e-mails de AWS notification et de confirmation d'abonnement provenant de toutes les AWS régions prises en charge par AWS Control Tower. Pour recevoir des e-mails de conformité sur votre compte d'audit, vous devez choisir le lien de confirmation d'abonnement contenu dans chaque e-mail provenant de chaque AWS région prise en charge par AWS Control Tower.

Commencer à utiliser AWS Control Tower à l'aide des API

Cette procédure de démarrage est destinée aux administrateurs d'AWS Control Tower. Cette procédure nécessite quelques prérequis et comprend deux étapes principales.

Dans cette procédure, vous allez utiliser les API d'AWS Control Tower et d'autres AWS services pour configurer et lancer une zone de landing zone. Ces API vous permettent de créer un environnement AWS Control Tower par programmation, soit par le biais de la AWS CloudFormation console, soit par le biais du AWS CLI.

Avant de lancer votre zone de landing zone AWS Control Tower, effectuez les tâches préalables suivantes :

- Déterminez la région d'origine la plus appropriée. Pour plus d'informations, consultez Conseils administratifs pour la configuration de la zone d'atterrissage .
- Consultez cet Prérequis : vérifications automatisées avant le lancement de votre compte de gestion article pour en savoir plus sur les contrôles automatisés effectués avant le lancement afin de vous assurer que votre compte de gestion est prêt à accepter les modifications visant à définir votre zone d'atterrissage.

Rubriques

Attentes relatives à la configuration de la zone d'atterrissage à l'aide d'API

Le processus de configuration de votre zone de landing AWS Control Tower comporte plusieurs étapes. Certains aspects de votre zone de landing zone AWS Control Tower sont configurables. Les autres choix ne peuvent pas être modifiés après la configuration.

Éléments clés à configurer lors de l'installation

- Vous pouvez sélectionner les noms de vos unités d'organisation de base lors de la configuration, et vous pouvez également modifier les noms de vos unités d'organisation après avoir configuré votre zone de landing zone. Par défaut, les unités d'organisation fondamentales sont nommées Security et Sandbox. Pour plus d'informations, consultez Directives pour la mise en place d'un environnement bien conçu.
- Lors de la configuration, vous pouvez sélectionner des noms personnalisés pour les comptes partagés créés par AWS Control Tower, appelés archive de journaux et audit par défaut, mais vous ne pouvez pas modifier ces noms après la configuration. (Il s'agit d'une sélection unique.)
- Lors de la configuration avec les API, vous devez spécifier les AWS comptes existants qu'AWS Control Tower utilisera comme comptes d'audit et d'archivage des journaux. Pour spécifier AWS des comptes existants, si ces comptes disposent de AWS Config ressources existantes, vous devez supprimer ou modifier les AWS Config ressources existantes avant de pouvoir les inscrire dans AWS Control Tower. (Il s'agit d'une sélection unique.)
- Si vous effectuez la configuration pour la première fois ou si vous passez à la version 3.0 de landing zone, vous pouvez choisir d'autoriser AWS Control Tower à configurer un AWS CloudTrail parcours au niveau de l'organisation pour votre organisation, ou de vous désinscrire des sentiers

gérés par AWS Control Tower et de gérer vos propres CloudTrail sentiers. Vous pouvez accepter ou refuser les pistes au niveau de l'organisation qui sont gérées par AWS Control Tower chaque fois que vous mettez à jour votre zone de landing zone.

- Vous pouvez éventuellement définir une politique de rétention personnalisée pour votre bucket de log et votre bucket d'accès aux logs Amazon S3, lorsque vous configurez ou mettez à jour votre zone de landing zone.

Choix de configuration qui ne peuvent pas être annulés

- Vous ne pouvez pas modifier votre région d'origine une fois que vous avez configuré votre zone de landing zone.
- Si vous approvisionnez des comptes avec des VPC, les CIDR VPC ne peuvent pas être modifiés une fois qu'ils ont été créés.

Les sections suivantes présentent en détail les prérequis et les étapes de configuration, avec des explications et des mises en garde. Pour des exemples de code supplémentaires, voirExemples : configurer une zone de landing zone AWS Control Tower avec des API uniquement.

Étape 1 : Configurez votre zone de landing zone

Le processus de configuration de votre zone de landing AWS Control Tower comporte plusieurs étapes. Certains aspects de votre zone de landing zone AWS Control Tower sont configurables, mais les autres choix ne peuvent pas être modifiés après la configuration. Pour en savoir plus sur ces considérations importantes avant de lancer votre zone d'atterrissage, consultez Attentes relatives à la configuration de la zone d'atterrissage .

Avant d'utiliser les API de zone d'atterrissage d'AWS Control Tower, vous devez d'abord appeler les API d'autres AWS services pour configurer votre zone d'atterrissage avant le lancement. Le processus comprend trois étapes principales :

- créer une nouvelle AWS Organizations organisation,
- configurer les adresses e-mail de votre compte partagé,
- et en créant un rôle IAM ou un utilisateur de l'IAM Identity Center disposant des autorisations requises pour appeler les API de la zone d'atterrissage.

Étape 1. Créez l'organisation qui contiendra votre zone de landing zone :

1. Appelez l' AWS Organizations `CreateOrganization`API et activez toutes les fonctionnalités pour créer l'unité d'organisation fondamentale. AWS Control Tower l'appelle initialement Security OU. Cette unité d'organisation de sécurité contient vos deux comptes partagés, appelés par défaut compte d'archivage du journal et compte d'audit.

   ```
   aws organizations create-organization --feature-set ALL
   ```

   AWS Control Tower peut configurer une ou plusieurs unités d'organisation supplémentaires. Nous vous recommandons de prévoir au moins une unité d'organisation supplémentaire dans votre zone de landing, en plus de l'unité d'organisation de sécurité. Si cette unité d'organisation supplémentaire est destinée à des projets de développement, nous vous recommandons de la nommer unité d'organisation Sandbox, comme indiqué dans leAWS stratégie multi-comptes pour votre zone de landing zone AWS Control Tower.

Étape 2. Provisionnez des comptes partagés si nécessaire :

Pour configurer votre zone de landing zone, AWS Control Tower a besoin de deux adresses e-mail. Si vous utilisez des API de zone d'atterrissage pour configurer AWS Control Tower pour la première fois, vous devez utiliser les AWS comptes de sécurité et d'archivage de journaux existants. Vous pouvez utiliser les adresses e-mail actuelles des adresses e-mail existantes Comptes AWS. Chacune de ces adresses e-mail servira de boîte de réception collaborative (un compte e-mail partagé) destinée aux différents utilisateurs de votre entreprise chargés de tâches spécifiques liées à AWS Control Tower.

Pour commencer à configurer une nouvelle zone de landing zone, si vous n'avez pas de AWS compte existant, vous pouvez configurer les comptes de sécurité et d'archivage AWS des journaux à l'aide d' AWS Organizations API.

1. Appelez l' AWS Organizations `CreateAccount`API pour créer le compte d'archivage du journal et le compte d'audit dans l'unité d'organisation de sécurité.

   ```
   aws organizations create-account --email mylog@example.com --account-name "Logging
    Account"
   ```

   ```
   aws organizations create-account --email mysecurity@example.com --account-name
    "Security Account"
   ```

2. (Facultatif) Vérifiez le statut de l'`CreateAccount`opération à l'aide de l' AWS Organizations `DescribeAccount`API.

Étape 3. Créez les rôles de service requis

Créez les rôles de service IAM suivants qui permettent à AWS Control Tower d'effectuer les appels d'API nécessaires à la configuration de votre zone de landing zone :

- `AWSControlTowerAdmin`
- `AWSControlTowerCloudTrailRole`
- `AWSControlTowerStackSetRole`
- `AWSControlTowerConfigAggregatorRoleForOrganizations`

Pour plus d'informations sur ces rôles et leurs politiques, consultezUtilisation de politiques basées sur l'identité (politiques IAM) pour AWS Control Tower.

Pour créer un rôle IAM :

1. Créez un rôle IAM avec les autorisations nécessaires pour appeler toutes les API de zone d'atterrissage. Vous pouvez également créer un utilisateur IAM Identity Center et lui attribuer les autorisations nécessaires.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "controltower:CreateLandingZone",
                "controltower:UpdateLandingZone",
                "controltower:ResetLandingZone",
                "controltower:DeleteLandingZone",
                "controltower:GetLandingZoneOperation",
                "controltower:GetLandingZone",
                "controltower:ListLandingZones",
                "controltower:ListTagsForResource",
                "controltower:TagResource",
                "controltower:UntagResource",
                "servicecatalog:*",
                "organizations:*",
```

```
                "sso:*",
                "sso-directory:*",
                "logs:*",
                "cloudformation:*",
                "kms:*",
                "iam:GetRole",
                "iam:CreateRole",
                "iam:GetSAMLProvider",
                "iam:CreateSAMLProvider",
                "iam:CreateServiceLinkedRole",
                "iam:ListRolePolicies",
                "iam:PutRolePolicy",
                "iam:ListAttachedRolePolicies",
                "iam:AttachRolePolicy",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Étape 2 : Lancez votre zone de landing zone

L'`CreateLandingZone`API AWS Control Tower nécessite une version de zone d'atterrissage et un fichier manifeste comme paramètres d'entrée. Vous pouvez utiliser le fichier manifeste pour configurer les fonctionnalités suivantes :

- Configurez éventuellement la conservation des journaux
- Gestion automatique de l'accès en Compte AWS option
- Configurez éventuellement AWS CloudTrail des sentiers
- Configurez éventuellement AWS KMS keys

Après avoir compilé votre fichier manifeste, vous êtes prêt à créer une nouvelle zone de landing zone.

> **Note**
>
> AWS Control Tower ne prend pas en charge le refus de contrôle par région lors de l'utilisation d'API pour configurer et lancer une zone de landing zone. Après avoir lancé avec succès votre zone de landing zone à l'aide d'API, vous pouvez utiliser la console AWS Control Tower pour configurer le contrôle de refus de la région.

1. Appelez l'`CreateLandingZone`API AWS Control Tower. Cette API nécessite une version de zone d'atterrissage et un fichier manifeste en entrée.

```
aws controltower create-landing-zone --landing-zone-version 3.3 --manifest "file://
LandingZoneManifest.json"
```

Exemple de manifeste LandingZoneManifest.json :

```
{
   "governedRegions": ["us-west-2","us-west-1"],
   "organizationStructure": {
       "security": {
           "name": "CORE"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   },
   "centralizedLogging": {
        "accountId": "222222222222",
        "configurations": {
            "loggingBucket": {
                "retentionDays": 60
            },
            "accessLoggingBucket": {
                "retentionDays": 60
            },
            "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX"
        },
        "enabled": true
   },
   "securityRoles": {
```

```
        "accountId": "333333333333"
    },
    "accessManagement": {
        "enabled": true
    }
}
```

> **Note**
>
> Comme indiqué dans l'exemple, les SecurityRoles comptes AccountIdfor CentralizedLogging et doivent être différents.

Sortie :

```
{
   "arn": "arn:aws:controltower:us-west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H",
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

2. Appelez l'`GetLandingZoneOperation`API pour vérifier le statut de l'`CreateLandingZone`opération. L'`GetLandingZoneOperation`API renvoie le statut `SUCCEEDED`FAILED, ou`IN_PROGRESS`.

```
aws controltower get-landing-zone-operation --operation-identifier "55XXXXXX-
eXXX-4XXX-aXXX-44XXXXXXXXXX"
```

Sortie :

```
{
    "operationDetails": {
        "operationType": "CREATE",
        "startTime": "Thu Nov 09 20:39:19 UTC 2023",
        "endTime": "Thu Nov 09 21:02:01 UTC 2023",
        "status": "SUCCEEDED"
    }
}
```

3. Lorsque le statut redevient « comme »`SUCCEEDED`, vous pouvez appeler l'`GetLandingZone`API pour vérifier la configuration de la zone d'atterrissage.

```
aws controltower get-landing-zone --landing-zone-identifier "arn:aws:controltower:us-
west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
```

Sortie :

```
{
    "landingZone": {
        "arn": "arn:aws:controltower:us-
west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H",
        "driftStatus": {
            "status": "IN_SYNC"
        },
        "latestAvailableVersion": "3.3",
        "manifest": {
            "accessManagement": {
                "enabled": true
            },
            "securityRoles": {
                "accountId": "333333333333"
            },
            "governedRegions": [
                "us-west-1",
                "eu-west-3",
                "us-west-2"
            ],
            "organizationStructure": {
                "sandbox": {
                    "name": "Sandbox"
                },
                "security": {
                    "name": "CORE"
                }
            },
            "centralizedLogging": {
                "accountId": "222222222222",
                "configurations": {
                    "loggingBucket": {
                        "retentionDays": 60
                    },
                    "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX",
                    "accessLoggingBucket": {
```

```
                        "retentionDays": 60
                    }
                },
                "enabled": true
            }
        },
        "status": "PROCESSING",
        "version": "3.3"
    }
}
```

Identifiez votre zone de landing

`ListLandingZones`Les appels peuvent vous aider à déterminer si votre compte est déjà configuré avec AWS Control Tower. Cette API renvoie un identifiant de zone d'atterrissage (ARN) dans n'importe quelle région commerciale, quelle que soit la région d'origine de la zone d'atterrissage. Les ARN des zones d'atterrissage sont uniques au niveau régional.

```
aws controltower list-landing-zones --region us-east-1
```

Pour les régions optionnelles, l'`ListLandingZones`API renvoie l'identifiant de la zone d'atterrissage uniquement si vous appelez l'API dans la même région que la région d'origine de l'API. Par exemple, si votre zone d'atterrissage est configurée dans af-south-1 et que vous appelez af-south-1, l'API renvoie `ListLandingZones` l'identifiant de la zone d'atterrissage. Si votre zone d'atterrissage est configurée dans af-south-1 et que vous appelez **`ListLandingZones`** ap-east-1, l'API ne renvoie pas l'identifiant de la zone d'atterrissage.

Sortie :

```
{
   "landingZones" [
        "arn": "arn:aws:controltower:us-
west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
   ]
}
```

Mettez à jour votre zone de landing zone

Lorsqu'une nouvelle version de zone d'atterrissage est disponible ou pour apporter d'autres modifications à la configuration de votre zone d'atterrissage, vous pouvez appeler l'`UpdateLandingZone`API et référencer un fichier manifeste mis à jour. Cette API renvoie un`OperationIdentifier`, que vous pouvez ensuite utiliser lorsque vous appelez l'`GetLandingZoneOperation`API pour vérifier l'état de l'opération de mise à jour.

Pour mettre à jour la zone d'atterrissage

1. Appelez l'`UpdateLandingZone`API AWS Control Tower et consultez la version mise à jour de la zone de landing zone ou votre manifeste mis à jour.

```
aws controltower update-landing-zone --landing-zone-version 3.3 --landing-zone-
identifier "arn:aws:controltower:us-west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
 --manifest file://LandingZoneManifest.json
```

LandingZoneManifest.json :

```
{
   "governedRegions": ["us-west-2","us-west-1"],
   "organizationStructure": {
       "security": {
           "name": "CORE"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   },
   "centralizedLogging": {
        "accountId": "222222222222",
        "configurations": {
            "loggingBucket": {
                "retentionDays":2555
            },
            "accessLoggingBucket": {
                "retentionDays": 2555
            },
            "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX"
        },
```

```
        "enabled": true
    },
    "securityRoles": {
        "accountId": "333333333333"
    },
    "accessManagement": {
        "enabled": true
    }
}
```

Sortie :

```
{
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

> **Réenregistrez éventuellement l'unité d'organisation pour mettre à jour les comptes**
>
> Pour les unités d'organisation AWS Control Tower enregistrées avec moins de 300 comptes, vous pouvez utiliser la console AWS Control Tower pour accéder à la page de l'unité d'organisation dans le tableau de bord et sélectionner Réenregistrer l'unité d'organisation pour mettre à jour les comptes de cette unité d'organisation.

Réinitialisez la zone d'atterrissage pour résoudre le problème de dérive

Lorsque vous créez votre zone d'atterrissage, celle-ci ainsi que toutes les unités organisationnelles (UO), les comptes et les ressources sont conformes aux règles de gouvernance appliquées par les contrôles que vous avez choisis. Lorsque vous et les membres de votre organisation utilisez la zone d'atterrissage, des modifications de ce statut de conformité peuvent se produire. Ces modifications sont appelées dérive.

Pour savoir si votre zone d'atterrissage est en dérive, vous pouvez appeler l'`GetLandingZone`API. Cette API renvoie l'état de dérive de la zone d'atterrissage `DRIFTED` ou`IN_SYNC`.

Pour résoudre le problème de dérive dans votre zone d'atterrissage, vous pouvez utiliser l'`ResetLandingZone`API pour rétablir la configuration d'origine de la zone d'atterrissage. Par exemple, AWS Control Tower active IAM Identity Center par défaut pour vous aider à gérer votre Comptes AWS, mais si vous configurez les paramètres de votre zone d'atterrissage d'origine avec

IAM Identity Center désactivé, l'appel `ResetLandingZone` maintient cette désactivation de la configuration IAM Identity Center.

Vous ne pouvez utiliser l'`ResetLandingZone`API que si vous utilisez la dernière version disponible pour la zone de landing zone. Vous pouvez appeler l'`GetLandingZone`API et comparer la version de votre zone d'atterrissage avec la dernière version disponible. Si nécessaire, vous pouvez faire en Mettez à jour votre zone de landing zone sorte que votre zone d'atterrissage utilise la dernière version disponible. Dans ces exemples, nous utilisons la version 3.3 comme dernière version.

1. Appelez l'API `GetLandingZone`. Si l'API renvoie un statut de dérive de`DRIFTED`, votre zone d'atterrissage est en dérive.
2. Appelez l'`ResetLandingZone`API pour rétablir la configuration d'origine de votre zone d'atterrissage.

```
aws controltower reset-landing-zone --landing-zone-identifier
 "arn:aws:controltower:us-west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
```

Sortie :

```
{
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

> **Note**
>
> La réinitialisation de la zone d'atterrissage ne met pas à jour la version de la zone d'atterrissage. Consultez Mettez à jour votre zone de landing zone pour plus de détails sur la mise à jour de la version de la zone d'atterrissage.

Démantelez votre zone d'atterrissage

Le processus de nettoyage de toutes les ressources d'une zone d'atterrissage est appelé mise hors service d'une zone d'atterrissage.

> **Important**
>
> Nous vous recommandons fortement de n'effectuer ce processus de désaffectation que si vous avez l'intention de cesser d'utiliser la zone de destination concernée. Il n'est pas possible de recréer la zone de destination après la désaffectation.

Pour plus de détails sur la mise hors service d'une zone d'atterrissage, y compris des informations importantes sur la manière dont AWS Control Tower gère vos données et celles qui existent déjà AWS Organizations, consultez. Procédure pas à pas : mise hors service d'une zone d'atterrissage d'une AWS Control Tower

Pour mettre hors service une zone d'atterrissage, appelez `DeleteLandingZone` l'API. Cette API renvoie un`OperationIdentifier`, que vous pouvez ensuite utiliser lorsque vous appelez l'`GetLandingZoneOperation`API pour vérifier l'état de l'opération de suppression.

```
aws controltower delete-landing-zone --landing-zone-identifier
"arn:aws:controltower:us-west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H"
```

Sortie :

```
{
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

Exemples : configurer une zone de landing zone AWS Control Tower avec des API uniquement

Cette présentation d'exemples est un document d'accompagnement. Pour obtenir des explications, des mises en garde et plus d'informations, consultez Getting started with AWS Control Tower using APIs.

Prérequis

Avant de créer une zone de landing zone AWS Control Tower, vous devez créer une organisation, deux comptes partagés et certains rôles IAM. Ce didacticiel pas à pas inclut ces étapes, avec des exemples de commandes et de sorties de la CLI.

Étape 1. Créez l'organisation et les deux comptes requis.

```
aws organizations create-organization --feature-set ALL
aws organizations create-account --email example+log@example.com --account-name "Log
 archive account"
aws organizations create-account --email example+aud@example.com --account-name "Audit
 account"
```

Étape 2. Créez les rôles IAM requis.

`AWSControlTowerAdmin`

```
cat <<EOF >controltower_trust.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "controltower.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF
aws iam create-role --role-name AWSControlTowerAdmin --path /service-role/ --assume-
role-policy-document file://controltower_trust.json
cat <<EOF >ct_admin_role_policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*"
        }
    ]
}
EOF
aws iam put-role-policy --role-name AWSControlTowerAdmin --policy-name
 AWSControlTowerAdminPolicy --policy-document file://ct_admin_role_policy.json
```

```
aws iam attach-role-policy --role-name AWSControlTowerAdmin --policy-arn
 arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy
```

AWSControlTowerCloudTrailRole

```
cat <<EOF >controltower_trust.json
        {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
EOF
aws iam create-role --role-name AWSControlTowerCloudTrailRole --path /service-role/ --
assume-role-policy-document file://cloudtrail_trust.json
cat <<EOF >cloudtrail_role_policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "logs:CreateLogStream",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
            "Effect": "Allow"
        },
        {
            "Action": "logs:PutLogEvents",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
            "Effect": "Allow"
        }
    ]
}
EOF
aws iam put-role-policy --role-name AWSControlTowerCloudTrailRole --
policy-name AWSControlTowerCloudTrailRolePolicy --policy-document file://
cloudtrail_role_policy.json
```

AWSControlTowerStackSetRole

```
cat <<EOF >cloudformation_trust.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudformation.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
EOF
aws iam create-role --role-name AWSControlTowerStackSetRole --path /service-role/ --
assume-role-policy-document file://cloudformation_trust.json
cat <<EOF >stackset_role_policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution"
            ],
            "Effect": "Allow"
        }
    ]
}
EOF
aws iam put-role-policy --role-name AWSControlTowerStackSetRole --policy-name
 AWSControlTowerStackSetRolePolicy --policy-document file://stackset_role_policy.json
```

AWSControlTowerConfigAggregatorRoleForOrganizations

```
cat <<EOF >config_trust.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
EOF
aws iam create-role --role-name AWSControlTowerConfigAggregatorRoleForOrganizations --
path /service-role/ --assume-role-policy-document file://config_trust.json
aws iam attach-role-policy --role-name
 AWSControlTowerConfigAggregatorRoleForOrganizations --policy-arn
 arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations
```

Étape 3. Obtenez les identifiants de compte et générez le fichier manifeste de la zone d'atterrissage.

Les deux premières commandes de l'exemple suivant stockent les identifiants des comptes que vous avez créés à l'étape 1 dans des variables. Ces variables aident ensuite à générer le fichier manifeste de la zone d'atterrissage.

```
sec_account_id=$(aws organizations list-accounts | jq -r '.Accounts[] | select(.Name ==
 "Audit account") | .Id')
log_account_id=$(aws organizations list-accounts | jq -r '.Accounts[] | select(.Name ==
 "Log archive account") | .Id')

cat <<EOF >landing_zone_manifest.json
{
   "governedRegions": ["us-west-1", "us-west-2"],
   "organizationStructure": {
       "security": {
           "name": "Security"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   },
   "centralizedLogging": {
        "accountId": "$log_account_id",
        "configurations": {
            "loggingBucket": {
                "retentionDays": 60
            },
            "accessLoggingBucket": {
```

```
                "retentionDays": 60
            }
        },
        "enabled": true
    },
    "securityRoles": {
        "accountId": "$sec_account_id"
    },
    "accessManagement": {
        "enabled": true
    }
}
EOF
```

Étape 4. Créez la zone d'atterrissage avec la dernière version.

Vous devez configurer la zone de landing zone avec le fichier manifeste et la dernière version. Cet exemple montre la version 3.3.

```
aws --region us-west-1 controltower create-landing-zone --manifest file://
landing_zone_manifest.json --landing-zone-version 3.3
```

La sortie contiendra un arn et un OperationIdentifier, comme indiqué dans l'exemple suivant.

```
{
    "arn": "arn:aws:controltower:us-west-1:0123456789012:landingzone/4B3H0ULNUOL2AXXX",
    "operationIdentifier": "16bb47f7-b7a2-4d90-bc71-7df4ca1201xx"
}
```

Étape 5. (Facultatif) Suivez l'état de votre opération de création de zone d'atterrissage.

Pour suivre l'état, utilisez l'OperationIdentifier issu de la sortie de la `create-landing-zone` commande précédente.

```
aws --region us-west-1 controltower get-landing-zone-operation --operation-identifier
 16bb47f7-b7a2-4d90-bc71-7df4ca1201xx
```

Exemple de sortie d'état :

```
{
    "operationDetails": {
```

```
        "operationType": "CREATE",
        "startTime": "2024-02-28T21:49:31Z",
        "status": "IN_PROGRESS"
    }
}
```

Vous pouvez utiliser l'exemple de script suivant pour vous aider à configurer une boucle qui indique l'état de l'opération à plusieurs reprises, comme un fichier journal. Dans ce cas, vous n'avez pas besoin de continuer à saisir la commande.

```
while true; do echo "$(date) $(aws --region us-west-1 controltower get-landing-
zone-operation --operation-identifier 16bb47f7-b7a2-4d90-bc71-7df4ca1201xx | jq -
r .operationDetails.status)"; sleep 15; done
```

Pour afficher des informations détaillées sur votre zone de landing

Étape 1. Trouvez l'ARN de la zone de landing

```
aws --region us-west-1 controltower list-landing-zones
```

La sortie inclura l'identifiant de la zone d'atterrissage, comme indiqué dans l'exemple de sortie suivant.

```
{
    "landingZones": [
        {
            "arn": "arn:aws:controltower:us-
west-1:123456789012:landingzone/4B3H0ULNUOL2AXXX"
        }
    ]
}
```

Étape 2. Obtenez les informations

```
aws --region us-west-1 controltower get-landing-zone --landing-zone-identifier
 arn:aws:controltower:us-west-1:123456789012:landingzone/4B3H0ULNUOL2AXXX
```

Voici un exemple du type de sortie que vous pouvez voir :

```
{
    "landingZone": {
```

```
        "arn": "arn:aws:controltower:us-
west-1:123456789012:landingzone/4B3H0ULNUOL2AXXX",
        "driftStatus": {
            "status": "IN_SYNC"
        },
        "latestAvailableVersion": "3.3",
        "manifest": {
            "accessManagement": {
                "enabled": true
            },
            "securityRoles": {
                "accountId": "9750XXXX4444"
            },
            "governedRegions": [
                "us-west-1",
                "us-west-2"
            ],
            "organizationStructure": {
                "sandbox": {
                    "name": "Sandbox"
                },
                "security": {
                    "name": "Security"
                }
            },
            "centralizedLogging": {
                "accountId": "012345678901",
                "configurations": {
                    "loggingBucket": {
                        "retentionDays": 60
                    },
                    "accessLoggingBucket": {
                        "retentionDays": 60
                    }
                },
                "enabled": true
            }
        },
        "status": "ACTIVE",
        "version": "3.3"
    }
}
```

Lancement d'une zone d'atterrissage à l'aide de AWS CloudFormation

Vous pouvez configurer et lancer une zone d' AWS CloudFormation atterrissage via la AWS CloudFormation console ou via le AWS CLI. Cette section fournit des instructions et des exemples pour lancer une zone d'atterrissage à l'aide d'API via AWS CloudFormation.

Rubriques

Conditions préalables au lancement d'une zone d'atterrissage à l'aide de AWS CloudFormation

1. À partir du AWS CLI, utilisez l' AWS Organizations `CreateOrganization`API pour créer une organisation et activer toutes les fonctionnalités.

   Pour des instructions plus détaillées, consultez Étape 1 : Configurez votre zone de landing zone .
2. À partir de la AWS CloudFormation console ou à l'aide du AWS CLI, déployez un AWS CloudFormation modèle qui crée les ressources suivantes dans le compte de gestion :
   - Compte Log Archive (parfois appelé compte « Logging »)
   - Compte d'audit (parfois appelé compte « Sécurité »)
   - Les rôles AWSControlTowerAdminAWSControlTowerCloudTrailRole, AWSControlTowerConfigAggregatorRoleForOrganizations, et AWSControlTowerStackSetRolede service.

     Pour plus d'informations sur la manière dont AWS Control Tower utilise ces rôles pour effectuer des appels d'API de zone d'atterrissage, consultez Étape 1 : Configuration de votre zone d'atterrissage.

```
Parameters:
  LoggingAccountEmail:
    Type: String
    Description: The email Id for centralized logging account
  LoggingAccountName:
    Type: String
    Description: Name for centralized logging account
```

```
  SecurityAccountEmail:
    Type: String
    Description: The email Id for security roles account
  SecurityAccountName:
    Type: String
    Description: Name for security roles account
Resources:
  MyOrganization:
    Type: 'AWS::Organizations::Organization'
    Properties:
      FeatureSet: ALL
  LoggingAccount:
    Type: 'AWS::Organizations::Account'
    Properties:
      AccountName: !Ref LoggingAccountName
      Email: !Ref LoggingAccountEmail
  SecurityAccount:
    Type: 'AWS::Organizations::Account'
    Properties:
      AccountName: !Ref SecurityAccountName
      Email: !Ref SecurityAccountEmail
  AWSControlTowerAdmin:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerAdmin
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: controltower.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
      ManagedPolicyArns:
        - !Sub >-
          arn:${AWS::Partition}:iam::aws:policy/service-role/
AWSControlTowerServiceRolePolicy
  AWSControlTowerAdminPolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyName: AWSControlTowerAdminPolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
```

```
          - Effect: Allow
            Action: 'ec2:DescribeAvailabilityZones'
            Resource: '*'
      Roles:
        - !Ref AWSControlTowerAdmin
  AWSControlTowerCloudTrailRole:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerCloudTrailRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: cloudtrail.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
  AWSControlTowerCloudTrailRolePolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyName: AWSControlTowerCloudTrailRolePolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Action:
              - 'logs:CreateLogStream'
              - 'logs:PutLogEvents'
            Resource: !Sub >-
              arn:${AWS::Partition}:logs:*:*:log-group:aws-controltower/
CloudTrailLogs:*
            Effect: Allow
      Roles:
        - !Ref AWSControlTowerCloudTrailRole
  AWSControlTowerConfigAggregatorRoleForOrganizations:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerConfigAggregatorRoleForOrganizations
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: config.amazonaws.com
            Action: 'sts:AssumeRole'
```

```
      Path: '/service-role/'
      ManagedPolicyArns:
        - !Sub arn:${AWS::Partition}:iam::aws:policy/service-role/
AWSConfigRoleForOrganizations
  AWSControlTowerStackSetRole:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerStackSetRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: cloudformation.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
  AWSControlTowerStackSetRolePolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyName: AWSControlTowerStackSetRolePolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Action: 'sts:AssumeRole'
            Resource: !Sub 'arn:${AWS::Partition}:iam::*:role/
AWSControlTowerExecution'
            Effect: Allow
      Roles:
        - !Ref AWSControlTowerStackSetRole

Outputs:
  LogAccountId:
    Value:
      Fn::GetAtt: LoggingAccount.AccountId
    Export:
      Name: LogAccountId
  SecurityAccountId:
    Value:
      Fn::GetAtt: SecurityAccount.AccountId
    Export:
      Name: SecurityAccountId
```

Créez une nouvelle zone de landing en utilisant AWS CloudFormation

À partir de la AWS CloudFormation console ou à l'aide du AWS CLI, déployez le AWS CloudFormation modèle suivant pour créer une zone d'atterrissage.

```
Parameters:
  Version:
    Type: String
    Description: The version number of Landing Zone
  GovernedRegions:
    Type: List
    Description: List of governed regions
  SecurityOuName:
    Type: String
    Description: The security Organizational Unit name
  SandboxOuName:
    Type: String
    Description: The sandbox Organizational Unit name
  CentralizedLoggingAccountId:
    Type: String
    Description: The AWS account ID for centralized logging
  SecurityAccountId:
    Type: String
    Description: The AWS account ID for security roles
  LoggingBucketRetentionPeriod:
    Type: Number
    Description: Retention period for centralized logging bucket
  AccessLoggingBucketRetentionPeriod:
    Type: Number
    Description: Retention period for access logging bucket
  KMSKey:
    Type: String
    Description: KMS key ARN used by CloudTrail and Config service to encrypt data in
 logging bucket
Resources:
  MyLandingZone:
    Type: 'AWS::ControlTower::LandingZone'
    Properties:
      Version:
        Ref: Version
      Tags:
        - Key: "keyname1"
          Value: "value1"
```

```
        - Key: "keyname2"
          Value: "value2"
      Manifest:
        governedRegions:
          Ref: GovernedRegions
        organizationStructure:
          security:
            name:
              Ref: SecurityOuName
          sandbox:
            name:
              Ref: SandboxOuName
        centralizedLogging:
          accountId:
            Ref: CentralizedLoggingAccountId
          configurations:
            loggingBucket:
              retentionDays:
                Ref: LoggingBucketRetentionPeriod
            accessLoggingBucket:
              retentionDays:
                Ref: AccessLoggingBucketRetentionPeriod
            kmsKeyArn:
              Ref: KMSKey
          enabled: true
        securityRoles:
          accountId:
            Ref: SecurityAccountId
        accessManagement:
          enabled: true
```

Gérez une zone d'atterrissage existante à l'aide de AWS CloudFormation

Vous pouvez l'utiliser AWS CloudFormation pour gérer une zone d'atterrissage que vous avez déjà lancée en l'important dans une AWS CloudFormation pile nouvelle ou existante. Consultez la section Intégrer les ressources existantes à CloudFormation la gestion pour obtenir des détails et des instructions.

Pour détecter et résoudre les problèmes de dérive dans une zone d'atterrissage, vous pouvez utiliser la console AWS Control Tower AWS CLI, le ou l'`ResetLandingZone`API.

Étapes suivantes

Maintenant que votre zone d'atterrissage est configurée, elle est prête à être utilisée.

Pour en savoir plus sur l'utilisation d'AWS Control Tower, consultez les rubriques suivantes :

- Pour connaître les pratiques administratives recommandées, veuillez consulter Best Practices (Bonnes pratiques).
- Vous pouvez configurer des utilisateurs et des groupes IAM Identity Center avec des rôles et des autorisations spécifiques. Pour des recommandations, consultez Recommandations pour configurer des groupes, des rôles et des politiques .
- Pour commencer à inscrire des organisations et des comptes issus de vos AWS Organizations déploiements, consultez Gouverner les organisations et les comptes existants.
- Vos utilisateurs finaux peuvent créer leurs propres AWS comptes dans votre zone de landing zone à l'aide de Account Factory. Pour de plus amples informations, veuillez consulter Autorisations pour configurer et approvisionner des comptes.
- À titre de garantieValidation de conformité pour AWS Control Tower, vos administrateurs cloud centraux peuvent consulter les archives des journaux dans le compte Log Archive, et les auditeurs tiers désignés peuvent consulter les informations d'audit dans le compte d'audit (partagé), qui est membre de l'unité d'organisation de sécurité.
- Pour en savoir plus sur les fonctionnalités d'AWS Control Tower, consultez la section Informations connexes.
- Consultez une liste de YouTube vidéos qui expliquent en détail comment utiliser les fonctionnalités d'AWS Control Tower.
- De temps en temps, vous devrez peut-être mettre à jour votre zone d'atterrissage pour obtenir les dernières mises à jour du backend, les dernières commandes et pour conserver votre zone up-to-date d'atterrissage. Pour de plus amples informations, veuillez consulter Gestion des mises à jour de configuration dans AWS Control Tower.
- Si vous rencontrez des problèmes lors de l'utilisation d'AWS Control Tower, consultezRésolution des problèmes.

Important

Si vous n'avez pas encore activé le MFA pour l'utilisateur root de votre compte, faites-le maintenant. Pour plus d'informations sur les meilleures pratiques pour l'utilisateur root, consultez la section Meilleures pratiques pour protéger l'utilisateur root de votre compte.

Limitations et quotas dans AWS Control Tower

Ce chapitre décrit les limites AWS de service et les quotas que vous devez garder à l'esprit lorsque vous utilisez AWS Control Tower. Si vous ne parvenez pas à configurer votre zone d'atterrissage en raison d'un problème de quota de service, contactez AWS Support.

Pour plus d'informations sur les limitations spécifiques aux contrôles, consultezLimites de contrôle.

> Un nouveau guide de référence sur les commandes
>
> Les informations relatives aux contrôles d'AWS Control Tower ont été transférées vers le guide de référence d'AWS Control Tower Controls.

Limitations d'AWS Control Tower

Cette section décrit les limitations connues et les cas d'utilisation non pris en charge dans AWS Control Tower.

- AWS Control Tower présente des limites générales de simultanéité. En général, une opération à la fois est autorisée. Deux exceptions à cette limitation sont autorisées :
  - Les commandes facultatives peuvent être activées et désactivées simultanément, par le biais d'un processus asynchrone. Jusqu'à cent (100) opérations liées au contrôle peuvent être en cours à la fois, au total, qu'elles soient appelées depuis la console ou depuis une API. Sur ces 100 opérations, jusqu'à 20 à la fois peuvent être des opérations de contrôle proactives.
  - Les comptes peuvent être approvisionnés, mis à jour et inscrits simultanément dans Account Factory, par le biais d'un processus asynchrone, avec jusqu'à cinq (5) opérations liées aux comptes en cours simultanément. La dégestion des comptes doit être effectuée un compte à la fois.
- Les adresses e-mail des comptes partagés dans l'unité d'organisation de sécurité peuvent être modifiées, mais vous devez mettre à jour votre zone de landing zone pour voir ces modifications dans la console AWS Control Tower.
- Une limite de cinq (5) SCP par unité d'organisation s'applique aux unités d'organisation situées dans votre zone d'atterrissage AWS Control Tower.
- AWS Control Tower prend en charge jusqu'à 10 000 comptes dans l'organisation de votre zone d'atterrissage, répartis entre toutes vos unités d'organisation.

- Les UO existantes comportant plus de 300 comptes directement imbriqués ne peuvent pas être enregistrées ou réenregistrées dans AWS Control Tower. Pour plus d'informations sur les limites liées à l'enregistrement des unités d'organisation, consultezLimites relatives aux régions et aux ensembles de piles.
- Les personnalisations pour AWS Control Tower (CfCT) ne sont pas disponibles dans ces zones Régions AWS, car certaines dépendances ne sont pas disponibles :
  - Asie-Pacifique (Jakarta et Osaka)
  - Israël (Tel Aviv)
  - Moyen-Orient (EAU)
  - Europe (Espagne)
  - Asie-Pacifique (Hyderabad)
  - Europe (Zurich)
  - Canada Ouest (Calgary)

  Vous pouvez déployer et gérer des ressources dans ces régions avec CfCT, si vous déployez CfCT dans votre région d'origine AWS Control Tower, mais que vous ne pouvez pas créer CfCT dans ces régions.
- AWS Control Tower Account Factory for Terraform (AFT) n'est pas disponible dans les versions suivantes Régions AWS, car certaines dépendances ne le sont pas :
  - Israël (Tel Aviv)
  - Moyen-Orient (EAU)
  - Europe (Espagne)
  - Asie-Pacifique (Hyderabad)
  - Europe (Zurich)
  - Canada Ouest (Calgary)
- Les régions suivantes ne prennent pas en charge le centre d'identité IAM.
  - Région du Moyen-Orient (EAU), me-central-1
  - Région Asie-Pacifique (Hyderabad), ap-south-2
  - Canada-Ouest (Calgary), ca-west-1

  Pour plus d'informations Régions AWS et d'assistance concernant IAM Identity Center, consultez la section Régions et points de terminaison dans le guide de l'utilisateur AWS d'Identity and Access Management.

- Les régions suivantes ne sont pas prises en charge AWS Service Catalog.
  - Canada-Ouest (Calgary), ca-west-1

  Pour plus d'informations sur les fonctionnalités d'AWS Control Tower dans les régions non prises en charge AWS Service Catalog, consultezAWS Control Tower est disponible dans l'ouest AWS du Canada (Calgary).
- Lorsque vous appelez une API de contrôle pour activer ou désactiver un contrôle, la limite pour les `DisableControl` mises à jour `EnableControl` et les mises à jour dans AWS Control Tower est de cent (100) opérations simultanées. Dix opérations (10) peuvent être en cours simultanément, les opérations restantes étant mises en file d'attente. Vous devrez peut-être ajuster votre code pour attendre qu'il soit terminé.
- Dans la limite globale de 100 opérations de contrôle, jusqu'à 20 opérations à la fois peuvent être des opérations de contrôle proactives.
- Lorsque vous approvisionnez des comptes via Account Factory Customizations (AFC), avec des plans basés sur Terraform, vous ne pouvez déployer ces plans que sur un seul. Région AWS Par défaut, AWS Control Tower se déploie dans la région d'origine.

Demander une augmentation de quota

La console Service Quotas fournit des informations sur les quotas d'AWS Control Tower. Vous pouvez utiliser la console Service Quotas pour consulter les quotas de service par défaut ou pour demander des augmentations de quotas pour des quotas ajustables.

Les quotas suivants peuvent être consultés via la console Service Quotas

- Quota d'opérations de compte simultanées : nombre maximal d'opérations de compte simultanées pouvant être effectuées simultanément. Par défaut : 5, maximum : 10, réglable
- Nombre de comptes dans une seule unité d'organisation : nombre maximum de comptes gérés par AWS Control Tower qui peuvent être présents dans une unité d'organisation. Si vous ajoutez des comptes au-delà de cette limite, le processus d'enregistrement de l'unité d'organisation dans AWS Control Tower ne peut pas être effectué. Pour en savoir plus sur le nombre de comptes par unité d'organisation, consultez Limites relatives aux régions et aux ensembles de piles la documentation d'AWS Control Tower. Par défaut : 300, non réglable.
- Opérations simultanées pour les unités organisationnelles (UO) : nombre maximal d'opérations simultanées liées aux unités organisationnelles qui peuvent être effectuées simultanément. Par défaut : 1, non ajustable.

Par exemple, vous pouvez demander une augmentation du quota de cinq opérations simultanées sur un compte sur un maximum de dix. Certaines caractéristiques de performance d'AWS Control Tower peuvent changer après une augmentation du quota. Par exemple, la mise à jour d'une unité d'organisation peut prendre plus de temps lorsqu'elle contient plusieurs comptes. Ou bien, l'exécution d'une action sur une UO avec cinq SCP peut prendre plus de temps qu'avec trois SCP.

> **Note**
>
> Une demande d'augmentation de quota de service peut prendre jusqu'à deux jours avant qu'elle ne prenne effet. N'oubliez pas de demander l'augmentation du quota auprès de votre région d'origine AWS Control Tower.

Vous pouvez également contacter le AWS Support pour demander une augmentation du quota pour certaines ressources dans AWS Control Tower. Vous pouvez également visionner la vidéo qui suit et découvrir comment automatiser certaines augmentations de quotas de service.

Vidéo : Automatisez les demandes d'augmentation des quotas de service, dans les services liés à AWS Control Tower

Cette vidéo (7:24) explique comment automatiser l'augmentation des quotas de service pour les AWS services intégrés connexes, sur la base des déploiements dans AWS Control Tower. Il explique également comment automatiser l'inscription de nouveaux comptes au support AWS Enterprise de votre organisation. Pour un visionnage de meilleure qualité, sélectionnez l'icône dans le coin inférieur droit de la vidéo pour l'afficher en plein écran. Le sous-titrage est disponible.

Présentation vidéo de l'augmentation des quotas dans AWS Control Tower.

Lorsque vous provisionnez de nouveaux comptes dans cet environnement, vous pouvez utiliser les événements du cycle de vie pour déclencher des demandes automatisées d'augmentation des quotas de service dans les limites spécifiées Régions AWS.

De plus amples informations sur AWS les quotas sont disponibles dans la référence AWS générale.

Limites de contrôle

> **Un nouveau guide de référence sur les commandes**
>
> Les informations relatives aux contrôles d'AWS Control Tower ont été transférées vers le guide de référence d'AWS Control Tower Controls.

Si vous modifiez les ressources d'AWS Control Tower, telles qu'un SCP, ou si vous supprimez une AWS Config ressource, telle qu'un enregistreur ou un agrégateur Config, AWS Control Tower ne peut plus garantir que les contrôles fonctionnent comme prévu. Par conséquent, la sécurité de votre environnement multi-comptes peut être compromise. Le modèle de sécurité à responsabilité AWS partagée s'applique à toutes les modifications que vous pourriez apporter.

> **Note**
>
> AWS Control Tower contribue à préserver l'intégrité de votre environnement en rétablissant la configuration standard des SCP des commandes lorsque vous mettez à jour votre zone de landing zone. Les modifications que vous avez éventuellement apportées aux SCP sont remplacées par la version standard du contrôle, dès sa conception.

Certains contrôles d'AWS Control Tower ne fonctionnent pas dans certains Régions AWS endroits où AWS Control Tower est disponible, car ces régions ne prennent pas en charge les fonctionnalités sous-jacentes requises. Cette limitation concerne certains contrôles de détection, certains contrôles proactifs et certains contrôles de la norme gérée par le Security Hub Service : AWS Control Tower. Pour plus d'informations sur la disponibilité régionale, consultez la documentation de la liste des services régionaux et la documentation de référence des contrôles Security Hub.

Le comportement de contrôle est également limité en cas de gouvernance mixte. Pour plus d'informations, consultez Évitez la gouvernance mixte lors de la configuration des régions.

Pour plus d'informations sur la façon dont AWS Control Tower gère les limites des régions et des contrôles, consultezConsidérations relatives à l'activation des AWS régions optionnelles.

Vous pouvez consulter les régions de chaque contrôle dans la console AWS Control Tower.

Les AWS régions suivantes ne prennent pas en charge les contrôles relevant de la norme gérée par le Security Hub Service : AWS Control Tower.

- Région Asie-Pacifique (Hong Kong), ap-east-1
- Région Asie-Pacifique (Jakarta), ap-southeast-3
- Région Asie-Pacifique (Osaka), ap-northeast-3
- Région Europe (Milan), eu-south-1
- Région Afrique (Cape Town), af-south-1
- Région du Moyen-Orient (Bahreïn), me-south-1
- Israël (Tel Aviv), il-central-1
- Région du Moyen-Orient (EAU), me-central-1
- Région Europe (Espagne), eu-south-2
- Région Asie-Pacifique (Hyderabad), ap-south-2
- Région Europe (Zurich), eu-central-2
- Région Asie-Pacifique (Melbourne), ap-southeast-4
- Canada-Ouest (Calgary), ca-west-1

Les éléments suivants Régions AWS ne prennent pas en charge les contrôles proactifs.

- Canada Ouest (Calgary)

Le tableau suivant indique les contrôles proactifs qui ne sont pas pris en charge dans certains cas Régions AWS.

Identifiant de contrôle	Régions non prises en charge
`CT.REDSHIFT.PR.5`	ap-southeast-4, ap-southeast-2, ap-southeast-3, eu-central-2, eu-south-2, il-central-1, me-central-1
`CT.DAX.PR.2`	us-west-1
`CT.GLUE.PR.2`	Non pris en charge

Le tableau suivant indique les contrôles de détection d'AWS Control Tower qui ne sont pas pris en charge dans certains cas Régions AWS.

Identifiant de contrôle	Régions non prises en charge
AWS-GR_AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED	ap-northeast-3, ap-southeast-3, il-central-1, ap-southeast-4, ca-west-1
AWS-GR_LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED	eu-south-2
AWS-GR_EMR_MASTER_NO_PUBLIC_IP	ap-northeast-3, ap-southeast-3, af-south-1, eu-south-1, eu-south-1, il-central-1, il-central-1, me-central-1, eu-sud-2, ap-sud-2, eu-central-2, ap-southeast-2 ap-southeast-4, ca-west-1
AWS-GR_EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK	eu-south-2
AWS-GR_NO_UNRESTRICTED_ROUTE_TO_IGW	ap-northeast-3, ap-southeast-3, ap-southeast-2, eu-south-2, ca-west-1
AWS-GR_SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS	ap-northeast-3, ap-southeast-3, af-south-1, eu-south-1, eu-south-1, il-central-1, il-central-1, me-central-1, eu-sud-2, ap-sud-2, eu-central-2, ap-southeast-2 ap-southeast-4, ca-west-1
AWS-GR_EC2_INSTANCE_NO_PUBLIC_IP	ap-northeast-3
AWS-GR_EKS_ENDPOINT_NO_PUBLIC_ACCESS	ap-northeast-3, ap-southeast-3, af-south-1, eu-south-1, eu-south-1, us-west-1, il-central-1, eu-central-1, eu-sud-2, eu-central-2, eu-central-2, eu-central-2 al-2, ap-southeast-4, ca-west-1
AWS-GR_ELASTICSEARCH_IN_VPC_ONLY	ap-southeast-3, il-central-1, eu-sud-2, ap-southeast-2, eu-central-2, ap-southeast-2, ap-southeast-4, ca-west-1

Identifiant de contrôle	Régions non prises en charge
AWS-GR_RESTRICTED_SSH	af-south-1, ap-northeast-3, ap-southeast-2, ap-southeast-3, ap-southeast-4, eu-central-2, eu-sud-1, eu-sud-2, il-central-1, me-central-1
AWS-GR_DMS_REPLICATION_NOT_PUBLIC	af-south-1, ap-south-2, ap-southeast-3, ap-southeast-4, eu-central-2, eu-sud-1, eu-sud-2, eu-sud-2, il-central-1, ca-ouest-1 a-west-1
AWS-GR_RDS_SNAPSHOTS_PUBLIC_PROHIBITED	af-south-1, ap-southeast-4, eu-central-2, eu-south-1, eu-south-2, il-central-1
AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED	ap-northeast-3
AWS-GR_ENCRYPTED_VOLUMES	af-south-1, ap-northeast-3, eu-south-1, il-central-1
AWS-GR_RESTRICTED_COMMON_PORTS	af-south-1, ap-northeast-3, eu-central-2, eu-sud-1, eu-south-2, il-central-1, me-central-1
AWS-GR_IAM_USER_MFA_ENABLED	il-central-1, me-central-1, eu-sud-2, ap-sud-2, eu-central-2, ap-southeast-4, ca-west-1
AWS-GR_MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS	il-central-1, me-central-1, eu-sud-2, ap-sud-2, eu-central-2, ap-southeast-4, ca-west-1
AWS-GR_SSM_DOCUMENT_NOT_PUBLIC	il-central-1, ca-west-1
AWS-GR_ROOT_ACCOUNT_MFA_ENABLED	il-central-1, me-central-1, ca-west-1
AWS-GR_S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC	il-central-1, eu-sud-2, eu-central-2
AWS-GR_RDS_STORAGE_ENCRYPTED	eu-central-2, eu-south-2
AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK	ap-south-2, eu-south-2

Identifiant de contrôle	Régions non prises en charge
AWS-GR_REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK	ap-south-2, ap-southeast-3, eu-sud-2, ca-west-1
AWS-GR_EC2_VOLUME_INUSE_CHECK	ca-west-1
AWS-GR_EBS_OPTIMIZED_INSTANCE	ca-west-1

Limites relatives aux régions et aux ensembles de piles

Si vous envisagez d'étendre la gouvernance à des unités d'organisation comportant un grand nombre de comptes répartis sur un grand nombre de comptes Régions AWS, vous risquez de vous heurter à des limites imposées par des ensembles de AWS CloudFormation piles quant à la taille globale d'une organisation. Vous pouvez estimer la limite à l'aide de cette formule :

Nombre de comptes gérés dans l'organisation x Nombre de régions gouvernées <= 150 000

En règle générale, nous nous attendons à ce que le nombre de comptes pris en charge lors de l'extension de la gouvernance à une unité d'organisation diminue en fonction du nombre de régions gouvernées.

Cette limitation apparaît si plus de 15 régions dans lesquelles AWS Control Tower est disponible sont activées lorsque vous étendez la gouvernance à une unité d'organisation. La limite supérieure du nombre de comptes par unité organisationnelle (UO) est réduite.

Par exemple, si 22 régions sont activées, la limite est de 220 comptes par unité d'organisation, au lieu de 300. Si vous souhaitez étendre la gouvernance aux unités d'organisation comptant plus de 220 comptes, vous devez réduire le nombre de régions activées. Cette réduction est due aux limites du stack set.

Directives :

- Avec 15 régions activées, les unités d'organisation comprenant jusqu'à 300 comptes sont prises en charge
- Avec 22 régions activées, les unités d'organisation comprenant jusqu'à 220 comptes sont prises en charge
- Avec 16 à 21 régions activées, la taille maximale de l'unité d'organisation prise en charge se situe entre 220 et 300 comptes

- Avec plus de 23 régions activées, la taille maximale de l'unité d'organisation prise en charge est inférieure à 220 comptes

Différences régionales en ce qui concerne les fonctionnalités d'AWS Control Tower

Certaines différences existent dans le comportement d'AWS Control Tower d'un bout à l'autre Régions AWS, car AWS Control Tower orchestre le comportement des autres AWS services. Par exemple :

- AWS Service Catalog n'est pas disponible partout Régions AWS où AWS Control Tower est disponible, ce qui modifie le comportement d'Account Factory dans ces régions.
- Dans certaines régions, Account Factory Customizations (AFC) n'est pas disponible car Service Catalog n'est pas disponible pour prendre en charge les fonctionnalités sous-jacentes des plans.
- Certaines commandes ne sont pas disponibles du tout en Régions AWS raison de l'absence de fonctionnalités sous-jacentes.
- AFT et CfCT ne sont pas disponibles du tout en Régions AWS raison de l'absence de fonctionnalités sous-jacentes.

Pour déterminer au mieux le comportement de votre environnement AWS Control Tower, déterminez votre région d'origine. Ensuite, évaluez les éléments suivants. Pour plus de détails, consultez la section Limitations et quotas dans AWS Control Tower.

- Est-il AWS Service Catalog disponible dans la région d'origine de votre choix ?
- Les commandes dont vous avez besoin sont-elles disponibles ? Voir Limites de contrôle.
- Le centre d'identité IAM est-il disponible dans la région d'origine de votre choix ?

Nouveau : Guide de référence d'AWS Control Tower Controls

Les informations relatives aux contrôles dans AWS Control Tower ont été transférées dans un nouveau guide, le guide de référence sur les contrôles d'AWS Control Tower.

Bonnes pratiques pour les administrateurs d'AWS Control Tower

Cette rubrique s'adresse principalement aux administrateurs de comptes de gestion.

Les administrateurs des comptes de gestion sont chargés d'expliquer certaines tâches que les contrôles d'AWS Control Tower empêchent les administrateurs de leurs comptes membres d'effectuer. Cette rubrique décrit certaines des meilleures pratiques et procédures pour transférer ces connaissances, et fournit d'autres conseils pour configurer et gérer efficacement votre environnement AWS Control Tower.

Expliquer l'accès aux utilisateurs

La console AWS Control Tower n'est disponible que pour les utilisateurs disposant des autorisations d'administrateur du compte de gestion. Seuls ces utilisateurs peuvent effectuer des tâches administratives dans votre zone de landing zone. Conformément aux meilleures pratiques, cela signifie que la majorité de vos utilisateurs et administrateurs de comptes membres ne verront jamais la console AWS Control Tower. En tant que membre du groupe des administrateurs de comptes de gestion, il est de votre responsabilité d'expliquer les informations suivantes aux utilisateurs et aux administrateurs de vos comptes membres, le cas échéant.

- Expliquez à quelles AWS ressources les utilisateurs et les administrateurs ont accès dans la zone de landing zone.
- Répertoriez les contrôles préventifs qui s'appliquent à chaque unité organisationnelle (UO) afin que les autres administrateurs puissent planifier et exécuter leurs AWS charges de travail en conséquence.

Expliquer l'accès aux ressources

Certains administrateurs et autres utilisateurs peuvent avoir besoin d'une explication des AWS ressources auxquelles ils ont accès dans votre zone de landing zone. Cet accès peut inclure un accès par programmation et un accès basé sur la console. D'une manière générale, l'accès en lecture et en écriture pour les AWS ressources est autorisé. Pour travailler dans ce cadre AWS, vos utilisateurs ont besoin d'un certain niveau d'accès aux services spécifiques dont ils ont besoin pour effectuer leur travail.

Certains utilisateurs, tels que vos AWS développeurs, peuvent avoir besoin de connaître les ressources auxquelles ils ont accès afin de pouvoir créer des solutions d'ingénierie. Les autres utilisateurs, tels que les utilisateurs finaux des applications exécutées sur les AWS services, n'ont pas besoin de connaître les AWS ressources de votre zone de landing zone.

AWS propose des outils permettant d'identifier l'étendue de l'accès aux AWS ressources d'un utilisateur. Une fois que vous avez identifié l'étendue de l'accès d'un utilisateur, vous pouvez partager ces informations avec l'utilisateur, conformément aux stratégies de gestion des informations de votre organisation. Pour de plus amples informations sur ces outils, veuillez consulter les rubriques suivantes.

- AWS conseiller d'accès : l'outil de conseiller d'accès AWS Identity and Access Management (IAM) vous permet de déterminer les autorisations dont disposent vos développeurs en analysant le dernier horodatage auquel une entité IAM, telle qu'un utilisateur, un rôle ou un groupe, a appelé un service. AWS Vous pouvez auditer l'accès au service et supprimer les autorisations inutiles, et vous pouvez automatiser le processus si nécessaire. Pour plus d'informations, consultez notre article AWS de blog sur la sécurité.
- Simulateur de politique IAM : avec le simulateur de politique IAM, vous pouvez tester et résoudre les problèmes liés aux politiques basées sur l'IAM et les ressources. Pour plus d'informations, voir Tester les politiques IAM avec le simulateur de politiques IAM.
- AWS CloudTrail journaux — Vous pouvez consulter AWS CloudTrail les journaux pour voir les actions entreprises par un utilisateur, un rôle ou Service AWS. Pour plus d'informations CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

  Les actions entreprises par les administrateurs de la zone d'atterrissage d'AWS Control Tower sont consultables dans le compte de gestion de la zone d'atterrissage. Les actions entreprises par les administrateurs des comptes membres et les utilisateurs sont consultables dans le compte d'archivage de journaux partagé.

  Vous pouvez consulter un tableau récapitulatif des événements de l'AWS Control Tower sur la page Activités.

Expliquer les contrôles préventifs

Un contrôle préventif garantit que les comptes de votre organisation sont conformes aux politiques de votre entreprise. Le statut d'un contrôle préventif est soit appliqué, soit non activé. Un contrôle préventif prévient les violations des politiques en utilisant des politiques de contrôle des services

(SCP). En comparaison, un contrôle de détection vous informe des différents événements ou états existants, au moyen de AWS Config règles définies.

Certains de vos utilisateurs, tels que AWS les développeurs, peuvent avoir besoin de connaître les contrôles préventifs qui s'appliquent à tous les comptes et unités d'organisation qu'ils utilisent, afin de pouvoir créer des solutions d'ingénierie. La procédure suivante comporte des conseils sur la façon de fournir ces informations aux utilisateurs concernés, conformément aux politiques de gestion des informations de votre organisation.

> **Note**
>
> Cette procédure suppose que vous avez déjà créé au moins une UO enfant dans votre zone de landing zone, ainsi qu'au moins un AWS IAM Identity Center utilisateur.

Pour montrer les contrôles préventifs aux utilisateurs ayant besoin de connaître

1. Connectez-vous à la console AWS Control Tower à l'adresse https://console.aws.amazon.com/controltower/.
2. Dans le menu de navigation de gauche, sélectionnez Organisation.
3. Dans le tableau, choisissez le nom de l'une des unités d'organisation pour lesquelles votre utilisateur a besoin d'informations sur les contrôles applicables.
4. Notez le nom de l'unité d'organisation et les commandes qui s'appliquent à cette unité d'organisation.
5. Répétez les deux étapes précédentes pour chaque unité d'organisation pour laquelle votre utilisateur a besoin d'informations.

Pour obtenir des informations détaillées sur les contrôles et leurs fonctions, consultez À propos des contrôles dans AWS Control Tower.

Planifiez la zone de landing de votre AWS Control Tower

Au cours du processus de configuration, AWS Control Tower lance une ressource clé associée à votre compte, appelée zone de destination, qui héberge vos organisations et leurs comptes.

> **Note**
>
> Vous pouvez avoir une zone de destination par organisation.

Pour plus d'informations sur les meilleures pratiques à suivre lors de la planification et de la configuration de votre zone d'atterrissage, consultezAWS stratégie multi-comptes pour votre zone de landing zone AWS Control Tower.

Comment configurer AWS Control Tower

Vous pouvez configurer une zone d'atterrissage AWS Control Tower dans une organisation existante, ou vous pouvez commencer par créer une nouvelle organisation contenant votre zone d'atterrissage AWS Control Tower.

- Lancer AWS Control Tower dans une organisation existante: Cette section est destinée aux clients qui ont un produit existant AWS Organizations prêt à être intégré à la gouvernance par AWS Control Tower.
- Lancer AWS Control Tower dans une nouvelle organisation: Cette section est destinée aux clients qui n'ont pas d' AWS Organizationsunité d'organisation ou de compte existants.

> **Note**
>
> Si vous disposez déjà d'une zone d' AWS Organizations atterrissage, vous pouvez étendre la gouvernance d'AWS Control Tower depuis la zone d'atterrissage existante à tout ou partie de vos unités d'organisation et comptes existants au sein d'une organisation. Voir Gouverner les organisations et les comptes existants.

Comparez les fonctionnalités

Voici une brève comparaison des différences entre l'ajout d'AWS Control Tower à une organisation existante ou l'extension de la gouvernance d'AWS Control Tower aux unités d'organisation et aux comptes. Certaines considérations particulières s'appliquent également si vous passez de la solution AWS Landing Zone à AWS Control Tower.

À propos de l'ajout à une organisation existante : vous pouvez ajouter AWS Control Tower à une organisation existante dans la AWS console. Dans ce cas, vous avez déjà créé une organisation

dans le AWS Organizations service, cette organisation n'est pas actuellement enregistrée auprès d'AWS Control Tower et vous souhaitez ajouter une zone de landing zone par la suite.

Lorsque vous ajoutez une zone de landing zone à une organisation existante, AWS Control Tower met en place une structure parallèle, au AWS Organizations niveau. Cela ne modifie pas les unités d'organisation et les comptes au sein de votre organisation existante.

À propos de l'extension de la gouvernance : l'extension de la gouvernance s'applique à des unités d'organisation et à des comptes spécifiques au sein d'une même organisation déjà enregistrée auprès d'AWS Control Tower, ce qui signifie qu'une zone de landing zone existe déjà pour cette organisation. L'extension de la gouvernance signifie que les contrôles d'AWS Control Tower sont étendus afin que leurs contraintes s'appliquent aux unités d'organisation et aux comptes spécifiques au sein de cette organisation enregistrée. Dans ce cas, vous ne lancez pas une nouvelle zone d'atterrissage, vous ne faites qu'étendre la zone d'atterrissage actuelle de votre organisation.

> **Important**
>
> Remarque particulière : si vous utilisez actuellement la solutionAWS Landing Zone (ALZ) pour AWS Organizations, contactez votre architecte de AWS solutions avant d'essayer d'activer AWS Control Tower dans votre organisation. AWS Control Tower ne peut pas effectuer de vérifications préalables visant à déterminer si AWS Control Tower est susceptible d'interférer avec le déploiement actuel de votre zone de landing zone. Pour de plus amples informations, veuillez consulter Procédure pas à pas : passer d'ALZ à AWS Control Tower. En outre, pour plus d'informations sur le transfert de comptes d'une zone d'atterrissage à une autre, voir Et si le compte ne répond pas aux prérequis ?

Lancer AWS Control Tower dans une organisation existante

En configurant une zone de landing zone AWS Control Tower dans une organisation existante, vous pouvez commencer à travailler immédiatement, en parallèle avec votre AWS Organizations environnement existant. Vos autres UO créées dans ce cadre AWS Organizations restent inchangées, car elles ne sont pas enregistrées auprès d'AWS Control Tower. Vous pouvez continuer à utiliser ces UO et ces comptes exactement tels qu'ils sont.

AWS Control Tower consolide ses activités en utilisant le compte de gestion de votre organisation existante comme compte de gestion. Aucun nouveau compte de gestion n'est nécessaire. Vous pouvez lancer votre zone de landing zone AWS Control Tower depuis votre compte de gestion existant.

> **Note**
>
> Pour configurer AWS Control Tower sur une organisation existante, vos limites de service doivent autoriser la création d'au moins deux comptes supplémentaires.

Effets de l'ajout d'AWS Control Tower à votre organisation existante

AWS Control Tower crée deux comptes dans votre organisation : un compte d'audit et un compte de journalisation. Ces comptes enregistrent les actions entreprises par votre équipe, dans leurs comptes d'utilisateur final individuels. Les comptes d'archive Audit et Log apparaissent dans l'unité d'organisation de sécurité au sein de votre zone de landing zone AWS Control Tower.

Lorsque vous configurez votre zone de landing zone, les comptes ajoutés par AWS Control Tower font partie de votre compte existant et AWS Organizations, en tant que tels, ils font partie de la facturation de votre organisation existante.

Résumé des fonctionnalités

L'activation d'AWS Control Tower sur une AWS Organizations organisation existante apporte plusieurs améliorations majeures à l'organisation.

- Cela permet une facturation unifiée entre les groupes de votre organisation, car les comptes ajoutés par AWS Control Tower feront partie de votre organisation existante.
- Il vous permet d'administrer tous les comptes à partir d'un seul compte de gestion dans votre unité d'organisation.
- Il simplifie la façon dont vous appliquez et appliquez les contrôles relatifs à la sécurité et à la conformité des comptes existants et nouveaux.

> **Important**
>
> Le lancement de votre zone de landing zone AWS Control Tower dans une AWS Organizations organisation existante ne vous permet pas d'étendre la gouvernance d'AWS Control Tower de cette organisation à d'autres unités d'organisation ou à d'autres comptes qui ne sont pas enregistrés auprès d'AWS Control Tower.

Pour lancer AWS Control Tower dans votre organisation existante, suivez le processus décrit dansCommencer à utiliser AWS Control Tower.

Pour plus d'informations sur la manière dont AWS Control Tower interagit avec les AWS Organizations organisations existantes, consultezGérez les organisations et les comptes avec AWS Control Tower.

Lancer AWS Control Tower dans une nouvelle organisation

Si vous utilisez AWS Control Tower pour la première fois et que vous n'y avez jamais travaillé AWS Organizations, le meilleur point de départ est de consulter notre Configuration document.

AWS Control Tower configure automatiquement une organisation pour vous lorsque vous n'en avez pas configuré une.

AWS stratégie multi-comptes pour votre zone de landing zone AWS Control Tower

Les clients d'AWS Control Tower demandent souvent des conseils sur la manière de configurer leur AWS environnement et leurs comptes pour obtenir les meilleurs résultats.AWS a créé un ensemble unifié de recommandations, appelé stratégie multi-comptes, pour vous aider à utiliser au mieux vos AWS ressources, y compris votre zone de landing zone AWS Control Tower.

AWS Control Tower agit essentiellement comme une couche d'orchestration qui fonctionne avec d'autres AWS services, qui vous aident à mettre en œuvre les recommandations AWS multi-comptes pour les AWS comptes et. AWS OrganizationsUne fois votre zone de landing zone configurée, AWS Control Tower continue de vous aider à maintenir vos politiques d'entreprise et vos pratiques de sécurité sur plusieurs comptes et charges de travail.

La plupart des zones d'atterrissage se développent au fil du temps. À mesure que le nombre d'unités organisationnelles (UO) et de comptes augmente dans votre zone de landing zone AWS Control Tower, vous pouvez étendre le déploiement de votre AWS Control Tower de manière à organiser efficacement vos charges de travail. Ce chapitre fournit des conseils prescriptifs sur la façon de planifier et de configurer votre zone d'atterrissage AWS Control Tower, conformément à la stratégie AWS multi-comptes, et de l'étendre au fil du temps.

Pour une discussion générale sur les meilleures pratiques pour les unités organisationnelles, voir Meilleures pratiques pour les unités organisationnelles dotées de AWS Organizations.

AWS stratégie multi-comptes : guide des meilleures pratiques

AWS les meilleures pratiques pour un environnement bien conçu recommandent de séparer vos ressources et vos charges de travail sur plusieurs comptes. AWS Vous pouvez considérer les AWS comptes comme des conteneurs de ressources isolés : ils permettent de catégoriser la charge de travail et de réduire le rayon d'action en cas de problème.

Définition d'un AWS compte

Un AWS compte fait office de conteneur de ressources et de limite d'isolation des ressources.

> **Note**
>
> Un AWS compte n'est pas la même chose qu'un compte utilisateur, qui est configuré via Federation ou AWS Identity and Access Management (IAM).

En savoir plus sur AWS les comptes

Un AWS compte permet d'isoler les ressources et de contenir les menaces de sécurité pour vos AWS charges de travail. Un compte fournit également un mécanisme de facturation et de gouvernance d'un environnement de charge de travail.

Le AWS compte est le principal mécanisme de mise en œuvre permettant de fournir un conteneur de ressources pour vos charges de travail. Si votre environnement est bien conçu, vous pouvez gérer efficacement plusieurs AWS comptes, et ainsi gérer plusieurs charges de travail et environnements.

AWS Control Tower met en place un environnement bien conçu. Il repose également sur AWS des comptes qui aident à gérer les modifications apportées à votre environnement qui peuvent s'étendre à plusieurs comptes. AWS Organizations

Définition d'un environnement bien conçu

AWS définit un environnement bien conçu comme un environnement qui commence par une zone d'atterrissage.

AWS Control Tower propose une zone d'atterrissage configurée automatiquement. Il applique des contrôles pour garantir le respect des directives de votre entreprise, sur plusieurs comptes de votre environnement.

Définition d'une zone d'atterrissage

La zone de landing zone est un environnement cloud qui propose un point de départ recommandé, notamment les comptes par défaut, la structure des comptes, les configurations réseau et de sécurité, etc. À partir d'une zone d'atterrissage, vous pouvez déployer des charges de travail qui utilisent vos solutions et applications.

Directives pour la mise en place d'un environnement bien conçu

Les trois éléments clés d'un environnement bien conçu, expliqués dans les sections suivantes, sont les suivants :

- AWS Comptes multiples
- Plusieurs unités organisationnelles (UO)
- Une structure bien planifiée

Utiliser plusieurs comptes AWS

Un seul compte ne suffit pas pour configurer un environnement bien conçu. En utilisant plusieurs comptes, vous pouvez mieux soutenir vos objectifs de sécurité et vos processus métier. Voici quelques avantages de l'utilisation d'une approche multi-comptes :

- Contrôles de sécurité — Les applications ont des profils de sécurité différents, elles nécessitent donc des politiques et des mécanismes de contrôle différents. Par exemple, il est beaucoup plus facile de parler à un auditeur et de lui indiquer un seul compte hébergeant la charge de travail du secteur des cartes de paiement (PCI).
- Isolation — Un compte est une unité de protection de sécurité. Les risques potentiels et les menaces de sécurité peuvent être maîtrisés dans un compte sans affecter les autres. Par conséquent, pour des raisons de sécurité, vous devrez peut-être isoler les comptes les uns des autres. Par exemple, vous pouvez avoir des équipes avec des profils de sécurité différents.
- De nombreuses équipes — Les équipes ont des responsabilités et des besoins en ressources différents. En configurant plusieurs comptes, les équipes ne peuvent pas interférer les unes avec les autres, comme c'est le cas lorsqu'elles utilisent le même compte.
- Isolation des données : isoler les banques de données d'un compte permet de limiter le nombre de personnes ayant accès aux données et pouvant gérer la banque de données. Cette isolation permet d'empêcher l'exposition non autorisée de données hautement privées. Par exemple,

l'isolation des données contribue au respect du règlement général sur la protection des données (RGPD).

- Processus métier — Les unités commerciales ou les produits ont souvent des objectifs et des processus complètement différents. Des comptes individuels peuvent être établis pour répondre aux besoins spécifiques de l'entreprise.
- Facturation — Un compte est le seul moyen de séparer les éléments au niveau de la facturation, y compris les frais de transfert, etc. La stratégie multi-comptes permet de créer des articles facturables distincts entre les unités commerciales, les équipes fonctionnelles ou les utilisateurs individuels.
- Allocation de AWS quotas : les quotas sont établis pour chaque compte. La séparation des charges de travail dans différents comptes confère à chaque compte (tel qu'un projet) un quota individuel bien défini.

Utiliser plusieurs unités organisationnelles

AWS Control Tower et d'autres frameworks d'orchestration de comptes peuvent apporter des modifications qui dépassent les limites des comptes. Par conséquent, les AWS meilleures pratiques concernent les modifications entre comptes, qui peuvent potentiellement perturber un environnement ou compromettre sa sécurité. Dans certains cas, les modifications peuvent affecter l'environnement global, au-delà des politiques. Par conséquent, nous vous recommandons de configurer au moins deux comptes obligatoires, Production et Staging.

En outre, les AWS comptes sont souvent regroupés en unités organisationnelles (UO), à des fins de gouvernance et de contrôle. Les unités d'organisation sont conçues pour gérer l'application des politiques sur plusieurs comptes.

Nous vous recommandons de créer au minimum un environnement de pré-production (ou de mise en scène) distinct de votre environnement de production, avec des contrôles et des politiques distincts. Les environnements de production et de préparation peuvent être créés et gérés comme des unités d'organisation distinctes, et facturés sous forme de comptes distincts. En outre, vous souhaiterez peut-être configurer une unité d'organisation Sandbox pour tester le code.

Utilisez une structure bien planifiée pour les UO dans votre zone d'atterrissage

AWS Control Tower configure automatiquement certaines unités d'organisation pour vous. À mesure que vos charges de travail et vos exigences augmentent au fil du temps, vous pouvez étendre la configuration initiale de la zone d'atterrissage en fonction de vos besoins.

> **Note**
>
> Les noms donnés dans les exemples suivent les conventions de AWS dénomination suggérées pour la configuration d'un AWS environnement multi-comptes. Vous pouvez renommer vos UO après avoir configuré votre zone de landing zone, en sélectionnant Modifier sur la page détaillée de l'UO.

Recommandations

Une fois qu'AWS Control Tower a configuré la première unité d'organisation requise pour vous, l'unité d'organisation de sécurité, nous vous recommandons de créer des unités d'organisation supplémentaires dans votre zone de landing zone.

Nous vous recommandons d'autoriser AWS Control Tower à créer au moins une unité d'organisation supplémentaire, appelée unité d'organisation Sandbox. Cette unité d'organisation est destinée à vos environnements de développement logiciel. AWS Control Tower peut configurer l'unité d'organisation Sandbox pour vous lors de la création de la zone de landing zone, si vous la sélectionnez.

Deux autres unités d'organisation recommandées que vous pouvez configurer vous-même : l'unité d'organisation d'infrastructure, pour contenir vos services partagés et vos comptes réseau, et une unité d'organisation pour contenir vos charges de travail de production, appelée unité d'organisation de charges de travail. Vous pouvez ajouter des unités d'organisation supplémentaires dans votre zone de landing via la console AWS Control Tower sur la page Organizational units.

UO recommandées en plus de celles configurées automatiquement

- Infrastructure UO : contient vos services partagés et vos comptes réseau.

  > **Note**
  >
  > AWS Control Tower ne configure pas l'unité d'organisation de l'infrastructure pour vous.

- Sandbox OU : unité d'organisation de développement logiciel. Par exemple, il peut avoir une limite de dépenses fixe ou ne pas être connecté au réseau de production.

> **Note**
>
> AWS Control Tower vous recommande de configurer l'unité d'organisation Sandbox, mais c'est facultatif. Il peut être configuré automatiquement dans le cadre de la configuration de votre zone d'atterrissage.

- UO de charges de travail : contient les comptes qui exécutent vos charges de travail.

> **Note**
>
> AWS Control Tower ne configure pas l'unité d'organisation Workloads pour vous.

Pour plus d'informations, consultez la section Organisation du démarrage de la production avec AWS Control Tower.

Exemple d'AWS Control Tower avec une structure d'unité d'organisation multi-comptes complète

AWS Control Tower prend en charge une hiérarchie d'unités d'organisation imbriquées, ce qui signifie que vous pouvez créer une structure d'unité organisationnelle hiérarchique répondant aux exigences de votre organisation. Vous pouvez créer un environnement AWS Control Tower conforme aux directives de stratégie AWS multi-comptes.

Vous pouvez également créer une structure d'unité d'organisation plus simple et plate, performante et conforme aux directives AWS multi-comptes. Ce n'est pas parce que vous pouvez créer une structure d'unité d'organisation hiérarchique que vous devez le faire.

- Pour consulter un schéma illustrant un ensemble d'unités d'organisation dans un environnement AWS Control Tower étendu et plat, avec des instructions relatives à AWS plusieurs comptes, voir Exemple : charges de travail dans une structure d'unité d'organisation plate.
- Pour plus d'informations sur le fonctionnement d'AWS Control Tower avec des structures d'unité d'organisation imbriquées, consultezUO imbriquées dans AWS Control Tower.
- Pour plus d'informations sur la manière dont AWS Control Tower s'aligne sur les AWS directives, consultez le livre AWS blanc intitulé Organizing Your AWS Environment Using Multiple Accounts.

Le schéma de la page liée montre que davantage d'UO de base et d'UO supplémentaires ont été créées. Ces unités d'organisation répondent aux besoins supplémentaires d'un déploiement de plus grande envergure.

Dans la colonne UO de base, deux unités d'organisation ont été ajoutées à la structure de base :

- Security_Prod OU — Fournit une zone en lecture seule pour les politiques de sécurité, ainsi qu'une zone d'audit de sécurité révolutionnaire.
- UO d'infrastructure — Vous souhaiterez peut-être séparer l'unité d'organisation d'infrastructure, recommandée précédemment, en deux unités d'organisation, Infrastructure_Test (pour l'infrastructure de pré-production) et Infrastructure_Prod (pour l'infrastructure de production).

Dans la zone UO supplémentaires, plusieurs UO supplémentaires ont été ajoutées à la structure de base. Voici les prochaines unités d'organisation recommandées à créer au fur et à mesure que votre environnement se développe :

- UO de charges de travail — L'unité d'organisation de charges de travail, recommandée précédemment mais facultative, a été séparée en deux unités d'organisation, Workloads_Test (pour les charges de travail de pré-production) et Workloads_Prod (pour les charges de travail de production).
- PolicyStaging OU : permet aux administrateurs système de tester les modifications apportées aux contrôles et aux politiques avant de les appliquer pleinement.
- UO suspendue : permet de localiser les comptes qui ont peut-être été temporairement désactivés.

À propos de The Root

La racine n'est pas une UO. Il s'agit d'un conteneur pour le compte de gestion, ainsi que pour tous les UO et comptes de votre organisation. Conceptuellement, la racine contient toutes les unités d'organisation. Il ne peut pas être supprimé. Vous ne pouvez pas gérer les comptes inscrits au niveau root dans AWS Control Tower. Gérez plutôt les comptes inscrits au sein de vos unités d'organisation. Pour un schéma utile, consultez la AWS Organizations documentation.

Conseils administratifs pour la configuration de la zone d'atterrissage

- La AWS région dans laquelle vous travaillez le plus devrait être votre région d'origine.

- Configurez votre zone de landing zone et déployez vos comptes Account Factory depuis votre région d'origine.
- Si vous investissez dans plusieurs AWS régions, assurez-vous que vos ressources cloud se trouvent dans la région où vous effectuerez la plupart de vos tâches administratives dans le cloud et exécuterez vos charges de travail.
- En conservant vos charges de travail et vos journaux dans la même AWS région, vous réduisez les coûts associés au déplacement et à la récupération des informations des journaux d'une région à l'autre.
- L'audit et les autres compartiments Amazon S3 sont créés dans la même AWS région à partir de laquelle vous lancez AWS Control Tower. Nous vous recommandons de ne pas déplacer ces compartiments.
- Vous pouvez créer vos propres compartiments de journal dans le compte Log Archive, mais cela n'est pas recommandé. N'oubliez pas de laisser les compartiments créés par AWS Control Tower.
- Vos journaux d'accès Amazon S3 doivent se trouver dans la même AWS région que les compartiments source.
- Lors du lancement, les points de terminaison du AWS Security Token Service (STS) doivent être activés dans le compte de gestion, pour toutes les régions prises en charge par AWS Control Tower. Sinon, le lancement peut échouer au milieu du processus de configuration.
- AWS Control Tower prend en charge le balisage uniquement pour les contrôles activés. Pour plus d'informations, consultez AWS Control Tower prend en charge le balisage pour les contrôles activés.
- Nous recommandons d'activer l'authentification multifactorielle (MFA) pour chaque compte géré par AWS Control Tower.

Considérations relatives aux VPC

- Le VPC créé par AWS Control Tower est limité au VPC Régions AWS dans lequel AWS Control Tower est disponible. Certains clients dont les charges de travail s'exécutent dans des régions non prises en charge souhaiteront peut-être désactiver le VPC créé avec votre compte Account Factory. Ils peuvent préférer créer un nouveau VPC à l'aide du portefeuille Service Catalog ou créer un VPC personnalisé qui s'exécute uniquement dans les régions requises.
- Le VPC créé par AWS Control Tower n'est pas le même que le VPC par défaut créé pour tous. Comptes AWS Dans les régions où AWS Control Tower est pris en charge, AWS Control Tower supprime le VPC par défaut lors de la création du VPC AWS Control Tower.

- Si vous supprimez votre VPC par défaut dans votre AWS région d'origine, il est préférable de le supprimer dans toutes les autres AWS régions.

Recommandations pour configurer des groupes, des rôles et des politiques

Lorsque vous configurez votre zone de destination, il est conseillé de décider à l'avance quels utilisateurs auront besoin d'accéder à certains comptes et pourquoi. Par exemple, un compte de sécurité ne doit être accessible qu'à l'équipe de sécurité, le compte de gestion doit être accessible uniquement à l'équipe des administrateurs du cloud, etc.

Pour plus d'informations sur ce sujet, consultezGestion des identités et des accès dans AWS Control Tower.

Restrictions recommandées

Vous pouvez restreindre l'étendue de l'accès administratif à vos organisations en configurant un rôle ou une politique IAM qui permet aux administrateurs de gérer uniquement les actions d'AWS Control Tower. L'approche recommandée consiste à utiliser la politique `arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy` IAM. Lorsque le `AWSControlTowerServiceRolePolicy` rôle est activé, un administrateur peut uniquement gérer AWS Control Tower. Assurez-vous d'inclure un accès approprié AWS Organizations pour gérer vos contrôles préventifs et vos SCP, ainsi que l'accès à AWS Config, pour gérer les contrôles de détection, dans chaque compte.

Lorsque vous configurez le compte d'audit partagé dans votre zone de destination, nous vous recommandons d'affecter le groupe `AWSSecurityAuditors` à des auditeurs tiers de vos comptes. Ce groupe donne à ses membres l'autorisation en lecture seule. Un compte ne doit pas disposer d'autorisations d'écriture sur l'environnement qu'il vérifie, car il peut enfreindre la conformité aux exigences de séparation des fonctions pour les auditeurs.

Vous pouvez imposer des conditions dans vos politiques de confiance en matière de rôles, afin de restreindre les comptes et les ressources qui interagissent avec certains rôles dans AWS Control Tower. Nous vous recommandons vivement de restreindre l'accès au `AWSControlTowerAdmin` rôle, car il autorise des autorisations d'accès étendues. Pour plus d'informations, voir Conditions facultatives relatives à vos relations de confiance en matière de rôle.

Conseils pour créer et modifier les ressources AWS Control Tower

Nous vous recommandons de suivre les bonnes pratiques suivantes lors de la création et de la modification de ressources dans AWS Control Tower. Ce guide peut changer lorsque le service est mis à jour. N'oubliez pas que le modèle de responsabilité partagée s'applique à votre environnement AWS Control Tower.

Conseils généraux

- Ne modifiez ni ne supprimez aucune ressource créée par AWS Control Tower, y compris les ressources du compte de gestion, des comptes partagés et des comptes membres. Si vous modifiez ces ressources, il peut vous être demandé de mettre à jour votre zone d'atterrissage ou de réenregistrer une UO, et les modifications peuvent entraîner des rapports de conformité inexacts.

  En particulier :

  - Gardez un AWS Config enregistreur actif. Si vous supprimez votre enregistreur Config, les contrôles de détection ne peuvent ni détecter ni signaler les dérives. Les ressources non conformes peuvent être signalées comme conformes en raison d'informations insuffisantes.
  - Ne modifiez ni ne supprimez les rôles AWS Identity and Access Management (IAM) créés dans les comptes partagés de l'unité organisationnelle (UO) chargée de la sécurité. La modification de ces rôles peut nécessiter une mise à jour de votre zone de destination.
  - Ne supprimez pas le `AWSControlTowerExecution` rôle de vos comptes de membre, même s'il s'agit de comptes non inscrits. Dans ce cas, vous ne pourrez pas inscrire ces comptes auprès d'AWS Control Tower, ni enregistrer leurs unités d'organisation parentes immédiates.
- N'en interdisez pas l'utilisation Régions AWS par le biais de SCP ou AWS Security Token Service ()AWS STS. Cela fera entrer AWS Control Tower dans un état non défini. Si vous n'autorisez pas les régions avec AWS STS, vos fonctionnalités échoueront dans ces régions, car l'authentification ne sera pas disponible dans ces régions. Utilisez plutôt la capacité de refus de la région AWS Control Tower, comme indiqué dans le contrôle, de refuser l'accès en AWS fonction de la demande Région AWS, qui fonctionne au niveau de la zone d'atterrissage, ou du contrôle de refus de la région de contrôle appliqué à l'unité d'organisation, qui fonctionne au niveau de l'unité d'organisation pour restreindre l'accès aux régions.
- Le AWS Organizations `FullAWSAccess` SCP doit être appliqué et ne doit pas être fusionné avec d'autres SCP. La modification de ce SCP n'est pas signalée comme une dérive ; toutefois, certaines modifications peuvent affecter les fonctionnalités d'AWS Control Tower de manière imprévisible, si l'accès à certaines ressources est refusé. Par exemple, si le SCP est détaché ou

modifié, un compte peut perdre l'accès à un AWS Config enregistreur ou créer une lacune dans la CloudTrail journalisation.

- N'utilisez pas l' AWS Organizations `DisableAWSServiceAccess`API pour désactiver l'accès du service AWS Control Tower à l'organisation dans laquelle vous avez configuré votre zone de landing zone. Dans ce cas, certaines fonctionnalités de détection de dérive d'AWS Control Tower risquent de ne pas fonctionner correctement sans l'assistance par message de AWS Organizations. Ces fonctionnalités de détection des dérives permettent à AWS Control Tower de signaler avec précision l'état de conformité des unités organisationnelles, des comptes et des contrôles de votre organisation. Pour plus d'informations, consultez API_DisableAWSServiceAccessla référence de AWS Organizations l'API.
- En général, AWS Control Tower exécute une seule action à la fois, qui doit être terminée avant qu'une autre action puisse commencer. Par exemple, si vous tentez de configurer un compte alors que le processus d'activation d'un contrôle est déjà en cours, le provisionnement du compte échouera.

  Exception :

  - AWS Control Tower autorise des actions simultanées pour déployer des contrôles optionnels. Pour plus d'informations, voir Déploiement simultané pour les contrôles facultatifs.
  - AWS Control Tower permet de créer, de mettre à jour ou d'inscrire jusqu'à dix actions simultanées sur des comptes, avec Account Factory.

> **Note**
>
> Pour plus d'informations sur les ressources créées par AWS Control Tower, consultezQuels sont les comptes partagés ?.

Conseils concernant les comptes et les unités d'organisation

- Nous vous recommandons de limiter chaque unité d'organisation enregistrée à un maximum de 300 comptes, afin de pouvoir mettre à jour ces comptes avec la fonctionnalité de réenregistrement de l'unité d'organisation chaque fois que des mises à jour de compte sont nécessaires, par exemple lorsque vous configurez de nouvelles régions à des fins de gouvernance.
- Pour réduire le temps nécessaire à l'enregistrement d'une unité d'organisation, nous vous recommandons de maintenir le nombre de comptes par unité d'organisation à environ 150, même si la limite est de 300 comptes par unité d'organisation. En règle générale, le temps nécessaire

pour enregistrer une UO augmente en fonction du nombre de régions dans lesquelles votre UO opère, multiplié par le nombre de comptes de l'UO.

- À titre d'estimation, une unité d'organisation avec 150 comptes a besoin d'environ 2 heures pour enregistrer et activer les contrôles, et d'environ 1 heure pour se réenregistrer. En outre, l'enregistrement d'une UO comportant de nombreux contrôles prend plus de temps qu'une UO comportant peu de contrôles.
- L'une des préoccupations liées à l'allongement du délai d'enregistrement d'une unité d'organisation est que ce processus bloque d'autres actions. Certains clients n'hésitent pas à prévoir des délais plus longs pour enregistrer ou réenregistrer une unité d'organisation, car ils préfèrent autoriser un plus grand nombre de comptes dans chaque unité d'organisation.

Quand se connecter en tant qu'utilisateur root

Certaines tâches administratives nécessitent que vous vous connectiez en tant qu'utilisateur racine. Vous pouvez vous connecter en tant qu'utilisateur root à un Compte AWS compte créé par Account Factory dans AWS Control Tower.

Vous devez vous connecter en tant qu'utilisateur racine pour effectuer les actions suivantes :

- Modifiez certains paramètres de compte, notamment le nom du compte, le mot de passe de l'utilisateur racine ou l'adresse e-mail. Pour plus d'informations, consultez Mettez à jour et déplacez les comptes Account Factory avec AWS Control Tower ou avec AWS Service Catalog.
- Pour fermer un Compte AWS.
- Pour plus d'informations sur les actions qui nécessitent des informations de connexion de l'utilisateur root, consultez la section Tâches nécessitant des informations d'identification de l'utilisateur root dans le Guide de AWS Account Management référence.

> **Note**
>
> Pour modifier ou activer votre plan AWS Support, vous devez être connecté en tant qu'utilisateur root ou disposer des autorisations IAM appropriées. .

Pour se connecter en tant qu'utilisateur racine

1. Ouvrez la page AWS de connexion.

Si vous n'avez pas l'adresse e-mail Compte AWS à laquelle vous souhaitez accéder, vous pouvez l'obtenir auprès d'AWS Control Tower. Ouvrez la console du compte de gestion, choisissez Comptes et recherchez l'adresse e-mail.

2. Entrez l'adresse e-mail Compte AWS à laquelle vous souhaitez accéder, puis choisissez Next.
3. Choisissez Forgot password? (Mot de passe oublié ?) pour que les instructions de réinitialisation du mot de passe soient envoyées à l'adresse e-mail de l'utilisateur racine.
4. Ouvrez le message électronique de réinitialisation du mot de passe à partir de la boîte aux lettres de l'utilisateur racine, puis suivez les instructions pour réinitialiser votre mot de passe.
5. Ouvrez la page de AWS connexion, puis connectez-vous avec votre mot de passe de réinitialisation.

AWS Organizations orientation

- Vous trouverez des conseils sur les meilleures pratiques pour protéger la sécurité de votre compte de gestion AWS Control Tower et de vos comptes membres dans la AWS Organizations documentation.
  - Bonnes pratiques pour le compte de gestion
  - Bonnes pratiques pour les comptes des membres
- Ne l'utilisez pas AWS Organizations pour mettre à jour les politiques de contrôle des services (SCP) associées à une unité d'organisation enregistrée auprès d'AWS Control Tower. Cela pourrait entraîner le passage des commandes à un état inconnu, ce qui vous obligera à réinitialiser votre zone d'atterrissage ou à réenregistrer votre unité d'organisation dans AWS Control Tower. Au lieu de cela, vous pouvez créer de nouveaux SCP et les associer aux UO plutôt que de modifier les SCP créés par AWS Control Tower.
- Le transfert de comptes individuels déjà inscrits vers AWS Control Tower, depuis l'extérieur d'une unité d'organisation enregistrée, entraîne une dérive qui doit être corrigée. veuillez consulter Types de dérive de gouvernance.
- Si vous créez, invitez ou déplacez des comptes au sein d'une organisation enregistrée auprès d'AWS Control Tower, ces comptes ne sont pas inscrits par AWS Control Tower et ces modifications ne sont pas enregistrées. AWS Organizations Si vous avez besoin d'accéder à ces comptes via SSO, consultez Accès au compte membre.
- Si vous déplacez une AWS Organizations unité d'organisation dans une organisation créée par AWS Control Tower, l'unité d'organisation externe n'est pas enregistrée par AWS Control Tower.

- AWS Control Tower gère le filtrage des autorisations AWS Organizations différemment. Si vos comptes sont approvisionnés avec AWS Control Tower Account Factory, les utilisateurs finaux peuvent voir les noms et les parents de toutes les unités d'organisation dans la console AWS Control Tower, même s'ils ne sont pas autorisés à récupérer directement ces noms et parents. AWS Organizations
- AWS Control Tower ne prend pas en charge les autorisations mixtes pour les organisations, telles que l'autorisation de consulter le parent d'une unité d'organisation, mais pas les noms des unités d'organisation. Pour cette raison, les administrateurs d'AWS Control Tower sont tenus de disposer d'autorisations complètes.
- Le AWS Organizations `FullAWSAccess` SCP doit être appliqué et ne doit pas être fusionné avec d'autres SCP. La modification de ce SCP n'est pas signalée comme une dérive ; toutefois, certaines modifications peuvent affecter les fonctionnalités d'AWS Control Tower de manière imprévisible, si l'accès à certaines ressources est refusé. Par exemple, si le SCP est détaché ou modifié, un compte peut perdre l'accès à un AWS Config enregistreur ou créer une lacune dans la CloudTrail journalisation.
- N'utilisez pas l' AWS Organizations `DisableAWSServiceAccess`API pour désactiver l'accès du service AWS Control Tower à l'organisation dans laquelle vous avez configuré votre zone de landing zone. Dans ce cas, certaines fonctionnalités de détection de dérive d'AWS Control Tower risquent de ne pas fonctionner correctement sans l'assistance par message de AWS Organizations. Ces fonctionnalités de détection des dérives permettent à AWS Control Tower de signaler avec précision l'état de conformité des unités organisationnelles, des comptes et des contrôles de votre organisation. Pour plus d'informations, consultez API_DisableAWSServiceAccessla référence de AWS Organizations l'API.

Conseils relatifs à l'IAM Identity Center

> **Note**
>
> Le SSO est une abréviation utilisée dans le secteur de la technologie pour désigner l'authentification unique. En termes généraux, le SSO est un service d'authentification de session et d'utilisateur. Il permet à quelqu'un d'utiliser un seul ensemble d'identifiants de connexion pour accéder à de nombreuses applications. Lorsque nous parlons de la fonctionnalité d'authentification unique dans AWS, nous faisons référence au AWS service appelé AWS Identity and Access Managementet abrégé en IAM ou IAM Identity Center.

AWS Control Tower vous recommande d'utiliser AWS Identity and Access Management (IAM) pour réguler l'accès à votre Comptes AWS. Cependant, vous avez la possibilité de choisir si AWS Control Tower configure IAM Identity Center pour vous, si vous le configurez vous-même, de la manière qui répond le mieux aux besoins de votre entreprise, ou si vous souhaitez sélectionner une autre méthode d'accès au compte.

Par défaut, AWS Control Tower configure l' AWS IAM Identity Center pour votre zone de landing zone, conformément aux recommandations relatives aux meilleures pratiques définies dans la section Organisation de votre AWS environnement à l'aide de plusieurs comptes. La plupart des clients choisissent la valeur par défaut. D'autres méthodes d'accès sont parfois nécessaires, pour des raisons de conformité réglementaire dans des secteurs ou des pays spécifiques, ou dans les pays Régions AWS où AWS IAM Identity Center n'est pas disponible.

Choisir une option

Depuis la console, vous pouvez choisir de gérer vous-même IAM Identity Center pendant le processus de configuration de la zone d'atterrissage, plutôt que de laisser AWS Control Tower le configurer pour vous. Plus tard, vous pouvez choisir de modifier cette sélection en modifiant les paramètres de la zone d'atterrissage et en mettant à jour votre zone d'atterrissage sur la page des paramètres de la zone d'atterrissage.

Pour arrêter AWS IAM Identity Center dans AWS Control Tower ou pour commencer à utiliser AWS IAM Identity Center

1. Accédez à la page des paramètres de la zone d'atterrissage
2. Sélectionnez l'onglet Configurations
3. Choisissez ensuite le bouton radio approprié pour modifier votre sélection pour AWS IAM Identity Center.

Une fois que vous avez choisi de gérer vous-même AWS IAM Identity Center en tant qu'IdP, AWS Control Tower crée uniquement les rôles et les politiques nécessaires à la gestion d'AWS Control Tower, tels que et. `AWSControlTowerAdmin` `AWSControlTowerAdminPolicy` Pour les zones de destination qui s'autogèrent, AWS Control Tower ne crée plus de rôles ni de groupements IAM destinés à un usage spécifique au client, ni pendant le processus de configuration de la zone d'atterrissage, ni pendant le provisionnement du compte avec Account Factory.

> **Note**
>
> Si vous supprimez AWS IAM Identity Center de votre zone de landing zone AWS Control Tower, les utilisateurs, les groupes et les ensembles d'autorisations créés par AWS Control Tower ne sont pas supprimés. Nous vous recommandons de supprimer ces ressources.

Les clients d'Account Factory ayant recours à d'autres fournisseurs d'identité (IdPs) tels qu'Azure AD, Ping ou Okta peuvent suivre le processus AWS IAM Identity Center pour se connecter à un fournisseur d'identité externe et intégrer leur IdP. Vous pouvez demander à nouveau à AWS Control Tower de générer vos groupements et vos rôles à tout moment, en modifiant les paramètres de la zone de landing zone.

- Pour obtenir des informations spécifiques sur la manière dont AWS Control Tower fonctionne avec IAM Identity Center en fonction de votre source d'identité, consultez la section Considérations relatives aux AWS IAM Identity Center clients dans la section Contrôles préalables au lancement de la page Getting Started de ce guide de l'utilisateur.
- Pour plus d'informations sur la manière dont le comportement d'AWS Control Tower interagit avec IAM Identity Center et les différentes sources d'identité, reportez-vous à la section Considérations relatives à la modification de votre source d'identité dans le guide de l'utilisateur d'IAM Identity Center.
- Consultez Travailler avec AWS IAM Identity Center et AWS Control Tower pour plus d'informations sur l'utilisation d'AWS Control Tower et d'IAM Identity Center.

Conseils d'Account Factory

Vous pouvez rencontrer des problèmes lorsque vous utilisez Account Factory pour créer un nouveau compte dans AWS Control Tower. Pour plus d'informations sur la manière de résoudre ces problèmes, consultez la section Échec du provisionnement du nouveau compte Dépannage du guide de l'utilisateur d'AWS Control Tower.

Nous vous recommandons de créer des utilisateurs fédérés ou des rôles IAM plutôt que des utilisateurs IAM. Les utilisateurs fédérés et les rôles IAM vous fournissent des informations d'identification temporaires. Les utilisateurs IAM disposent d'informations d'identification à long terme qui peuvent être difficiles à gérer. Pour plus d'informations, consultez la section Identités IAM (utilisateurs, groupes d'utilisateurs et rôles) dans le guide de l'utilisateur IAM.

Si vous êtes authentifié en tant qu'utilisateur IAM ou utilisateur d'IAM Identity Center lors de la création d'un nouveau compte dans Account Factory ou lorsque vous utilisez la fonctionnalité d'inscription d'un compte AWS Control Tower, vérifiez que votre utilisateur a accès à votre portefeuille. AWS Service Catalog Dans le cas contraire, vous risquez de recevoir un message d'erreur de la part de Service Catalog. Pour plus d'informations, consultez Erreur Aucun chemin de lancement trouvé la section Dépannage du guide de l'utilisateur d'AWS Control Tower.

> **Note**
>
> Jusqu'à cinq comptes peuvent être provisionnés à la fois.

Conseils pour s'abonner à SNS Topics

- La rubrique `aws-controltower-AllConfigNotifications` SNS reçoit tous les événements publiés par AWS Config, y compris les notifications de conformité et les notifications d' CloudWatch événements Amazon. Par exemple, cette rubrique vous indique si une violation du contrôle s'est produite. Il fournit également des informations sur d'autres types d'événements. (Pour en savoir plus, consultez ce qu'ils publient lorsque cette rubrique est configurée.) AWS Config
- Les événements de données issus du `aws-controltower-BaselineCloudTrail` parcours sont également conçus pour être publiés dans la rubrique `aws-controltower-AllConfigNotifications` SNS.
- Pour recevoir des notifications de conformité détaillées, nous vous recommandons de vous abonner à la rubrique `aws-controltower-AllConfigNotifications` SNS. Cette rubrique regroupe les notifications de conformité provenant de tous les comptes enfants.
- Pour recevoir des notifications de dérive et d'autres notifications ainsi que des notifications de conformité, mais moins de notifications en général, nous vous recommandons de vous abonner à la rubrique `aws-controltower-AggregateSecurityNotifications` SNS.
- Pour recevoir des notifications concernant les erreurs d'AWS Control Tower Account Factory for Terraform (AFT), vous pouvez vous abonner à une rubrique SNS intitulée aft_failure_notifications, affichée dans le référentiel AFT. Par exemple :

```
resource "aws_sns_topic" "aft_failure_notifications" {
    name = "aft-failure-notifications"
    kms_master_key_id = "alias/aws/sns"
}
```

- Toutes les rubriques SNS sont chiffrées au repos grâce au chiffrement du disque. Pour plus d'informations, voir Chiffrement des données.

Pour plus d'informations sur les sujets liés aux réseaux sociaux et à la conformité, consultez la section Prévention et notification.

Conseils relatifs aux clés KMS

AWS Control Tower fonctionne avec AWS Key Management Service (AWS KMS). Si vous souhaitez chiffrer et déchiffrer les ressources de votre AWS Control Tower à l'aide d'une clé de chiffrement que vous gérez, vous pouvez éventuellement la générer et la configurer. AWS KMS keys Vous pouvez ajouter ou modifier une clé KMS à chaque fois que vous mettez à jour votre zone de landing zone. En tant que bonne pratique, nous vous recommandons d'utiliser vos propres clés KMS et de les modifier de temps à autre.

AWS KMS vous permet de créer des clés KMS multirégionales et des clés asymétriques. Cependant, AWS Control Tower ne prend pas en charge les clés multirégionales ni les clés asymétriques. AWS Control Tower effectue une pré-vérification de vos clés existantes. Un message d'erreur peut s'afficher si vous sélectionnez une clé multirégionale ou une clé asymétrique. Dans ce cas, générez une autre clé à utiliser avec les ressources AWS Control Tower.

Pour les clients qui exploitent un cluster AWS CloudHSM : créez un magasin de clés personnalisé associé à votre cluster CloudHSM. Vous pouvez ensuite créer une clé KMS, qui se trouve dans le magasin de clés personnalisé CloudHSM que vous avez créé. Vous pouvez ajouter cette clé KMS à AWS Control Tower.

Vous devez apporter une mise à jour spécifique à la politique d'autorisation d'une clé KMS pour qu'elle fonctionne avec AWS Control Tower. Pour plus de détails, reportez-vous à la section intitulée Mettre à jour la politique relative aux clés KMS.

Services basés sur l'IA et AWS Control Tower

Vous pouvez créer des politiques de contrôle des services (SCP) qui vous permettent de refuser que vos données soient stockées par des services basés sur l'IA sur. AWS Ces politiques SCP précisent que les services basés sur l'IA, tels qu'Amazon Rekognition ou CodeWhisperer Amazon, ne peuvent pas stocker et utiliser vos données pour améliorer d'autres services basés sur l'IA. AWS

Ces politiques de désactivation du SCP par l'IA peuvent s'appliquer à l'ensemble de votre organisation, à une unité d'organisation ou à un compte spécifique. Les politiques sont en vigueur à l'échelle mondiale. Vous trouverez plus d'informations sur ces politiques dans les politiques de désinscription des services d'IA, dans la AWS Organizations documentation.

Pour obtenir une liste des AWS services qui utilisent l'IA, ainsi que des exemples de politiques, voir Syntaxe et exemples de politiques de désinscription des services d'IA dans le guide de AWS Organizations l'utilisateur.

Gestion des mises à jour de configuration dans AWS Control Tower

Il est de la responsabilité des membres de l'équipe des administrateurs cloud centraux de tenir votre zone de landing zone à jour. La mise à jour de votre zone de landing zone garantit qu'AWS Control Tower est corrigée et mise à jour. En outre, pour protéger votre zone d'atterrissage contre d'éventuels problèmes de conformité, les membres de l'équipe d'administration centrale du cloud doivent résoudre les problèmes de dérive dès qu'ils sont détectés et signalés.

> **Note**
>
> La console AWS Control Tower indique à quel moment votre zone d'atterrissage doit être mise à jour. Si aucune option de mise à jour ne s'affiche, cela signifie que votre zone d'atterrissage est déjà à jour.

Le tableau suivant contient une liste des mises à jour de la zone de landing zone d'AWS Control Tower, avec des liens vers les descriptions de chaque version.

Version	Date de publication	Description
3.3	12-12-2023	Zone d'atterrissage version 3.3
3.2	6-09-2023	Zone d'atterrissage version 3.2
3.1	20/09/2023	Zone d'atterrissage version 3.1
3.0	26/07/2022	Zone d'atterrissage version 3.0
2.9	22-04-2022	Zone d'atterrissage version 2.9
2,8	2-10-2022	Zone d'atterrissage version 2.8
2.7	4-8-2021	Zone d'atterrissage version 2.7
2.6	29-12-2020	Zone d'atterrissage version 2.6
2,5	18-11-2020	Zone d'atterrissage version 2.5

Version	Date de publication	Description
2,4	Aucun	Aucun
2.3	3-5-2020	Zone d'atterrissage version 2.3
2.2	13-11-19	Zone d'atterrissage version 2.2
2.1	24-6-19	Zone d'atterrissage version 2.1

Chaque fois que vous mettez à jour votre zone d'atterrissage, vous avez la possibilité de modifier les paramètres de votre zone d'atterrissage.

Avantages de la mise à jour

- Vous pouvez modifier vos régions gouvernées
- Vous pouvez modifier votre politique de conservation des journaux
- Vous pouvez ajouter ou supprimer le refus de contrôle par région.
- Vous pouvez appliquer des clés de chiffrement AWS KMS
- Vous pouvez activer ou désactiver le suivi au niveau de votre organisation. CloudTrail
- Vous pouvez résoudre le problème de dérive de la zone d'atterrissage

Lorsque vous mettez à jour votre zone de landing zone, vous recevez automatiquement les dernières fonctionnalités d'AWS Control Tower. Consultez la version actuelle de votre zone d'atterrissage sur la page des paramètres de la zone d'atterrissage.

En cas d'échec d'une mise à jour, AWS Control Tower ne revient pas à une version précédente de la zone de landing zone. Il se peut que votre zone d'atterrissage soit dans un état indéterminé. Dans ce cas, contactez AWS le support. Pour plus d'informations sur la résolution d'un échec de mise à jour, consultezImpossible de mettre à jour la zone d'atterrissage.

Vous avez la possibilité d'effacer les mappages du centre AWS d'identité (anciennement appelé AWS SSO) non utilisés lorsque vous mettez à jour votre zone de landing zone. Pour plus d'informations, consultez Notes de terrain : effacez automatiquement les mappages de centres d'identité IAM non utilisés lors des mises à niveau d'AWS Control Tower.

Prérequis pour la mise à jour et la réinitialisation : désactiver Requester Pays

Avant de mettre à jour ou de réinitialiser votre zone de landing zone, assurez-vous que la fonctionnalité Requester Pays n'est pas activée dans le compartiment de journalisation Amazon S3 pour le compte Log Archive. Vous devez désactiver cette fonctionnalité avant de commencer le processus de mise à jour ou de réinitialisation. Lorsque AWS Control Tower configure votre compartiment de journalisation, cette fonctionnalité n'est pas activée. Par conséquent, seuls les clients qui ont ensuite activé la fonction Requester Pays doivent la désactiver. Pour plus d'informations, consultez la politique relative aux compartiments Amazon S3 CloudTrail et l'utilisation des compartiments Requester Pays.

À propos des mises à jour

Des mises à jour sont nécessaires pour corriger une dérive en matière de gouvernance ou pour passer à une nouvelle version d'AWS Control Tower. Pour effectuer une mise à jour complète d'AWS Control Tower, vous devez d'abord mettre à jour votre zone de landing zone, puis mettre à jour les comptes inscrits individuellement. Vous devrez peut-être effectuer trois types de mises à jour à différents moments.

- Une mise à jour de la zone d'atterrissage : le plus souvent, ce type de mise à jour est effectué en choisissant Mettre à jour sur la page des paramètres de la zone d'atterrissage. Il se peut que vous deviez effectuer une mise à jour de la zone d'atterrissage pour résoudre certains types de dérive, et vous pouvez choisir Reset si nécessaire.
- Mise à jour d'un ou plusieurs comptes individuels : vous devez mettre à jour les comptes si les informations associées changent ou si certains types de dérive se sont produits. Si un compte nécessite une mise à jour, le statut du compte indiquera « Mise à jour disponible » sur la page Comptes.

  Pour mettre à jour un seul compte, accédez à la page détaillée du compte et sélectionnez Mettre à jour le compte. Les comptes peuvent également être mis à jour par un processus manuel, en choisissant Re-register OU, ou selon une approche de script automatique, décrite dans une section ultérieure de cette page.
- Une mise à jour complète : une mise à jour complète inclut une mise à jour de votre zone de destination, suivie d'une mise à jour de tous les comptes inscrits dans votre unité d'organisation enregistrée. Des mises à jour complètes sont requises avec une nouvelle version d'AWS Control Tower, telle que 2.9, 3.0, etc.

> **Note**
>
> Une fois la mise à jour de la zone d'atterrissage terminée, vous ne pouvez pas annuler la mise à jour ou revenir à une version précédente.

Mettre à jour votre zone de destination

Le moyen le plus simple de mettre à jour votre zone d'atterrissage AWS Control Tower est d'utiliser la page des paramètres de la zone d'atterrissage, à laquelle vous pouvez accéder en choisissant Paramètres de la zone d'atterrissage dans la navigation de gauche du tableau de bord AWS Control Tower.

La page des paramètres de la zone d'atterrissage affiche la version actuelle de votre zone d'atterrissage et répertorie toutes les versions mises à jour qui peuvent être disponibles. Vous pouvez choisir le bouton Update (Mettre à jour) si vous avez besoin de mettre à jour votre version.

> **Note**
>
> Vous pouvez également mettre à jour votre zone de destination manuellement. La durée de la mise à jour est à peu près la même, que vous utilisiez le bouton Update (Mettre à jour) ou le processus manuel. Pour effectuer une mise à jour manuelle de votre zone de destination uniquement, veuillez consulter les étapes 1 et 2 suivantes.

Mises à jour manuelles

La procédure suivante explique les étapes d'une mise à jour complète manuelle d'AWS Control Tower. Pour mettre à jour un compte individuel, consultezMettre à jour le compte dans la console.

Pour mettre à jour votre zone d'atterrissage manuellement, avec n'importe quel nombre de comptes par unité d'organisation

1. Ouvrez un navigateur Web et accédez à la console AWS Control Tower à l'adresse https://console.aws.amazon.com/controltower/home/update.
2. Vérifiez les informations contenues dans l'assistant et choisissez Mettre à jour. Cela met à jour le backend de la zone d'atterrissage ainsi que vos comptes partagés. Ce processus peut prendre un peu plus d'une demi-heure.

3. Mettez à jour les comptes de vos membres (cette procédure doit être suivie pour une unité organisationnelle contenant plus de 300 comptes).
4. Dans le volet de navigation de gauche, sélectionnez Organisation.
5. Pour mettre à jour chaque compte, suivez les étapes indiquées dansMettre à jour le compte dans la console.

> Réenregistrez éventuellement l'unité d'organisation pour mettre à jour les comptes
>
> Pour les unités d'organisation AWS Control Tower enregistrées avec moins de 300 comptes, vous pouvez accéder à la page de l'unité d'organisation dans le tableau de bord et sélectionner Réenregistrer l'unité d'organisation pour mettre à jour les comptes de cette unité d'organisation.

Résolvez la dérive avec Reset and Re-register

La dérive se produit souvent lorsque vous et les membres de votre organisation utilisez la zone d'atterrissage.

La détection des dérives est automatique dans AWS Control Tower. Les analyses automatisées de vos SCP vous aident à identifier les ressources qui nécessitent des modifications ou des mises à jour de configuration à effectuer pour remédier à la dérive.

Pour réparer la plupart des types de dérive, choisissez Réinitialiser sur la page des paramètres de la zone d'atterrissage. Vous pouvez également résoudre certains types de dérive en choisissant de réenregistrer une unité d'organisation. Pour plus d'informations sur les types de dérive et sur la manière de les résoudre, reportez-vous aux Types de dérive de gouvernance sections etDétectez et corrigez les dérives dans AWS Control Tower.

Un cas particulier de résolution de dérive se produit pour la dérive des rôles. Si un rôle requis n'est pas disponible, la console affiche une page d'avertissement et des instructions sur la façon de restaurer le rôle. Votre zone d'atterrissage n'est pas disponible tant que la dérive des rôles n'est pas résolue. Cette réinitialisation à la dérive n'est pas la même chose qu'une réinitialisation complète de la zone d'atterrissage. Pour plus d'informations, voir Ne pas supprimer les rôles obligatoires dans la section intituléeTypes de dérive à résoudre immédiatement.

⚠ Lorsque vous prenez des mesures pour résoudre le problème de dérive sur une version en zone d'atterrissage, deux comportements sont possibles.

- Si vous utilisez la dernière version de la zone d'atterrissage, lorsque vous sélectionnez Réinitialiser puis Confirmer, les ressources de votre zone d'atterrissage dérivée sont réinitialisées selon la configuration enregistrée d'AWS Control Tower. La version de la zone d'atterrissage reste la même.
- Si vous n'utilisez pas la dernière version, vous devez sélectionner Mettre à jour. La zone d'atterrissage est mise à niveau vers la dernière version de la zone d'atterrissage. La dérive est résolue dans le cadre de ce processus.

Fournir et mettre à jour des comptes à l'aide de l'automatisation

Vous pouvez configurer ou mettre à jour des comptes individuels dans AWS Control Tower de différentes manières :

- Vous pouvez configurer et personnaliser des comptes avec AWS Control Tower Account Factory for Terraform (AFT). Pour plus d'informations, consultez Présentation d'AWS Control Tower Account Factory pour Terraform (AFT).
- Vous pouvez mettre à jour les comptes avec Customizations for AWS Control Tower (CfCT). Pour plus d'informations, consultez Présentation des personnalisations pour AWS Control Tower (CfCT) .
- Automatisation des scripts : si vous préférez utiliser une approche par API, vous pouvez mettre à jour les comptes à l'aide de l'infrastructure API de Service Catalog et mettre AWS CLI à jour les comptes par lots. Vous devez appeler l'`UpdateProvisionedProduct`API de Service Catalog pour chaque compte. Vous pouvez écrire un script pour mettre à jour les comptes, un par un, avec cette API. De plus amples informations sur cette approche, lors de l'ajout de régions pour la gouvernance, sont disponibles dans un article de blog intitulé Enabling guardrails in new AWS Regions.

  Vous pouvez mettre à jour jusqu'à cinq (5) comptes à la fois. Vous devez attendre qu'au moins une mise à jour du compte aboutisse avant de procéder à la mise à jour suivante. Par conséquent, le processus peut prendre beaucoup de temps s'il existe beaucoup de comptes, mais il n'est pas compliqué. Pour plus d'informations sur cette approche, consultez Procédure pas à pas :

Automatisez le provisionnement des comptes dans AWS Control Tower par les API Service Catalog.

> **Vidéo de démonstration**
>
> Vidéo de procédureIl est conçu pour le provisionnement automatique des comptes à l'aide d'un script, mais les étapes s'appliquent également à la mise à jour des comptes. Utilisez l'`UpdateProvisionedProduct`API au lieu de l'`ProvisionProduct`API.

Une autre étape de l'automatisation par script consiste à vérifier le statut Succeed de l'événement du `UpdateLandingZone` cycle de vie d'AWS Control Tower. Utilisez-le comme déclencheur pour commencer à mettre à jour les comptes individuels, comme décrit dans la vidéo. Un événement du cycle de vie marque la fin d'une séquence d'activités. La survenue de cet événement signifie donc qu'une mise à jour de la zone d'atterrissage est terminée. La mise à jour de la zone de destination doit être terminée avant que les mises à jour des comptes ne commencent. Pour plus d'informations sur l'utilisation des événements du cycle de vie, consultez Événements du cycle de vie.

Voir aussi :

- Utiliser AWS CloudShell pour travailler avec AWS Control Tower.
- Automatisez les tâches dans AWS Control Tower .

Automatisez les tâches dans AWS Control Tower

De nombreux clients préfèrent automatiser les tâches dans AWS Control Tower, telles que le provisionnement des comptes, l'attribution des contrôles et l'audit. Vous pouvez configurer ces actions automatisées en appelant à :

- AWS Service Catalog API
- AWS Organizations API
- API AWS Control Tower
- la AWS CLI

La Informations connexes page contient des liens vers de nombreux articles de blog techniques excellents qui peuvent vous aider à automatiser des tâches dans AWS Control Tower. Les sections suivantes fournissent des liens vers les sections de ce guide de l'utilisateur d'AWS Control Tower qui peuvent vous aider à automatiser les tâches.

Automatisation des tâches de contrôle

Vous pouvez automatiser les tâches liées à l'application et à la suppression de contrôles (également appelés barrières de sécurité) via l'API AWS Control Tower. Pour plus de détails, consultez le document de référence sur les API AWS Control Tower.

Pour plus d'informations sur la manière d'effectuer des opérations de contrôle avec les API AWS Control Tower, consultez le billet de blog AWS Control Tower releases API, predefined controls to your organization units.

Automatisation des tâches liées à la zone d'atterrissage

Les API de zone d'atterrissage d'AWS Control Tower vous aident à automatiser certaines tâches liées à votre zone d'atterrissage. Pour plus de détails, consultez le document de référence sur les API AWS Control Tower.

Automatisation de l'enregistrement de l'UO

Les API de base d'AWS Control Tower vous aident à automatiser certaines tâches, telles que l'enregistrement d'une unité d'organisation. Pour plus de détails, consultez le document de référence sur les API AWS Control Tower.

Fermeture automatique du compte

Vous pouvez automatiser la fermeture des comptes des membres d'AWS Control Tower à l'aide d'une AWS Organizations API. Pour plus d'informations, consultez Fermez le compte d'un membre AWS Control Tower via AWS Organizations.

Provisionnement et mise à jour automatisés des comptes

AWS Control Tower Account Factory Customization (AFC) vous aide à créer des comptes à partir de la console AWS Control Tower, à l'aide de AWS CloudFormation modèles personnalisés que nous appelons des plans. Ce processus est automatisé dans le sens où vous pouvez créer de nouveaux comptes et les mettre à jour à plusieurs reprises, après avoir configuré un seul plan, sans avoir à gérer les pipelines.

AWS Control Tower Account Factory for Terraform (AFT) suit un GitOps modèle pour automatiser les processus de mise en service et de mise à jour des comptes dans AWS Control Tower. Pour plus d'informations, consultez Provisionner des comptes avec AWS Control Tower Account Factory for Terraform (AFT) .

Les personnalisations pour AWS Control Tower (CfCT) vous aident à personnaliser la zone d'atterrissage de votre AWS Control Tower et à respecter les AWS meilleures pratiques. Les personnalisations sont mises en œuvre à l'aide AWS CloudFormation de modèles et de politiques de contrôle des services (SCP). Pour plus d'informations, consultez Présentation des personnalisations pour AWS Control Tower (CfCT) .

Pour plus d'informations et pour visionner une vidéo sur le provisionnement automatique des comptes, voir Procédure pas à pas : mise en service automatisée des comptes dans AWS Control Tower et Approvisionnement automatique avec les rôles IAM.

Voir également Mettre à jour les comptes par script.

Audit programmatique des comptes

Pour plus d'informations sur l'audit des comptes par programmation, consultez Rôles programmatiques et relations de confiance pour le compte d'audit AWS Control Tower.

Automatiser d'autres tâches

Pour savoir comment augmenter certains quotas de service AWS Control Tower à l'aide d'une méthode de demande automatisée, visionnez cette vidéo : Automate Service Limit Increases.

Pour les blogs techniques traitant des cas d'utilisation de l'automatisation et de l'intégration, voir Automatisation et intégration.

Deux exemples open source sont disponibles GitHub pour vous aider dans certaines tâches d'automatisation liées à la sécurité.

- L'exemple appelé aws-control-tower-org-setup-sample montre comment automatiser la configuration du compte d'audit en tant qu'administrateur délégué pour les services liés à la sécurité.
- L'exemple intitulé aws-control-tower-account- setup-using-step-functions montre comment automatiser les meilleures pratiques de sécurité à l'aide de Step Functions, lors de l'approvisionnement et de la configuration de nouveaux comptes. Cet exemple inclut l'ajout de principes aux AWS Service Catalog portefeuilles partagés au sein de l'organisation et l'association automatique de groupes AWS IAM Identity Center à de nouveaux comptes à l'échelle de l'organisation. Il montre également comment supprimer le VPC par défaut dans chaque région.

L'architecture AWS de référence de sécurité inclut des exemples de code pour automatiser les tâches liées à AWS Control Tower. Pour plus d'informations, consultez les pages de directives AWS prescriptives et le référentiel associé GitHub .

Pour plus d'informations sur l'utilisation d'AWS Control Tower with AWS CloudShell, un AWS service qui facilite le travail dans l' AWS interface de ligne de commande, consultez la section AWS CloudShell et la AWS CLI.

AWS Control Tower étant une couche d'orchestration pour AWS Organizations, de nombreux autres AWS services sont disponibles au moyen d'API et de la AWS CLI. Pour plus d'informations, consultez la section AWS Services associés.

Utiliser AWS CloudShell pour travailler avec AWS Control Tower

AWS CloudShell est un AWS service qui facilite le travail dans la AWS CLI. Il s'agit d'un shell pré-authentifié basé sur un navigateur que vous pouvez lancer directement depuis le. AWS Management ConsoleIl n'est pas nécessaire de télécharger ou d'installer des outils de ligne de commande. Vous pouvez exécuter AWS CLI des commandes AWS Control Tower et d'autres AWS services à partir de votre shell préféré (shell Bash PowerShell ou Z).

Lorsque vous lancez AWS CloudShell depuis le AWS Management Console, les AWS informations d'identification que vous avez utilisées pour vous connecter à la console sont disponibles dans une nouvelle session shell. Vous pouvez ignorer la saisie de vos informations d'identification de configuration lorsque vous interagissez avec AWS Control Tower d'autres AWS services, et vous

utiliserez la AWS CLI version 2, qui est préinstallée sur l'environnement informatique du shell. Vous êtes pré-authentifié avec. AWS CloudShell

Obtention des autorisations IAM pour AWS CloudShell

AWS Identity and Access Management fournit des ressources de gestion des accès qui permettent aux administrateurs d'accorder des autorisations d'accès aux utilisateurs IAM et aux utilisateurs d'IAM Identity Center. AWS CloudShell

Le moyen le plus rapide pour un administrateur d'accorder l'accès aux utilisateurs est d'utiliser une politique AWS gérée. Une politique gérée parAWS est une politique autonome qui est créée et gérée par AWS. La politique AWS gérée suivante pour CloudShell peut être attachée aux identités IAM :

- `AWSCloudShellFullAccess`: accorde l'autorisation d'utilisation AWS CloudShell avec un accès complet à toutes les fonctionnalités.

Si vous souhaitez limiter l'étendue des actions qu'un utilisateur IAM ou IAM Identity Center peut effectuer AWS CloudShell, vous pouvez créer une politique personnalisée qui utilise la stratégie `AWSCloudShellFullAccess` gérée comme modèle. Pour plus d'informations sur la limitation des actions disponibles pour les utilisateurs dans CloudShell, consultez la section Gestion de l' AWS CloudShell accès et de l'utilisation avec les politiques IAM dans le Guide de l'AWS CloudShell utilisateur.

> **Note**
>
> Votre identité IAM nécessite également une politique qui accorde l'autorisation de passer des appels à AWS Control Tower. Pour plus d'informations, consultez la section Autorisations requises pour utiliser la AWS Control Tower console.

Interagir avec AWS Control Tower l'utilisation AWS CloudShell

Après le lancement AWS CloudShell depuis le AWS Management Console, vous pouvez immédiatement commencer à interagir avec AWS Control Tower depuis l'interface de ligne de commande. AWS CLI les commandes fonctionnent de manière standard dans CloudShell.

> **Note**
>
> Lorsque vous AWS CLI l'utilisez AWS CloudShell, vous n'avez pas besoin de télécharger ou d'installer de ressources supplémentaires. Vous êtes déjà authentifié dans le shell, vous n'avez donc pas besoin de configurer les informations d'identification avant de passer des appels.

Lancement AWS CloudShell

- À partir de AWS Management Console, vous pouvez lancer CloudShell en choisissant les options suivantes disponibles dans la barre de navigation :
  - Choisissez l' CloudShell icône.
  - Commencez à taper « cloudshell » dans le champ de recherche, puis choisissez l' CloudShelloption.

  Maintenant que vous avez commencé CloudShell, vous pouvez saisir toutes AWS CLI les commandes dont vous avez besoin pour travailler AWS Control Tower. Par exemple, vous pouvez vérifier votre AWS Config statut.

Utilisation AWS CloudShell pour faciliter la configuration AWS Control Tower

Avant d'exécuter ces procédures, sauf indication contraire, vous devez être connecté à la AWS Management Console région d'origine de votre zone d'atterrissage, et vous devez être connecté en tant qu'utilisateur IAM Identity Center ou utilisateur IAM avec des autorisations administratives pour le compte de gestion contenant votre zone d'atterrissage.

1. Voici comment vous pouvez utiliser les commandes AWS Config CLI AWS CloudShell pour déterminer l'état de votre enregistreur de configuration et de votre canal de diffusion avant de commencer à configurer votre zone AWS Control Tower d'atterrissage.

   Vérifiez votre AWS Config statut

   Commandes d'affichage :

   - `aws configservice describe-delivery-channels`
   - `aws configservice describe-delivery-channel-status`

- `aws configservice describe-configuration-recorders`
- `The normal response is something like "name": "default"`

2. Si vous avez un AWS Config enregistreur ou un canal de diffusion existant que vous devez supprimer avant de configurer votre zone de AWS Control Tower landing zone, voici quelques commandes que vous pouvez saisir :

   Gérez vos ressources préexistantes AWS Config

   Commandes de suppression :

   - `aws configservice stop-configuration-recorder --configuration-recorder-name` *`NAME-FROM-DESCRIBE-OUTPUT`*
   - `aws configservice delete-delivery-channel --delivery-channel-name` *`NAME-FROM-DESCRIBE-OUTPUT`*
   - `aws configservice delete-configuration-recorder --configuration-recorder-name` *`NAME-FROM-DESCRIBE-OUTPUT`*

   > **Important**
   >
   > Ne supprimez pas les AWS Control Tower ressources pour AWS Config. La perte de ces ressources peut AWS Control Tower entraîner l'entrée dans un état incohérent.

   Pour plus d'informations, consultez la documentation AWS Config

   - Gestion de l'enregistreur de configuration (AWS CLI)
   - Gestion du canal de distribution

3. Cet exemple montre les commandes AWS CLI AWS CloudShell à partir desquelles vous devez entrer pour activer ou désactiver l'accès sécurisé AWS Organizations. Car il AWS Control Tower n'est pas nécessaire d'activer ou de désactiver l'accès sécurisé pour AWS Organizations, ce n'est qu'un exemple. Toutefois, vous devrez peut-être activer ou désactiver l'accès sécurisé pour d'autres AWS services si vous automatisez ou personnalisez des actions dans. AWS Control Tower

Activer ou désactiver l'accès aux services sécurisés

- `aws organizations enable-aws-service-access`
- `aws organizations disable-aws-service-access`

Créez un compartiment Amazon S3 avec AWS CloudShell

Dans l'exemple suivant, vous pouvez AWS CloudShell créer un compartiment Amazon S3, puis utiliser la PutObjectméthode pour ajouter un fichier de code en tant qu'objet dans ce compartiment.

1. Pour créer un bucket dans une AWS région spécifiée, entrez la commande suivante dans la ligne de CloudShell commande :

   ```
   aws s3api create-bucket --bucket insert-unique-bucket-name-here --region us-east-1
   ```

   Si l'appel aboutit, la ligne de commande affiche une réponse du service similaire au résultat suivant :

   ```
   {
       "Location": "/insert-unique-bucket-name-here"
   }
   ```

   > **Note**
   >
   > Si vous ne respectez pas les règles de dénomination des compartiments (en utilisant uniquement des lettres minuscules, par exemple), le message d'erreur suivant s'affiche : Une erreur s'est produite (InvalidBucketName) lors de l'appel de l' CreateBucket opération : Le compartiment spécifié n'est pas valide.

2. Pour télécharger un fichier et l'ajouter en tant qu'objet au bucket qui vient d'être créé, appelez la PutObject méthode suivante :

   ```
   aws s3api put-object --bucket insert-unique-bucket-name-here --key add_prog --body
    add_prog.py
   ```

   Si l'objet est correctement chargé dans le compartiment Amazon S3, la ligne de commande affiche une réponse du service similaire à la sortie suivante :

```
{
            "ETag": "\"ab123c1:w:wad4a567d8bfd9a1234ebeea56\""}
```

`ETag`Il s'agit du hachage de l'objet qui a été stocké. Il peut être utilisé pour vérifier l'intégrité de l'objet chargé sur Amazon S3.

Création de AWS Control Tower ressources avec AWS CloudFormation

AWS Control Tower est intégré à AWS CloudFormation un service qui vous aide à modéliser et à configurer vos AWS ressources afin que vous puissiez passer moins de temps à créer et à gérer vos ressources et votre infrastructure. Vous créez un modèle qui décrit toutes les AWS ressources souhaitées, par exemple `AWS::ControlTower::EnabledControl` pour les contrôles. AWS CloudFormation fournit et configure ces ressources pour vous.

Lorsque vous l'utilisez AWS CloudFormation, vous pouvez réutiliser votre modèle pour configurer vos AWS Control Tower ressources de manière cohérente et répétée. Décrivez vos ressources une seule fois, puis fournissez les mêmes ressources encore et encore dans plusieurs Comptes AWS régions.

AWS Control Tower et AWS CloudFormation modèles

Pour fournir et configurer des ressources AWS Control Tower et des services associés, vous devez comprendre les AWS CloudFormation modèles. Les modèles sont des fichiers texte formatés en JSON ou YAML. Ces modèles décrivent les ressources que vous souhaitez mettre à disposition dans vos AWS CloudFormation piles. Si vous n'êtes pas familiarisé avec JSON ou YAML, vous pouvez utiliser AWS CloudFormation Designer pour vous aider à démarrer avec les AWS CloudFormation modèles. Pour plus d'informations, consultez Qu'est-ce que AWS CloudFormation Designer ? dans le AWS CloudFormation Guide de l'utilisateur.

AWS Control Tower prend en charge la création `AWS::ControlTower::EnabledControl` (ressources de contrôle), `AWS::ControlTower::LandingZone` (zones d'atterrissage) et `AWS::ControlTower::EnabledBaseline` (lignes de base) dans AWS CloudFormation. Pour plus d'informations, notamment des exemples de modèles JSON et YAML pour ces types de ressources, consultez le guide AWS Control Towerde l'AWS CloudFormation utilisateur.

> **Note**
>
> La limite pour les `DisableControl` mises à jour `EnableControl` et les mises à jour AWS Control Tower est de 100 opérations simultanées, dont 20 au maximum concernent les contrôles proactifs.

Pour consulter des AWS Control Tower exemples relatifs à la CLI et à la console, consultez la section Activer les contrôles avec AWS CloudFormation.

En savoir plus sur AWS CloudFormation

Pour en savoir plus AWS CloudFormation, consultez les ressources suivantes :

- AWS CloudFormation
- AWS CloudFormation Guide de l'utilisateur
- Référence d'API AWS CloudFormation
- AWS CloudFormation Guide de l'utilisateur de l'interface de ligne de commande

Personnalisez la zone de landing de votre AWS Control Tower

Certains aspects de votre zone de landing zone AWS Control Tower sont configurables dans la console, tels que la sélection des régions et les contrôles optionnels. D'autres modifications peuvent être apportées en dehors de la console, grâce à l'automatisation.

Par exemple, vous pouvez créer des personnalisations plus poussées de votre zone d'atterrissage grâce à la fonctionnalité Customizations for AWS Control Tower, une structure de personnalisation de GitOps type C qui fonctionne avec les AWS CloudFormation modèles et les événements du cycle de vie d'AWS Control Tower.

Personnalisation depuis la console AWS Control Tower

Pour personnaliser votre zone de landing zone, suivez les étapes indiquées par la console AWS Control Tower.

Sélectionnez des noms personnalisés lors de la configuration

- Vous pouvez sélectionner les noms de vos unités d'organisation de premier niveau lors de la configuration. Vous pouvez renommer vos unités d'organisation à tout moment à l'aide de la AWS Organizations console, mais leur modification AWS Organizations peut entraîner une dérive réparable.
- Vous pouvez sélectionner les noms de vos comptes d'audit et d'archivage des journaux partagés, mais vous ne pouvez pas les modifier après la configuration. (Il s'agit d'une sélection unique.)

> **Conseil**
>
> N'oubliez pas que le fait de renommer une unité d' AWS Organizations organisation ne met pas à jour le produit provisionné correspondant dans Account Factory. Pour mettre à jour automatiquement le produit provisionné (et éviter toute dérive), vous devez exécuter l'opération de l'unité d'organisation via AWS Control Tower, notamment en créant, en supprimant ou en réenregistrant une unité d'organisation.

Sélectionnez AWS les régions

- Vous pouvez personnaliser votre zone de landing zone en sélectionnant des AWS régions spécifiques pour la gouvernance. Suivez les étapes indiquées dans la console AWS Control Tower.
- Vous pouvez sélectionner et désélectionner les AWS régions à des fins de gouvernance lorsque vous mettez à jour votre zone de landing zone.
- Vous pouvez définir le contrôle Region Deny sur Activé ou Non activé, et contrôler l'accès des utilisateurs à la plupart des AWS services dans les AWS régions non gouvernées.

Pour plus d'informations sur les domaines Régions AWS dans lesquels le CfCT est soumis à des limites de déploiement, consultezLimites de contrôle.

Personnalisez en ajoutant des commandes facultatives

- Les contrôles facultatifs et fortement recommandés sont facultatifs, ce qui signifie que vous pouvez personnaliser le niveau d'application pour votre zone d'atterrissage en choisissant ceux que vous souhaitez activer. Les commandes facultatives ne sont pas activées par défaut.
- Les contrôles facultatifs de résidence des données vous permettent de personnaliser les régions dans lesquelles vous stockez vos données et d'autoriser l'accès à celles-ci.
- Les contrôles optionnels inclus dans la norme Security Hub intégrée vous permettent de scanner votre environnement AWS Control Tower afin de détecter les risques de sécurité.
- Les contrôles proactifs optionnels vous permettent de vérifier vos AWS CloudFormation ressources avant qu'elles ne soient provisionnées, afin de vous assurer que les nouvelles ressources seront conformes aux objectifs de contrôle de votre environnement.

Personnalisez vos AWS CloudTrail sentiers

- Lorsque vous mettez à jour votre zone de landing zone vers la version 3.0 ou ultérieure, vous pouvez choisir d'accepter ou de refuser les CloudTrail parcours au niveau de l'organisation gérés par AWS Control Tower. Vous pouvez modifier cette sélection à chaque fois que vous mettez à jour votre zone de landing zone. AWS Control Tower crée une trace au niveau de l'organisation dans votre compte de gestion, et cette trace passe au statut actif ou inactif, selon votre choix. La zone d'atterrissage 3.0 ne prend pas en charge les CloudTrail sentiers au niveau du compte ; toutefois, si vous en avez besoin, vous pouvez configurer et gérer vos propres sentiers. Vous pouvez avoir à payer des frais supplémentaires pour les sentiers dupliqués.

Créez des comptes de membres personnalisés dans la console

- Vous pouvez créer des comptes membres AWS Control Tower personnalisés, et vous pouvez mettre à jour les comptes membres existants pour ajouter des personnalisations, depuis la console AWS Control Tower. Pour plus d'informations, consultez Personnalisez les comptes avec Account Factory Customization (AFC).

Automatisez les personnalisations en dehors de la console AWS Control Tower

Certaines personnalisations ne sont pas disponibles via la console AWS Control Tower, mais elles peuvent être mises en œuvre de différentes manières. Par exemple :

- Vous pouvez personnaliser les comptes pendant le provisionnement, dans un flux de travail de GitOps type C, avec Account Factory for Terraform (AFT).

  AFT est déployé avec un module Terraform, disponible dans le référentiel AFT.
- Vous pouvez personnaliser la zone d'atterrissage de votre AWS Control Tower grâce à Customizations for AWS Control Tower (CfCT), un ensemble de fonctionnalités basé sur des AWS CloudFormation modèles et des politiques de contrôle des services (SCP). Vous pouvez déployer les modèles et politiques personnalisés sur des comptes individuels et des unités organisationnelles (UO) au sein de votre organisation.

  Le code source de CfCT est disponible dans un GitHub dépôt.

Avantages des personnalisations pour AWS Control Tower (CfCT)

L'ensemble de fonctionnalités que nous appelons Customizations for AWS Control Tower (CfCT) vous permet de créer des personnalisations plus étendues pour votre zone d'atterrissage que celles que vous pouvez créer dans la console AWS Control Tower. Il propose un processus automatisé de GitOps type X. Vous pouvez remodeler votre zone d'atterrissage pour répondre aux besoins de votre entreprise.

Ce processus infrastructure-as-codede personnalisation intègre des AWS CloudFormation modèles aux politiques de contrôle des AWS services (SCP) et aux événements du cycle de vie d'AWS Control Tower, afin que vos déploiements de ressources restent synchronisés avec votre zone

de landing zone. Par exemple, lorsque vous créez un nouveau compte avec Account Factory, les ressources associées au compte et à l'unité d'organisation peuvent être déployées automatiquement.

> **Note**
>
> Contrairement à Account Factory et AFT, CfCT n'est pas spécifiquement destiné à créer de nouveaux comptes, mais à personnaliser les comptes et les unités d'organisation dans votre zone de landing zone en déployant les ressources que vous spécifiez.

Avantages

- Développez un AWS environnement personnalisé et sécurisé — Vous pouvez développer plus rapidement votre environnement AWS Control Tower multi-comptes et intégrer les AWS meilleures pratiques dans un flux de travail de personnalisation reproductible.
- Instanciez vos exigences : vous pouvez personnaliser la zone de landing de votre AWS Control Tower en fonction des besoins de votre entreprise, à l'aide des AWS CloudFormation modèles et des politiques de contrôle des services qui expriment vos intentions en matière de politique.
- Automatisez davantage grâce aux événements du cycle de vie d'AWS Control Tower : les événements du cycle de vie vous permettent de déployer des ressources en fonction de la fin d'une série d'événements précédente. Vous pouvez compter sur un événement du cycle de vie pour vous aider à déployer automatiquement des ressources sur des comptes et des unités d'organisation.
- Étendez votre architecture réseau : vous pouvez déployer des architectures réseau personnalisées qui améliorent et protègent votre connectivité, comme une passerelle de transit.

Exemples supplémentaires de CfCT

- Un exemple d'utilisation réseau avec Customizations for AWS Control Tower (CfCT) est présenté dans le billet de blog sur l' AWS architecture, Deploy consistent DNS with Service Catalog and AWS Control Tower customizations.
- Un exemple spécifique lié à CfCT et Amazon GuardDuty est disponible GitHub dans le `aws-samples`référentiel.
- Des exemples de code supplémentaires concernant CfCT sont disponibles dans le cadre de l'architecture de référence de AWS sécurité, dans le `aws-samples`référentiel. La plupart de ces exemples contiennent des exemples de `manifest.yaml` fichiers dans un répertoire nommé`customizations_for_aws_control_tower`.

Pour plus d'informations sur l'architecture AWS de référence de sécurité, consultez les pages de conseils AWS prescriptifs.

Présentation des personnalisations pour AWS Control Tower (CfCT)

Les personnalisations pour AWS Control Tower (CfCT) vous aident à personnaliser la zone d'atterrissage de votre AWS Control Tower et à respecter les AWS meilleures pratiques. Les personnalisations sont mises en œuvre à l'aide AWS CloudFormation de modèles et de politiques de contrôle des services (SCP).

Cette fonctionnalité CfCT est intégrée aux événements du cycle de vie d'AWS Control Tower, afin que vos déploiements de ressources restent synchronisés avec votre zone de landing zone. Par exemple, lorsqu'un nouveau compte est créé via Account Factory, toutes les ressources associées au compte sont déployées automatiquement. Vous pouvez déployer les modèles et politiques personnalisés sur des comptes individuels et des unités organisationnelles (UO) au sein de votre organisation.

La vidéo suivante décrit les meilleures pratiques pour déployer un pipeline cFCT évolutif et les personnalisations courantes des cFCT.

La section suivante fournit des considérations architecturales et des étapes de configuration pour le déploiement de Customizations for AWS Control Tower (CfCT). Il inclut un lien vers le AWS CloudFormationmodèle qui lance, configure et exécute les AWS services requis, conformément aux AWS meilleures pratiques en matière de sécurité et de disponibilité.

Cette rubrique s'adresse aux architectes et aux développeurs d'infrastructures informatiques ayant une expérience pratique de l'architecture dans le AWS cloud.

Pour plus d'informations sur les dernières mises à jour et modifications apportées à Customizations for AWS Control Tower (CfCT), consultez le fichier ChangeLog.md dans le référentiel. GitHub

Présentation de l'architecture

Le déploiement de CfCT crée l'environnement suivant dans le AWS cloud.

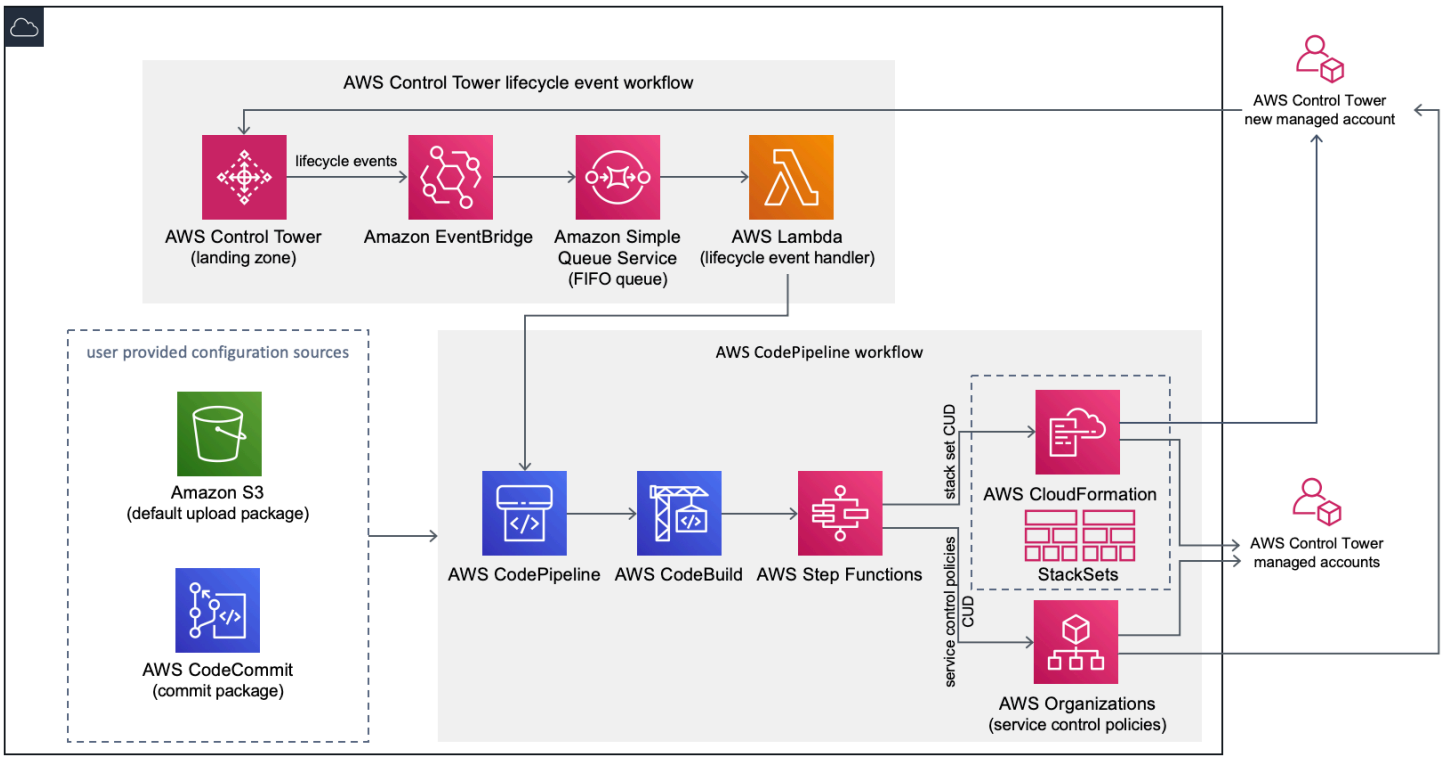


Figure 1 : Personnalisations pour l'architecture AWS Control Tower

CfCT inclut un AWS CloudFormation modèle que vous déployez dans votre compte de gestion AWS Control Tower. Le modèle lance tous les composants nécessaires à la création des flux de travail, afin que vous puissiez personnaliser votre zone de landing zone AWS Control Tower.

> **Remarque**
>
> Le CfCT doit être déployé dans la région d'origine d'AWS Control Tower et dans le compte de gestion de la tour de contrôle AWS, car c'est là que votre zone d'atterrissage AWS Control Tower est déployée. Pour plus d'informations sur la configuration d'une zone d'atterrissage AWS Control Tower, reportez-vous àPremiers pas.

Lorsque vous déployez CfCT, il empaquète et télécharge les ressources personnalisées vers la source du pipeline de code, au moyen d'Amazon Simple Storage Service (Amazon S3). Le processus de téléchargement appelle automatiquement la machine d'état des politiques de contrôle des services (SCP) et la machine d'AWS CloudFormation StackSetsétat pour déployer les SCP au niveau de l'unité d'organisation ou pour déployer des instances de pile au niveau de l'unité d'organisation ou du compte.

> **Remarque**
>
> Par défaut, CfCT crée un compartiment Amazon S3 pour stocker la source du pipeline, mais vous pouvez modifier l'emplacement pour en faire un AWS CodeCommitréférentiel. Pour plus d'informations, consultez Configurer Amazon S3 en tant que source de configuration.

CfCT déploie deux flux de travail :

- un AWS CodePipelineflux de travail
- et un flux de travail relatif aux événements liés au cycle de vie d'AWS Control Tower.

Le AWS CodePipeline flux de travail

Le AWS CodePipeline flux de travail configure AWS CodePipeline, AWS CodeBuildprojette et AWS Step Functionsorchestre la gestion des SCP au AWS CloudFormation StackSets sein de votre organisation.

Lorsque vous téléchargez le package de configuration, CFct invoque le pipeline de code pour exécuter trois étapes.

- Étape de construction : valide le contenu du package de configuration à l'aide d'AWS CodeBuild.
- SCP Stage — invoque la machine d'état des politiques de contrôle des services, qui appelle l' AWS Organizations API pour créer des SCP.
- AWS CloudFormation Stage : invoque la machine d'état du stack set pour déployer les ressources spécifiées dans la liste des comptes ou des unités d'organisation, que vous avez fournie dans le fichier manifeste.

À chaque étape, le pipeline de code invoque les fonctions stack set et SCP step, qui déploient des ensembles de piles et des SCP personnalisés sur les comptes individuels ciblés ou sur une unité organisationnelle complète.

> **Remarque**
>
> Pour obtenir des informations détaillées sur la personnalisation du package de configuration, reportez-vous àGuide de personnalisation du CfCT.

Le flux de travail des événements liés au cycle de vie d'AWS Control Tower

Lorsqu'un nouveau compte est créé dans AWS Control Tower, un événement du cycle de vie peut appeler le AWS CodePipeline flux de travail. Vous pouvez personnaliser le package de configuration via ce flux de travail, qui comprend une règle d' EventBridgeévénement Amazon, une file d'attente « premier entré, premier sorti » (FIFO) Amazon Simple Queue Service (Amazon SQS) et une fonction. AWS Lambda

Lorsque la règle d' EventBridge événement Amazon détecte un événement du cycle de vie correspondant, elle transmet l'événement à la file d'attente FIFO Amazon SQS, invoque la AWS Lambda fonction et invoque le pipeline de code pour effectuer le déploiement en aval des stack sets et des SCP.

Coût

Le coût d'exécution de CfCT dépend du nombre d' AWS CodePipeline essais, de la durée des AWS CodeBuild essais, du nombre et de la durée des AWS Lambda fonctions, ainsi que du nombre d' EventBridge événements Amazon publiés. Par exemple, si vous exécutez 100 versions en un mois à l'aide de build.general1.small où chaque version s'exécute pendant cinq minutes, le coût approximatif de l'exécution de CfCT est de 3$ par mois. Pour plus de détails, vous pouvez consulter la page Web de tarification de chaque AWS service que vous utilisez.

Le bucket Amazon Simple Storage Service (Amazon S3) et les ressources du référentiel basé sur CodeCommit AWS Git sont conservés après la suppression du modèle, afin de protéger vos informations de configuration. Selon l'option que vous sélectionnez, vous êtes facturé en fonction de la quantité de données stockées dans le compartiment Amazon S3 et du nombre de requêtes Git (non applicable à la ressource Amazon S3). Consultez les CodeCommit tarifs d'Amazon S3 et d'AWS pour plus de détails.

Services relatifs aux composants

Les AWS services suivants sont des composants de Customizations for AWS Control Tower (CfCT).

AWS CodeCommit

Sur la base de vos entrées dans le AWS CloudFormation modèle, CfCT peut créer un AWS CodeCommitréférentiel avec le même exemple de configuration que celui expliqué dans la section Amazon Simple Storage Service.

Pour cloner le AWS CodeCommit référentiel CfCT sur votre ordinateur local, vous devez créer des informations d'identification qui vous donnent un accès temporaire au référentiel, comme expliqué dans le guide de l'AWS CodeCommit utilisateur. Pour plus d'informations sur la compatibilité des versions, voir Configuration pour AWS CodeCommit.

AWS CodePipeline

AWS CodePipeline valide, teste et implémente les modifications en fonction des mises à jour du package de configuration, que vous apporterez soit dans le compartiment Amazon S3 par défaut, soit dans le AWS CodeCommit référentiel. Pour plus d'informations sur la modification du contrôle de source de configuration en AWS CodeCommit, consultez Utiliser Amazon S3 comme source de configuration. Le pipeline comprend des étapes pour valider et gérer les fichiers et modèles de configuration, les comptes principaux, les politiques de contrôle des AWS Organizations services, et AWS CloudFormation StackSets. Pour plus d'informations sur les étapes du pipeline, reportez-vous à Guide de personnalisation du CfCT

AWS Key Management Service

CfCT crée une clé de `CustomControlTowerKMSKey` chiffrement AWS Key Management Service(AWS KMS). Cette clé est utilisée pour chiffrer les objets du compartiment de configuration Amazon S3, de la file d'attente Amazon SQS et des paramètres sensibles du magasin de paramètres Systems AWS Manager. Par défaut, seuls les rôles fournis par CfCT sont autorisés à effectuer des opérations de chiffrement ou de déchiffrement avec cette clé. Pour accéder au fichier de configuration, à la file d'attente FIFO ou aux `SecureString` valeurs du magasin de paramètres, des administrateurs doivent être ajoutés à la `CustomControlTowerKMSKey` politique. La rotation automatique des touches est activée par défaut.

AWS Lambda

CfCT utilise des AWS Lambda fonctions pour invoquer les composants d'installation lors de l'installation et du déploiement initiaux AWS CloudFormation StackSets ou des AWS Organizations SCP lors d'un événement du cycle de vie d'AWS Control Tower.

Amazon Simple Notification Service

CfCT peut publier des notifications, telles que l'approbation du pipeline sur des sujets Amazon Simple Notification Service (Amazon SNS) pendant le flux de travail. Amazon SNS est lancé uniquement lorsque vous choisissez de recevoir des notifications d'approbation du pipeline.

Amazon Simple Storage Service

Lorsque vous déployez CfCT, CfCT crée un bucket Amazon Simple Storage Service (Amazon S3) avec un nom unique :

Exemple : nom du compartiment Amazon S3

`custom-control-tower-configuration-`*`accountID`*`-`*`region`*

Le bucket contient un exemple de fichier de configuration appelé `_custom-control-tower-configuration.zip`

Notez le trait de soulignement principal dans le nom du fichier.

Ce fichier zip fournit un exemple de manifeste et les exemples de modèles associés qui décrivent la structure de dossiers nécessaire. Ces exemples vous aident à développer un package de configuration pour personnaliser votre zone de landing AWS Control Tower. L'exemple de manifeste identifie les configurations requises pour les ensembles de piles et les politiques de contrôle des services (SCP) dont vous aurez besoin lors de la mise en œuvre de vos personnalisations.

Vous pouvez utiliser cet exemple de package de configuration comme modèle pour développer et télécharger votre package personnalisé, qui déclenche automatiquement le pipeline de configuration CfCT.

Pour plus d'informations sur la personnalisation du fichier de configuration, consultezGuide de personnalisation du CfCT.

Amazon Simple Queue Service

CfCT utilise une file d'attente FIFO Amazon Simple Queue Service (Amazon SQS) pour capturer les événements du cycle de vie d'Amazon. EventBridge Il déclenche une AWS Lambda fonction qui invoque le déploiement AWS CloudFormation StackSets ou AWS CodePipeline les SCP. Pour plus d'informations sur les SCP, consultez AWS Organizations.

AWS Step Functions

CfCT crée Step Functions pour orchestrer les déploiements de personnalisation. Ces Step Functions traduisent les fichiers de configuration pour déployer les personnalisations nécessaires dans les environnements.

AWS Systems Manager Parameter Store

AWS Systems Manager Parameter Store stocke les paramètres de configuration CfCT. Ces paramètres vous permettent d'intégrer des modèles de configuration associés. Par exemple, vous pouvez configurer chaque compte pour enregistrer AWS CloudTrail les données dans un compartiment Amazon S3 centralisé. En outre, le magasin de paramètres Systems Manager fournit un emplacement centralisé où les administrateurs peuvent consulter les entrées et les paramètres CfCT.

Considérations relatives au déploiement

Assurez-vous de lancer Customizations for AWS Control Tower (CfCT) dans le même compte et dans la même région que ceux où votre zone d'atterrissage AWS Control Tower est déployée ; en d'autres termes, vous devez la déployer sur le compte de gestion AWS Control Tower de votre région d'origine AWS Control Tower. Par défaut, CfCT crée et exécute le package de configuration de la zone d'atterrissage en configurant un pipeline de configuration dans ce compte et cette région.

Préparation au déploiement

Certaines options s'offrent à vous lorsque vous préparez votre AWS CloudFormation modèle pour le déploiement initial. Vous pouvez choisir la source de configuration et autoriser l'approbation manuelle des déploiements de pipelines. Les deux sections suivantes expliquent plus en détail ces options.

Choisissez votre source de configuration

Par défaut, le modèle crée un bucket Amazon Simple Storage Service (Amazon S3) pour stocker l'exemple de package de configuration sous la forme d'`.zip`un fichier appelé. `_custom-control-tower-configuration.zip` Le compartiment Amazon S3 est contrôlé par version et vous pouvez mettre à jour le package de configuration selon vos besoins. Pour plus d'informations sur la mise à jour du package de configuration, consultez Utiliser Amazon S3 comme source de configuration.

> **Remarque**
>
> Le nom du fichier d'exemple de package de configuration commence par un trait de soulignement (_) afin qu'il ne AWS CodePipeline soit pas lancé automatiquement. Lorsque vous avez fini de personnaliser le package de configuration, veillez à le télécharger `custom-control-tower-configuration.zip` sans le trait de soulignement (_) afin de commencer le déploiement dans. AWS CodePipeline

Vous pouvez modifier l'emplacement de stockage du package de configuration du compartiment S3 vers un référentiel AWS CodeCommit Git en sélectionnant l'`AWS CodeCommit`option dans le AWS CloudFormation paramètre. Cette option vous permet de gérer facilement le contrôle des versions.

> **Remarque**
>
> Lorsque vous utilisez le compartiment S3 par défaut, assurez-vous que le package de configuration est disponible sous forme de `.zip` fichier. Lorsque vous utilisez le AWS CodeCommit référentiel, assurez-vous que le package de configuration y est placé sans compresser les fichiers. Pour plus d'informations sur la création et le stockage du package de configuration dans AWS CodeCommit, consultezGuide de personnalisation du CfCT.

Vous pouvez utiliser l'exemple de package de configuration pour créer votre propre source de configuration personnalisée. Lorsque vous êtes prêt à déployer vos configurations personnalisées, téléchargez manuellement le package de configuration, soit dans le compartiment Amazon S3, soit dans le AWS CodeCommit référentiel. Le pipeline démarre automatiquement lorsque vous téléchargez le fichier de configuration.

> **Remarque**
>
> Lorsque vous l'utilisez AWS CodeCommit pour stocker le package de configuration, il n'est pas nécessaire de compresser le package. Pour plus d'informations sur la création et le stockage du package de configuration dans AWS CodeCommit, reportez-vous àGuide de personnalisation du CfCT.

Choisissez les paramètres d'approbation de la configuration de votre pipeline

Le AWS CloudFormation modèle offre la possibilité d'approuver le déploiement des modifications de configuration manuellement. Par défaut, l'approbation manuelle n'est pas activée. Pour plus d'informations, reportez-vous à l'étape 1. Lancez la pile.

Lorsque l'approbation manuelle est activée, le pipeline de configuration valide les personnalisations apportées au manifeste de fichiers et aux modèles d'AWS Control Tower, puis il suspend le processus jusqu'à ce que l'approbation manuelle soit accordée. Après approbation, le déploiement passe aux étapes restantes du pipeline, selon les besoins, afin de mettre en œuvre la fonctionnalité Customizations for AWS Control Tower (CfCT).

Vous pouvez utiliser le paramètre d'approbation manuelle pour empêcher l'exécution des personnalisations relatives à la configuration d'AWS Control Tower, en rejetant la première tentative d'exécution dans le pipeline. Ce paramètre vous permet également de valider manuellement les personnalisations pour les modifications de configuration d'AWS Control Tower, en tant que contrôle final avant la mise en œuvre.

Pour mettre à jour les personnalisations pour AWS Control Tower

Si vous avez déjà déployé CfCT, vous devez mettre à jour la AWS CloudFormation pile pour obtenir la dernière version du framework CfCT. Pour plus de détails, reportez-vous à la section Mettre à jour la pile.

Modèle et code source

Les personnalisations pour AWS Control Tower (CfCT) sont déployées dans votre compte de gestion après le lancement de votre AWS CloudFormation modèle. Vous pouvez télécharger le modèle depuis, GitHub puis le lancer depuis AWS CloudFormation.

Le customizations-for-aws-control-tower.template déploie les éléments suivants :

- Un AWS CodeBuild projet
- Un AWS CodePipeline projet
- Une EventBridge règle Amazon
- AWS Lambda fonctions
- Une file d'attente Amazon Simple Queue Service
- Un bucket Amazon Simple Storage Service avec un exemple de package de configuration
- AWS Step Functions

> **Note**
>
> Vous pouvez personnaliser le modèle en fonction de vos besoins spécifiques.

Référentiel de code source

Vous pouvez visiter notre GitHub référentiel pour télécharger les modèles et les scripts pour CfCT et pour partager les personnalisations de votre zone d'atterrissage avec d'autres personnes.

Déploiement automatique

Avant de lancer le déploiement automatique, passez en revue les considérations. Suivez les step-by-step instructions de cette section pour configurer et déployer la solution dans votre compte de gestion AWS Control Tower.

Temps de déploiement : environ 15 minutes

Prérequis

Le CfCT doit être déployé dans votre compte de gestion AWS Control Tower et dans votre région d'origine AWS Control Tower. Si aucune zone d'atterrissage n'est configurée, reportez-vous àPremiers pas.

Étapes de déploiement

La procédure de déploiement du CfCT comprend deux étapes principales. Pour obtenir des instructions détaillées, suivez les liens pour chaque étape.

Étape 1. Lancement de la pile

- Lancez le AWS CloudFormation modèle dans votre compte de gestion.
- Passez en revue les paramètres du modèle et ajustez-les si nécessaire.

Étape 2. Création d'un package personnalisé

- Créez un package de configuration personnalisé.

> **Important**
>
> Pour télécharger le AWS CloudFormation modèle approprié et lancer CfCT, suivez le GitHub lien indiqué dans cette section. Ne suivez pas les anciens liens vers des compartiments S3 précédemment spécifiés.

Étape 1. Lancement de la pile

Le AWS CloudFormation modèle de cette section déploie les personnalisations pour AWS Control Tower (CfCT) dans votre compte.

> **Remarque**
>
> Vous êtes responsable du coût des AWS services utilisés pendant que vous utilisez CfCT. Pour en savoir plus, consultez Coût.

1. Pour lancer Customizations for AWS Control Tower, téléchargez le modèle depuis, GitHub puis lancez-le depuis AWS CloudFormation.
2. Le modèle est lancé par défaut dans la région USA Est (Virginie du Nord). Pour lancer CfCT dans une autre AWS région, utilisez le sélecteur de région dans la barre de navigation de la console.

   > **Note**
   >
   > Le CfCT doit être lancé dans la même région et sur le même compte que ceux où vous avez déployé votre zone d'atterrissage AWS Control Tower, à savoir votre région d'origine.

3. Sur la page Créer une pile, vérifiez que l'URL du modèle s'affiche correctement dans la zone de texte URL et choisissez Next.
4. Sur la page Spécifier les détails de la pile, attribuez un nom à votre pile CfCT.
5. Sous Paramètres, passez en revue les paramètres suivants et modifiez-les dans le modèle, si nécessaire.

Configuration du pipeline		
Paramètre	Par défaut	Description
Étape d'approbation du pipeline	No	Choisissez si vous souhaitez modifier la configuration du pipeline de l'étape d'approbation automatique par défaut à une étape d'approbation manuelle. Pour de plus amples informations, veuillez consulter the section called

Configuration du pipeline		
Paramètre	Par défaut	Description
		"Guide de personnalisation du CfCT".
Adresse e-mail d'approbation du pipeline	<Optional Input>	Adresse e-mail pour les notifications d'approbation. Pour utiliser ce paramètre, vous devez définir le paramètre Étape d'approbation du pipeline sur`Yes`.
CodePipelineSource d'AWS	`Amazon S3`	La source d'AWS CodePipeline pour vous aider à sélectionner où stocker et configurer les personnalisations CfCT.
CodeCommit Configuration d'AWS		
Paramètre	Par défaut	Description
CodeCommitRéférentiel existant ?	No	Choisissez si vous souhaitez utiliser un dépôt CodeCommit Git existant. Si vous le souhaitez`Yes`, vous devez définir le paramètre CodePipeline Source sur`AWS CodeCommit` .

CodeCommit Configuration d'AWS		
Paramètre	Par défaut	Description
CodeCommit Nom du référentiel	`custom-control-tower-configuration`	Le nom du dépôt Git. Pour utiliser ce paramètre, vous devez définir le paramètre AWS CodePipeline Source sur`AWS CodeCommit` . Ce nom est utilisé pour créer un nouveau dépôt Git et doit être unique. Si vous fournissez le nom d'un dépôt Git existant, vous devez définir le CodeCommit référentiel existant ? définissez le paramètre sur Oui et entrez le nom exact de ce dépôt.
CodeCommit Nom de la succursale	`main`	Branche Git dans laquelle le package de personnalisation est stocké. Les référentiels Git peuvent comporter de nombreuses branches. Il s'agit du nom par défaut attribué à la branche dans le dépôt Git. Pour utiliser ce paramètre , vous devez définir le paramètre CodePipeline Source sur`AWS CodeCommit` .

CloudFormation StackSets Configuration d'AWS		
Paramètre	Par défaut	Description
Type de simultanéité des régions	`PARALLEL`	Sélectionnez le type de simultanéité des StackSets opérations de déploiement dans les régions. Ce paramètre s'applique à la création, à la mise à jour et à la suppression de flux de travail. L'autre valeur autorisée est`SEQUENTIAL` .
Pourcentage maximal de simultanés	`100`	Pourcentage maximum de comptes dans lequel vous souhaitez effectuer cette opération simultanément. La valeur maximale autorisée est de 100. Pour plus d'informations, reportez-vous à la section Options de fonctionnement du Stack Set.

CloudFormation StackSets Configuration d'AWS		
Paramètre	Par défaut	Description
Pourcentage de tolérance aux défaillances	`10`	Pourcentage de comptes, par région, pour lesquels cette opération de stack peut échouer avant qu'AWS n' CloudFormation arrête l'opération dans cette région. La valeur minimale autorisée est 0 et la valeur maximale autorisée est 100. Pour plus d'informations, reportez-vous à la section Options de fonctionnement du Stack Set.

6. Choisissez Next (Suivant).
7. Sur la page Configurer les options de pile, choisissez Suivant.
8. Sur la page Vérification, vérifiez et confirmez les paramètres. N'oubliez pas de cocher la case indiquant que le modèle va créer les ressources AWS Identity and Access Management (IAM).
9. Sélectionnez Create stack (Créer une pile) pour déployer la pile.

   Vous pouvez consulter l'état de la pile dans la AWS CloudFormation console dans la colonne État. Vous devriez voir le statut CREATE_COMPLETE dans 15 minutes environ.

Étape 2. Création d'un package personnalisé

Avec la pile lancée, vous pouvez personnaliser votre zone d'atterrissage AWS Control Tower et vos politiques de contrôle des services (SCP) en personnalisant le package de configuration inclus. Pour obtenir des instructions détaillées sur la création d'un package personnalisé, reportez-vous auGuide de personnalisation du CfCT.

> **Remarque**
>
> Le pipeline ne s'exécute pas sans le téléchargement du package de configuration personnalisé.

Mettre à jour la pile

Si vous avez déjà déployé des personnalisations pour AWS Control Tower (CfCT), suivez la procédure pour mettre à jour la AWS CloudFormation pile pour la dernière version du framework CfCT.

> **Important**
>
> Avant de pouvoir effectuer la procédure suivante, vous devez télécharger le dernier modèle depuis GitHub un bucket Amazon Simple Storage Service (Amazon S3). Pour savoir comment démarrer avec Amazon S3, consultez Getting started with Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

1. Connectez-vous à la consoleAWS CloudFormation.
2. Sélectionnez vos personnalisations existantes pour la CloudFormation pile AWS Control Tower (CfCT), puis sélectionnez Mettre à jour.
3. Sous Prérequis — Préparer le modèle, sélectionnez Remplacer le modèle actuel.
4. Sous Spécifier le modèle, procédez comme suit :
   a. Pour Source du modèle, sélectionnez Remplacer le modèle actuel.
   b. Pour l'URL Amazon S3, entrez l'URL du modèle que vous avez précédemment chargé sur Amazon S3, puis choisissez Next. GitGub
   c. Vérifiez que l'URL du modèle est correcte. Choisissez ensuite Next et Next à nouveau.
5. Sous Paramètres, passez en revue les paramètres du modèle et modifiez-les si nécessaire. Reportez-vous à l'étape 1. Lancez la pile pour obtenir des informations détaillées sur les paramètres.
6. Choisissez Next (Suivant).
7. Sur la page Configurer les options de pile, choisissez Suivant.

8. Sur la page Vérification, vérifiez et confirmez les paramètres. Assurez-vous de cocher la case indiquant que le modèle est susceptible de créer des ressources AWS Identity and Access Management (IAM).
9. Choisissez Afficher l'ensemble de modifications et vérifiez les modifications.
10. Choisissez Mettre à jour la pile pour déployer la pile.

    Vous pouvez consulter l'état de la pile dans la AWS CloudFormation console dans la colonne État. Vous devriez voir le statut UPDATE_COMPLETE dans 15 minutes environ.

Suppression d'un ensemble de piles

Vous pouvez supprimer un ensemble de piles si vous avez activé la suppression d'un ensemble de piles dans le fichier manifeste. Par défaut, le paramètre `enable_stack_set_deletion` est défini sur `false`. Dans cette configuration, aucune action n'est entreprise pour supprimer l'ensemble de piles associé lorsqu'une ressource est supprimée du fichier manifeste CFct.

Si vous modifiez la valeur de `enable_stack_set_deletion` to `true` dans le fichier manifeste, CFct supprime l'ensemble de piles et toutes ses ressources lorsque vous supprimez une ressource associée du fichier manifeste.

Cette fonctionnalité est prise en charge dans la version 2 du fichier manifeste.

> **Important**
>
> Lorsque vous définissez la valeur de `enable_stack_set_deletion` to pour la première fois`true`, la prochaine fois que vous invoquerez CfCT, TOUTES les ressources qui commencent par le préfixe`CustomControlTower-`, auxquelles est associée la balise `Key:AWS_Solutions, Value: CustomControlTowerStackSet` clé et qui ne sont pas déclarées dans le fichier manifeste sont préparées pour être supprimées.

Voici un exemple de définition de ce paramètre dans un `manifest.yaml` fichier :

```
version: 2021-03-15
region: us-east-1
enable_stack_set_deletion: true   #New opt-in functionality
```

```
resources:
  - name: demo_resource_1
    resource_file: s3://demo_bucket/resource.template
    deployment_targets:
      accounts:
        - 012345678912
    deploy_method: stack_set
    ...
    regions:
    - us-east-1
    - us-west-2

  - name: demo_resource_2
    resource_file: s3://demo_bucket/resource.template
    deployment_targets:
      accounts:
        - 012345678912
    deploy_method: stack_set
    ...
    regions:
    - us-east-1
    - eu-north-1
```

Configurer Amazon S3 comme source de configuration

Lorsque vous configurez des personnalisations pour AWS Control Tower, celui-ci stocke un fichier de configuration initiale, appelé `_custom-control-tower-configuration.zip` fichier, dans un bucket Amazon Simple Storage Service (Amazon S3), nommé. `custom-control-tower-configuration-`*`account-ID`*`-`*`region`*

> **Remarque**
>
> Si vous choisissez de télécharger et de modifier ce fichier, n'oubliez pas de compresser les modifications, de les enregistrer sous un nouveau nom de fichier`custom-control-tower-configuration.zip`, puis de le télécharger à nouveau dans le même compartiment Amazon S3.
>
> Le compartiment Amazon S3 est la source par défaut du pipeline. Lorsque les paramètres par défaut sont en place, le téléchargement d'un fichier zip de configuration sans le préfixe

de soulignement dans le nom du fichier vers le compartiment S3 lancera automatiquement le pipeline.

Le fichier zip est protégé par le chiffrement côté serveur (SSE) avec AWS Key Management Service (AWS KMS) et le refus d'utilisation de la clé KMS. Pour accéder au fichier zip, vous devez mettre à jour la politique des clés KMS afin de spécifier le ou les rôles auxquels l'accès doit être accordé. Le rôle peut être un rôle d'administrateur, un rôle d'utilisateur ou les deux. Suivez cette procédure :

1. Accédez à la consoleAWS Key Management Service.
2. Dans Clés gérées par le client, sélectionnez CustomControlTowerKMSKey.
3. Sélectionnez l'onglet Politique clé. Sélectionnez ensuite Modifier.
4. Sur la page Modifier la politique relative aux clés, recherchez la section Autoriser l'utilisation de la clé dans le code et ajoutez l'une des autorisations suivantes :
   - Pour ajouter un rôle d'administration, procédez comme suit :

     `arn:aws:iam::<account-ID>:role/<administrator-role>`
   - Pour ajouter un utilisateur :

     `arn:aws:iam::<account-ID>:user/<username>`
5. Sélectionnez Save Changes (Enregistrer les modifications).
6. Accédez à la console Amazon S3, recherchez le compartiment S3 contenant le fichier zip de configuration, puis sélectionnez Télécharger.
7. Apportez les modifications de configuration nécessaires au fichier manifeste et aux fichiers modèles. Pour plus d'informations sur la personnalisation des fichiers de manifeste et de modèle, consultezthe section called "Guide de personnalisation du CfCT".
8. Téléchargez vos modifications :
   a. Compressez les fichiers de configuration modifiés et nommez le fichier :`custom-control-tower-configuration.zip`.
   b. Téléchargez le fichier sur Amazon S3 à l'aide de SSE avec la AWS KMS clé principale :. `CustomControlTowerKMSKey`

Collecte de métriques opérationnelles

Les personnalisations pour AWS Control Tower (CfCT) incluent une option permettant d'envoyer des métriques opérationnelles anonymes à. AWS AWS utilise ces données pour comprendre comment les clients utilisent le CfCT, ainsi que d'autres services et produits connexes. Lorsque la collecte de données est activée, les informations suivantes sont envoyées à AWS :

- ID de solution : identifiant de AWS solution
- ID unique (UUID) : identifiant unique généré aléatoirement pour chaque déploiement
- Horodatage : horodatage de la collecte de données
- Nombre d'exécutions de la machine à états : compte de manière incrémentielle le nombre de fois que cette machine à états s'exécute
- Version du manifeste : version du manifeste utilisée dans la configuration

> **Note**
>
> AWS est propriétaire des données qu'il collecte. La collecte de données est soumise à la AWS Politique de confidentialité.

Pour refuser l'envoi de mesures opérationnelles anonymes à AWS, effectuez l'une des tâches suivantes :

- Mettez à jour la section de mappage des AWS CloudFormation modèles comme suit :

  à partir de

```
AnonymousData:
     SendAnonymousData:
        Data: Yes
```

  sur

```
AnonymousData:
     SendAnonymousData:
        Data: No
```

- Une fois CfCT déployé, recherchez la clé du paramètre **`/org/primary/metrics_flag`** SSM dans la console Parameter Store et mettez à jour la valeur en. **`No`**

Guide de personnalisation du CfCT

Le guide Customizations for AWS Control Tower (CfCT) s'adresse aux administrateurs, aux DevOps professionnels, aux éditeurs de logiciels indépendants, aux architectes d'infrastructures informatiques et aux intégrateurs de systèmes qui souhaitent personnaliser et étendre leurs environnements AWS Control Tower pour leur entreprise et leurs clients. Il fournit des informations sur la personnalisation et l'extension de l'environnement AWS Control Tower avec le package de personnalisation CfCT.

> **Note**
>
> Pour déployer et configurer (CfCT), vous devez déployer et traiter un package de configuration via AWS CodePipeline. Les sections suivantes décrivent le processus en détail.

Vue d'ensemble du pipeline de code

Le package de configuration nécessite Amazon Simple Storage Service (Amazon S3 AWS CodePipeline) et. Le package de configuration contient les éléments suivants :

- Un fichier manifeste
- Un ensemble de modèles d'accompagnement
- Autres fichiers JSON pour décrire et implémenter les personnalisations de votre environnement AWS Control Tower

Par défaut, le package `_custom-control-tower-configuration.zip` de configuration est chargé dans un compartiment Amazon S3 avec la convention de dénomination suivante :

`custom-control-tower-configuration-`*`accountID`*`-`*`region`*.

> **Note**
>
> Par défaut, CfCT crée un compartiment Amazon S3 pour stocker la source du pipeline, mais vous pouvez remplacer l'emplacement de la source par un AWS CodeCommit référentiel.

Pour plus d'informations, voir Modifier un pipeline CodePipeline dans le guide de AWS CodePipeline l'utilisateur.

Le fichier manifeste est un fichier texte qui décrit les AWS ressources que vous pouvez déployer pour personnaliser votre zone de landing zone. CodePipeline effectue les tâches suivantes :

- extrait le fichier manifeste, l'ensemble de modèles qui l'accompagne et les autres fichiers JSON
- effectue des validations de manifestes et de modèles
- invoque des sections du fichier manifeste pour exécuter des étapes de pipeline spécifiques.

Lorsque vous mettez à jour le package de configuration en personnalisant le fichier manifeste et en supprimant le trait de soulignement (_) du nom du fichier de configuration, il démarre automatiquement. AWS CodePipeline

> **Note**
>
> Le nom du fichier d'exemple de package de configuration commence par un trait de soulignement (_) afin qu'il ne AWS CodePipeline soit pas automatiquement déclenché. Lorsque vous avez terminé la personnalisation du package de configuration, téléchargez le fichier `custom-control-tower-configuration.zip` sans le trait de soulignement (_) afin de déclencher le déploiement dans AWS CodePipeline.

AWS CodePipeline étapes

Le pipeline CfCT nécessite plusieurs AWS CodePipeline étapes pour implémenter et mettre à jour votre environnement AWS Control Tower.

1. Étape source

   L'étape source est la phase initiale. Votre package de configuration personnalisé lance cette étape du pipeline. La source AWS CodePipeline peut être un compartiment Amazon S3 ou un AWS CodeCommit référentiel dans lequel le package de configuration peut être hébergé.
2. Étape de construction

   La phase de construction nécessite AWS CodeBuild de valider le contenu du package de configuration. Ces vérifications incluent le test de la syntaxe et du schéma du `manifest.yaml`

fichier, ainsi que de tous les AWS CloudFormation modèles inclus dans le package ou hébergés à distance, à l'aide de AWS CloudFormation `validate-template` et`cfn_nag`. Si le fichier manifeste et les AWS CloudFormation modèles réussissent les tests, le pipeline passe à l'étape suivante. Si les tests échouent, vous pouvez consulter les CodeBuild journaux pour identifier le problème et modifier le fichier source de configuration selon vos besoins.

3. Étape d'approbation manuelle (en option)

   L'étape d'approbation manuelle est facultative. Si vous activez cette étape, elle fournit un contrôle supplémentaire sur le pipeline de configuration. Il suspend le pipeline pendant le déploiement, jusqu'à ce qu'une approbation soit donnée. Vous pouvez opter pour l'approbation manuelle en modifiant le paramètre Étape d'approbation du pipeline sur Oui lorsque vous lancez la pile.

4. Étape de la politique de contrôle des services

   L'étape de la politique de contrôle des services appelle la machine d'état des politiques de contrôle des services pour appeler AWS Organizations des API qui créent des politiques de contrôle des services (SCP).

5. Étape CloudFormation des ressources AWS

   L'étape AWS CloudFormation des ressources appelle la machine d'état du stack set pour déployer les ressources spécifiées dans la liste des comptes ou des unités organisationnelles (UO) que vous avez fournie dans le fichier manifeste. La machine d'état crée les AWS CloudFormation ressources dans l'ordre dans lequel elles sont spécifiées dans le fichier manifeste, sauf si une dépendance aux ressources est spécifiée.

Définition d'une configuration personnalisée

Vous allez définir votre configuration AWS Control Tower personnalisée à l'aide du fichier manifeste, de l'ensemble de modèles qui l'accompagne et d'autres fichiers JSON. Vous allez empaqueter ces fichiers dans une structure de dossiers et les placer dans le compartiment Amazon S3 sous forme de `.zip` fichier, comme indiqué dans l'exemple de code suivant.

Structure de dossier de configuration personnalisée

```
- manifest.yaml
- policies/                                                [optional]
   - service control policies files (*.json)
- templates/                                               [optional]
   - template files for AWS CloudFormation Resources (*.template)
```

L'exemple précédent décrit la structure d'un dossier de configuration personnalisé. La structure des dossiers reste la même, que vous choisissiez Amazon S3 ou un AWS CodeCommit référentiel comme emplacement de stockage source. Si vous choisissez Amazon S3 comme stockage source, compressez tous les dossiers et fichiers dans un `custom-control-tower-configuration.zip` fichier et chargez uniquement le `.zip` fichier dans le compartiment Amazon S3 désigné.

> **Note**
>
> Si vous en utilisez AWS CodeCommit, placez les fichiers dans le référentiel sans les compresser.

Le fichier manifeste

Le `manifest.yaml` fichier est un fichier texte qui décrit vos AWS ressources. L'exemple suivant montre la structure du fichier manifeste.

```
---
region: String
version: 2021-03-15

resources:
  #set of CloudFormation resources or SCP policies
...
```

Comme indiqué dans l'exemple de code précédent, les deux premières lignes du fichier manifeste spécifient les valeurs de la région et les mots clés de version. Voici les définitions de ces mots clés.

region — Chaîne de texte pour la région par défaut d'AWS Control Tower. Cette valeur doit être un nom de AWS région valide (tel que `us-east-1`eu-west-1, ou`ap-southeast-1`). La région d'origine d'AWS Control Tower est la région par défaut lorsque vous créez des ressources AWS Control Tower personnalisées (telles qu'AWS CloudFormation StackSets), sauf si une région plus spécifique aux ressources est spécifiée.

```
region:your-home-region
```

version — Numéro de version du schéma du manifeste. La dernière version prise en charge est le 15/03/2021.

```
version: 2021-03-15
```

> **Note**
>
> Nous vous recommandons vivement d'utiliser la dernière version. Pour mettre à jour les propriétés du manifeste dans la dernière version, reportez-vous àMises à niveau de la version.

Le mot clé suivant présenté dans l'exemple précédent est le mot clé resources. La section des ressources du fichier manifeste est hautement structurée. Il contient une liste détaillée des AWS ressources, qui seront déployées automatiquement par le pipeline CfCT. Ces descriptions des ressources et de leurs paramètres disponibles sont données dans la section suivante.

La section des ressources du fichier manifeste

Cette rubrique décrit la section des ressources du fichier manifeste, dans laquelle vous allez définir les ressources requises pour vos personnalisations. Cette section du fichier manifeste commence dans les ressources de mots clés et se poursuit jusqu'à la fin du fichier.

La section des ressources du fichier manifeste spécifie les AWS CloudFormation StackSets ou les AWS Organizations SCP, que CfCT déploie automatiquement via le pipeline de code. Vous pouvez répertorier les unités d'organisation, les comptes et les régions pour déployer des instances de stack.

Les instances Stack sont déployées au niveau du compte plutôt qu'au niveau de l'unité d'organisation. Les SCP sont déployés au niveau de l'UO. Pour plus d'informations, voir Création de vos propres personnalisations.

L'exemple de modèle suivant décrit les entrées possibles disponibles pour la section des ressources du fichier manifeste.

```
resources: # List of resources
  - name: [String]
    resource_file: [String] [Local File Path, S3 URI, S3 URL]
    deployment_targets: # account and/or organizational unit names
      accounts: # array of strings, [0-9]{12}
        - 012345678912
        - AccountName1
      organizational_units: #array of strings
```

```
        - OuName1
        - OuName2
    deploy_method: scp | stack_set
    parameters: # List of parameters [SSM, Alfred, Values]
      - parameter_key: [String]
        parameter_value: [String]
    export_outputs: # list of ssm parameters to store output values
      - name: /org/member/test-ssm/app-id
        value: $[output_ApplicationId]
    regions: #list of strings
    - [String]
```

Le reste de cette rubrique fournit des définitions détaillées pour les mots clés présentés dans l'exemple de code précédent.

name — Le nom associé au AWS CloudFormation StackSets. La chaîne que vous fournissez attribue un nom plus convivial à un ensemble de piles.

- Type : chaîne
- Obligatoire : oui
- Valeurs valides : a-z, A-Z, 0-9 et un trait de soulignement (_). Tout autre caractère est automatiquement remplacé par un trait de soulignement (_).

description — Description de la ressource.

- Type : chaîne
- Obligatoire : non

resource_file — Ce fichier peut être spécifié comme l'emplacement relatif du fichier manifeste, une URI ou une URL Amazon S3 pointant vers un AWS CloudFormation modèle ou une politique de contrôle des AWS Organizations services en JSON pour la création de AWS CloudFormation ressources ou de SCP.

- Type : chaîne
- Obligatoire : oui

1. L'exemple suivant montre le`resource_file`, donné comme emplacement relatif du fichier de ressources dans le package de configuration.

```
resources:
  - name: SecurityRoles
    resource_file: templates/custom-security.template
```

2. L'exemple suivant montre le fichier de ressources fourni sous forme d'URI Amazon S3

```
resources:
  - name: SecurityRoles
    resource_file: s3://bucket-name/[key-name]
```

3. L'exemple suivant montre le fichier de ressources fourni sous forme d'URL HTTPS Amazon S3

```
resources:
  - name: SecurityRoles
    resource_file: https://bucket-name.s3.Region.amazonaws.com/key-name
```

> **Note**
>
> Si vous fournissez une URL Amazon S3, vérifiez que la politique du compartiment autorise l'accès en lecture au compte de gestion AWS Control Tower à partir duquel vous déployez CfCT. Si vous fournissez une URL HTTPS Amazon S3, vérifiez que le chemin utilise la notation par points. Par exemple, `S3.us-west-1`. CfCT ne prend pas en charge les points de terminaison contenant un tiret entre S3 et la région, tels que. `S3-us-west-2`

4. L'exemple suivant montre une politique de compartiment Amazon S3 et un ARN dans lequel les ressources sont stockées.

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::AccountId:root"},
        "Action": "s3:GetObject",
        "Resource": "arn:aws:s3:::my-bucket/*”
       }
   ]
}
```

Vous allez remplacer la *AccountId*variable illustrée dans l'exemple par l'ID de AWS compte du compte de gestion qui déploie CfCT. Pour plus d'exemples, reportez-vous aux exemples de politiques relatives aux compartiments dans le guide de l'utilisateur d'Amazon Simple Storage Service.

paramètres — Spécifie le nom et la valeur des AWS CloudFormation paramètres.

- Type : MapList
- Obligatoire : non

La section des paramètres contient des paires de paramètres clé/valeur. Le pseudo-modèle suivant décrit la section des paramètres.

```
parameters:
  - parameter_key: [String]
    parameter_value: [String]
```

- parameter_key — La clé associée au paramètre.
  - Type : chaîne
  - Obligatoire : Oui (sous la propriété des paramètres)
  - Valeurs valides : a-z, A-Z et 0-9
- parameter_value — La valeur d'entrée associée au paramètre.
  - Type : chaîne
  - Obligatoire : Oui (sous la propriété des paramètres)

deploy_method — Méthode de déploiement pour déployer des ressources dans le compte. Actuellement, deploy_method prend en charge le déploiement de ressources à l'aide de l'`stack_set`option de déploiement des ressources via AWS CloudFormation StackSets, ou de l'`scp`option si vous déployez des SCP.

- Type : chaîne
- Valeurs valides : `stack_set` | `scp`
- Obligatoire : oui

deployment_targets — Liste des comptes ou des unités organisationnelles (UO) dans lesquels CfCT déploiera les AWS CloudFormation ressources, spécifiées sous forme de comptes ou d'unité_organisations.

> **Note**
>
> Si vous souhaitez déployer un SCP, la cible doit être une unité d'organisation et non un compte.

- Type : liste de chaînes `account name` ou `account number` pour indiquer que cette ressource sera déployée dans la liste de comptes donnée, ou `0U names` pour indiquer que cette ressource sera déployée dans la liste d'unités d'organisation donnée.
- Obligatoire : au moins un des comptes ou unité_organisations
  - comptes :

    Type : liste de chaînes `account name` ou `account number` pour indiquer que cette ressource sera déployée dans la liste de comptes donnée.
  - unités_organisationnelles :

    Type : liste de chaînes `0U names` indiquant que cette ressource sera déployée dans une liste d'unités d'organisation donnée. Si vous fournissez une UO qui ne contient pas de comptes et que la propriété accounts n'est pas ajoutée, CFct crée uniquement le stack set.

    > **Note**
    >
    > L'ID du compte de gestion de l'organisation n'est pas une valeur autorisée. CfCT ne prend pas en charge le déploiement d'instances de stack dans le compte de gestion de l'organisation.

export_outputs — Liste des paires nom/valeur qui indiquent les clés de paramètres SSM. Ces clés de paramètres SSM vous permettent de stocker les sorties du modèle dans le magasin de paramètres SSM. La sortie est destinée à être consultée par d'autres ressources, définies précédemment dans le fichier manifeste.

```
export_outputs: # List of SSM parameters
  - name: [String]
```

```
    value: [String]
```

- Type : Liste des paires de clés de nom et de valeur. Le nom contient la `name` chaîne d'une clé de magasin de paramètres SSM et la valeur contient la `value` chaîne du paramètre.
- Valeurs valides : Toute chaîne ou `$[output_`*`CfnOutput-Logical-ID`*`]` variable où *`CfnOutput-logical-ID`* correspond à la variable de sortie du modèle. Pour plus d'informations sur la section Sorties d'un AWS CloudFormation modèle, voir Sorties dans le guide de AWS CloudFormation l'utilisateur.
- Obligatoire : non

Par exemple, l'extrait de code suivant stocke la variable de `VPCID` sortie du modèle dans la clé de paramètre SSM nommée. `/org/member/audit/vpc_id`

```
export_outputs: # List of SSM parameters
  - name: /org/member/audit/VPC-ID
    value: $[output_VPCID]
```

> **Note**
>
> Le nom de la clé export_outputs peut contenir une valeur autre que. `output` Par exemple, si le nom est`/org/environment-name`, la valeur peut être`production`.

régions — Liste des régions dans lesquelles CfCT déploiera les instances de AWS CloudFormation stack.

- Type : Toute liste de noms de régions AWS commerciales, pour indiquer que cette ressource sera déployée dans la liste de régions donnée. Si ce mot clé n'existe pas dans le fichier manifeste, les ressources sont déployées uniquement dans la région d'origine.
- Obligatoire : non

Root OU

CfCT prend en charge Root en tant que valeur pour une unité organisationnelle (UO) `organizational_units` dans la version V2 du manifeste (2021-03-15).

- Si vous choisissez la méthode de `scp` déploiement suivante : lorsque vous ajoutez Root under`organizational_units`, AWS Control Tower applique les politiques à toutes les UO situées sous Root. Si vous choisissez la méthode de déploiement`stack_set`, lorsque vous ajoutez Root sous`organizational_units`, CfCT déploie les stack sets dans tous les comptes sous Root inscrits dans AWS Control Tower, à l'exception du compte de gestion.
- Conformément aux bonnes pratiques d'AWS Control Tower, le compte de gestion est uniquement destiné à gérer les comptes des membres et à des fins de facturation. N'exécutez pas de charges de travail de production dans le compte de gestion AWS Control Tower.

  Conformément aux directives relatives aux meilleures pratiques, le déploiement d'AWS Control Tower place le compte de gestion sous l'unité d'organisation racine, afin qu'il dispose d'un accès complet et ne fasse pas appel à des ressources supplémentaires. Pour cette raison, le AWSControlTowerExecutionrôle n'est pas déployé sur le compte de gestion.
- Nous vous recommandons de suivre ces bonnes pratiques pour le compte de gestion. Si vous avez un cas d'utilisation spécifique qui vous oblige à déployer des stacksets dans le compte de gestion, incluez les comptes comme cible de déploiement et spécifiez le compte de gestion. Dans le cas contraire, n'incluez pas les comptes comme cible de déploiement. Vous devez créer les ressources manquantes, y compris les rôles IAM requis, dans le compte de gestion.

Pour déployer des stacksets dans le compte de gestion, incluez-les `accounts` comme cible de déploiement et spécifiez le compte de gestion. Dans le cas contraire, n'incluez pas les comptes comme cible de déploiement.

```
---
region: your-home-region
version: 2021-03-15

resources:

  …truncated…

    deployment_targets:
      organizational_units:
        - Root
```

> **Note**
>
> La fonctionnalité Root OU n'est prise en charge que dans la version V2 du fichier manifeste (2021-03-15). Si vous ajoutez Root en tant qu'unité d'organisation sous`organizational_units`, n'ajoutez aucune autre unité d'organisation.

UO imbriquée

CfCT prend en charge la liste d'une ou plusieurs unités d'organisation imbriquées sous le `organizational_units` mot clé dans la version V2 du manifeste (15/03/2021).

Un chemin complet (à l'exception de la racine) pour l'unité d'organisation imbriquée est requis, en utilisant deux points comme séparateur entre les unités d'organisation. Pour la méthode de déploiement`scp`, AWS Control Tower déploie les SCP vers la dernière unité organisationnelle du chemin d'unité d'organisation imbriqué. Pour ce qui est de la méthode de déploiement`stack_set`, AWS Control Tower déploie les ensembles de piles sur tous les comptes situés sous la dernière unité organisationnelle du chemin d'unité d'organisation imbriqué.

Par exemple, considérez le chemin`OUName1:OUName2:OUName3`. La dernière unité d'organisation du chemin est`OUName3`. CfCT déploie les SCP `OUName3` et les ensembles de piles sur tous les comptes situés directement sous`OUName3`, uniquement.

```
---
region: your-home-region
version: 2021-03-15

resources:

  …truncated…

    deployment_targets:
      organizational_units:
        - OuName1:OUName2:OUName3
```

> **Note**
>
> La fonctionnalité d'unité d'organisation imbriquée n'est prise en charge que dans la version V2 du fichier manifeste (15/03/2021).

Créez vos propres personnalisations

Pour créer vos propres personnalisations, vous pouvez modifier le `manifest.yaml` fichier en ajoutant ou en mettant à jour des politiques et AWS CloudFormation des ressources de contrôle des services (SCP). Pour les ressources qui doivent être déployées, vous pouvez ajouter ou supprimer des comptes et des unités d'organisation. Vous pouvez ajouter ou modifier les modèles dans les dossiers du package, créer vos propres dossiers et référencer les modèles ou les dossiers du `manifest.yaml` fichier.

Cette section explique les deux principales étapes de la création de vos propres personnalisations :

- comment configurer votre propre package de configuration pour les politiques de contrôle des services
- comment configurer votre propre package de configuration pour les ensembles de AWS CloudFormation piles

Configurer un package de configuration pour les politiques de contrôle des services

Cette section explique comment créer un package de configuration pour les politiques de contrôle des services (SCP). Les deux parties principales de ce processus sont (1) la préparation du fichier manifeste et (2) la préparation de la structure de dossiers.

Étape 1 : Modifier le fichier manifest.yaml

Utilisez le `manifest.yaml` fichier d'exemple comme point de départ. Entrez toutes les configurations nécessaires. Ajoutez les `deployment_targets` détails `resource_file` et.

L'extrait suivant montre le fichier manifeste par défaut.

```
---
region: us-east-1
version: 2021-03-15

resources: []
```

La valeur pour `region` est ajoutée automatiquement lors du déploiement. Il doit correspondre à la région dans laquelle vous avez déployé CfCT. Cette région doit être identique à la région AWS Control Tower.

Pour ajouter un SCP personnalisé dans le `example-configuration` dossier du package zip stocké dans le compartiment Amazon S3, ouvrez le `example-manifest.yaml` fichier et commencez à le modifier.

```
---
region: your-home-region
version: 2021-03-15

resources:
  - name: test-preventive-controls
    description: To prevent from deleting or disabling resources in member accounts
    resource_file: policies/preventive-controls.json
    deploy_method: scp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - OUName1
        - OUName2

…truncated…
```

L'extrait suivant montre un exemple de fichier manifeste personnalisé. Vous pouvez ajouter plusieurs politiques lors d'une seule modification.

```
---
region: us-east-1
version: 2021-03-15

resources:
  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - OUName1
        - OUName2
```

Étape 2 : Création d'une structure de dossiers

Vous pouvez ignorer cette étape si vous utilisez une URL Amazon S3 pour le fichier de ressources et si vous utilisez des paramètres avec des paires clé/valeur.

Vous devez inclure une politique SCP au format JSON pour prendre en charge le manifeste, car le fichier manifeste fait référence au fichier JSON. Assurez-vous que les chemins des fichiers correspondent aux informations de chemin fournies dans le fichier manifeste.

- Un fichier JSON de politique contient les SCP à déployer sur les unités d'organisation.

L'extrait suivant montre la structure des dossiers de l'exemple de fichier manifeste.

```
- manifest.yaml
- policies/
   - block-s3-public.json
```

L'extrait de code suivant est un exemple de fichier de régulation`block-s3-public.json`.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"GuardPutAccountPublicAccessBlock",
         "Effect":"Deny",
         "Action":"s3:PutAccountPublicAccessBlock",
         "Resource":"arn:aws:s3:::*"
      }
   ]
}
```

Configurez un package de configuration pour AWS CloudFormation StackSets

Cette section explique comment configurer un package de configuration pour AWS CloudFormation StackSets. Les deux parties principales de ce processus sont les suivantes : (1) préparer le fichier manifeste et (2) mettre à jour la structure des dossiers.

Étape 1 : modifier le fichier manifeste existant

Ajoutez les nouvelles AWS CloudFormation StackSets informations au fichier manifeste que vous avez modifié précédemment.

Juste pour examen, l'extrait suivant contient le même fichier manifeste personnalisé que celui affiché précédemment pour configurer un package de configuration pour les SCP. Vous pouvez maintenant modifier davantage ce fichier pour inclure les détails de vos ressources.

```
---
region: us-east-1
version: 2021-03-15

resources:

  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp
    #Apply to the following OU(s)
    deployment_targets:
    organizational_units: #array of strings
    - OUName1
    - OUName2
```

L'extrait suivant montre un exemple de fichier manifeste modifié qui contient les `resources` détails. L'ordre de `resources` détermine l'ordre d'exécution pour créer des `resources` dépendances. Vous pouvez modifier l'exemple de fichier manifeste suivant en fonction des besoins de votre entreprise.

```
---
region: your-home-region
version: 2021-03-15

…truncated…

resources:
  - name: stackset-1
    resource_file: templates/create-ssm-parameter-keys-1.template
    parameters:
      - parameter_key: parameter-1
        parameter_value: value-1
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - account number or account name
        - 123456789123
      organizational_units: #array of strings, ou ids, ou-xxxx
```

```
        - OuName1
        - OUName2
    export_outputs:
      - name: /org/member/test-ssm/app-id
        value: $[output_ApplicationId]
    regions:
      - region-name

  - name: stackset-2
    resource_file: s3://bucket-name/key-name
    parameters:
      - parameter_key: parameter-1
        parameter_value: value-1
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - account number or account name
        - 123456789123
      organizational_units: #array of strings
        - OuName1
        - OUName2
regions:
  - region-name
```

L'exemple suivant montre que vous pouvez ajouter plusieurs AWS CloudFormation ressources dans le fichier manifeste.

```
---
region: us-east-1
version: 2021-03-15

resources:
  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - Custom
        - Sandbox

  - name: transit-network
```

```
    resource_file: templates/transit-gateway.template
    parameter_file: parameters/transit-gateway.json
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - Prod
        - 123456789123 #Network
      organizational_units: #array of strings
        - Custom
    export_outputs:
      - name: /org/network/transit-gateway-id
        value: $[output_TransitGatewayID]
    regions:
      - us-east-1
```

Étape 2 : mise à jour de la structure des dossiers

Lorsque vous mettez à jour la structure des dossiers, vous pouvez inclure tous les fichiers AWS CloudFormation modèles de support et les fichiers de politique SCP présents dans le fichier manifeste. Vérifiez que les chemins des fichiers correspondent à ceux fournis dans le fichier manifeste.

- Un fichier modèle contient les AWS ressources à déployer dans les unités d'organisation et les comptes.
- Un fichier de régulation contient les paramètres d'entrée utilisés dans le fichier modèle.

L'exemple suivant montre la structure de dossiers de l'exemple de fichier manifeste créé à l'étape 1.

```
- manifest.yaml
- policies/
   - block-s3-public.json
- templates/
   - transit-gateway.template
```

L'assistant « alfred » et les fichiers de AWS CloudFormation paramètres

CfCT vous fournit un mécanisme connu sous le nom d'assistant Alfred pour obtenir la valeur d'une clé de magasin de paramètres SSM définie dans le modèle. AWS CloudFormation À l'aide de l'assistant Alfred, vous pouvez utiliser des valeurs stockées dans le magasin de paramètres SSM

sans mettre à jour le AWS CloudFormation modèle. Pour plus d'informations, voir Qu'est-ce qu'un AWS CloudFormation modèle ? dans le guide de AWS CloudFormation l'utilisateur.

> **Important**
>
> L'assistant Alfred a deux limites. Les paramètres ne sont disponibles que dans la région d'origine du compte de gestion AWS Control Tower. Il est recommandé d'envisager de travailler avec des valeurs qui ne changent pas d'une instance de pile à l'autre. Lorsque l'assistant « alfred » récupère les paramètres, il choisit une instance de pile aléatoire dans l'ensemble de piles qui exporte la variable.

Exemple

Supposons que vous disposiez de deux ensembles de AWS CloudFormation piles. Le Stack set 1 possède une instance de stack et se déploie sur un compte dans une région. Il crée un Amazon VPC et des sous-réseaux dans une zone de disponibilité, et le `VPC ID` et `subnet ID` doit être transmis au stack set 2 sous forme de valeurs de paramètres. Avant que le `VPC ID` et `subnet ID` puisse être transmis à l'ensemble de piles 2, le `VPC ID` et `subnet ID` doit être stocké dans le jeu de piles 1 à l'aide de`AWS:::SSM::Parameter`. Pour plus d'informations, consultez `AWS:::SSM::Parameter` dans le Guide de l'utilisateur AWS CloudFormation .

AWS CloudFormation set de piles 1 :

Dans l'extrait suivant, l'assistant Alfred peut obtenir des valeurs pour et à `subnet ID` partir du magasin de paramètres `VPC ID` et les transmettre en entrée à la StackSet machine à états.

```
VpcIdParameter:
    Type: AWS::SSM::Parameter
    Properties:
      Name: '/stack_1/vpc/id'
      Description: Contains the VPC id
      Type: String
      Value: !Ref MyVpc

SubnetIdParameter:
    Type: AWS::SSM::Parameter
    Properties:
      Name: '/stack_1/subnet/id'
      Description: Contains the subnet id
```

```
      Type: String
      Value: !Ref MySubnet
```

AWS CloudFormation set de 2 piles :

L'extrait montre les paramètres spécifiés dans le fichier de AWS CloudFormation pile 2. `manifest.yaml`

```
parameters:
      - parameter_key: VpcId
        parameter_value: $[alfred_ssm_/stack_1/vpc/id]
      - parameter_key: SubnetId
        parameter_value: $[alfred_ssm_/stack_1/subnet/id]
```

AWS CloudFormation Stack Set 2.1 :

L'extrait montre que vous pouvez répertorier les `alfred_ssm` propriétés pour prendre en charge les paramètres de type. CommaDelimitedList Pour plus d'informations, consultez `Parameters` dans le Guide de l'utilisateur AWS CloudFormation .

```
parameters:
      - parameter_key: VpcId # Type: String
        parameter_value: $[alfred_ssm_/stack_1/vpc/id']
      - parameter_key: SubnetId # Type: String
        parameter_value: $[ alfred_ssm_/stack_1/subnet/id']
      - parameter_key: AvailablityZones # Type: CommaDelimitedList
        parameter_value:
  - "$[alfred_ssm_/availability_zone_1]"
 - "$[alfred_ssm_/availability_zone_2]"
```

Schéma JSON pour le package de personnalisation

Le schéma JSON du package de personnalisation pour CfCT se trouve dans le référentiel de code source sur GitHub. Vous pouvez utiliser le schéma avec bon nombre de vos outils de développement préférés, et il peut vous être utile pour réduire les erreurs lorsque vous créez votre propre `manifest.yaml` fichier.

Mises à niveau de la version

Pour plus d'informations sur la dernière version de Customizations for AWS Control Tower (CfCT), consultez le fichier ChangeLog.md dans le référentiel. GitHub

> **Warning**
>
> La version 2.2.0 de Customizations for AWS Control Tower (CfCT) a introduit un schéma de manifeste (version 2021-03-15) pour s'aligner sur les API de service associées. AWS Le schéma du manifeste permet à un seul fichier manifest.yaml de gérer les ressources prises en charge (AWS CloudFormation modèles et SCP) via des flux de travail découplés. DevOps Nous vous recommandons vivement de mettre à jour le schéma du manifeste de la version 2020-01-01 à la version 2021-03-15 ou ultérieure.
> CfCT continue de prendre en charge les versions 2021-03-15 et 2020-01-01 du fichier. `manifest.yaml` Aucune modification de votre configuration existante n'est requise. Cependant, la version 2020-01-01 est en fin de support. Nous ne fournissons plus de mises à jour ni n'ajoutons d'améliorations à la version 2020-01-01. Les fonctionnalités de l'unité d'organisation racine et de l'unité d'organisation imbriquée ne sont pas prises en charge dans la version 2020-01-01.

Propriétés obsolètes dans la version du manifeste 2021-03-15 :

```
organization_policies
policy_file
apply_to_accounts_in_ou

cloudformation_resources
template_file
deploy_to_account
deploy_to_ou
ssm_parameters
```

Étapes de mise à niveau obligatoires

Lorsque vous effectuez une mise à niveau vers la version du schéma du manifeste 15/03/2021, voici les modifications que vous devez apporter pour mettre à jour vos fichiers. Les sections suivantes décrivent les modifications obligatoires et recommandées pour la transition.

Politiques des organisations

1. Déplacez les SCP sous organization_policies sous les nouvelles ressources de propriété.
2. Remplacez la propriété policy_file par la nouvelle propriété resource_file.
3. Remplacez apply_to_accounts_in_ou par la nouvelle propriété deployment_targets. La liste des unités d'organisation doit être définie sous la sous-propriété organizational_units. La sous-propriété accounts n'est pas prise en charge pour les politiques des organisations.
4. Ajoutez une nouvelle propriété deploy_method avec la valeur scp.

AWS CloudFormation ressources

1. Déplacez les CloudFormation ressources sous cloudformation_resources sous les nouvelles ressources de propriété.
2. Remplacez la propriété template_file par la nouvelle propriété resource_file.
3. Remplacez le deploy_to_ou par la nouvelle propriété deployment_targets. La liste des unités d'organisation doit être définie sous la sous-propriété organizational_units.
4. Remplacez le paramètre deploy_to_accounts par la nouvelle propriété deployment_targets. La liste des comptes doit être définie sous les comptes de sous-propriétés.
5. Remplacez la propriété ssm_parameters par la nouvelle propriété export_outputs.

Étapes de mise à niveau hautement recommandées

AWS CloudFormation paramètres

1. Remplacez la propriété parameter_file par de nouveaux paramètres de propriété.
2. Supprimez le chemin du fichier dans la valeur de la propriété parameter_file.
3. Copiez la clé et la valeur du paramètre à partir du fichier JSON de paramètre existant dans le nouveau format de la propriété des paramètres. Cela vous aidera à les gérer dans le fichier manifeste.

> **Note**
>
> La propriété parameter_file est prise en charge dans la version du manifeste 2021-03-15.

Mise en réseau dans AWS Control Tower

AWS Control Tower fournit un support de base pour la mise en réseau via des VPC.

Si la configuration ou les fonctionnalités par défaut du VPC AWS Control Tower ne répondent pas à vos besoins, vous pouvez utiliser d'autres AWS services pour configurer votre VPC. Pour plus d'informations sur l'utilisation des VPC et d'AWS Control Tower, consultez la section Création d'une infrastructure réseau multi-VPC AWS évolutive et sécurisée.

Rubriques en relation

- Pour plus d'informations sur le fonctionnement d'AWS Control Tower lorsque vous inscrivez des comptes dotés de VPC existants, consultez. Inscription de comptes existants auprès de VPC
- Avec Account Factory, vous pouvez provisionner des comptes qui incluent un VPC AWS Control Tower, ou vous pouvez provisionner des comptes sans VPC. Pour plus d'informations sur la façon de supprimer le VPC AWS Control Tower ou de configurer des comptes AWS Control Tower sans VPC, consultez. Procédure pas à pas : configurer AWS Control Tower sans VPC
- Pour plus d'informations sur la modification des paramètres de compte pour les VPC, consultez la documentation d'Account Factory sur la mise à jour d'un compte.
- Pour plus d'informations sur l'utilisation du réseau et des VPC dans AWS Control Tower, consultez la section relative à la mise en réseau sur la page d'informations connexes de ce guide de l'utilisateur.

VPC et AWS régions dans AWS Control Tower

Lors de la création d'un compte, un VPC AWS par défaut est AWS créé dans chaque région, même dans les régions que vous ne gérez pas avec AWS Control Tower. Ce VPC par défaut n'est pas le même qu'un VPC créé par AWS Control Tower pour un compte provisionné, mais le AWS VPC par défaut dans une région non gouvernée peut être accessible aux utilisateurs IAM.

Les administrateurs peuvent activer le refus de contrôle par région, afin que vos utilisateurs finaux ne soient pas autorisés à se connecter à un VPC dans une région prise en charge par AWS Control Tower mais en dehors de vos régions gouvernées. Pour configurer le refus de contrôle par région, rendez-vous sur la page des paramètres de la zone d'atterrissage et sélectionnez Modifier les paramètres.

Le refus de contrôle de la région bloque les appels d'API vers la plupart des services non gouvernés Régions AWS. Pour plus d'informations, consultez la section Refuser l'accès AWS en fonction de la demande Région AWS. .

> **Note**
>
> Le refus de contrôle de la région peut ne pas empêcher les utilisateurs IAM de se connecter à un VPC AWS par défaut dans une région où AWS Control Tower n'est pas pris en charge.

Vous pouvez éventuellement supprimer les VPC AWS par défaut dans les régions non gouvernées. Pour répertorier le VPC par défaut dans une région, vous pouvez utiliser une commande CLI similaire à cet exemple :

```
aws ec2 --region us-west-1 describe-vpcs --filter Name=isDefault,Values=true
```

Présentation d'AWS Control Tower et des VPC

Voici quelques informations essentielles concernant les VPC AWS Control Tower :

- Le VPC créé par AWS Control Tower lorsque vous configurez un compte dans Account Factory n'est pas le même que le AWS VPC par défaut.
- Lorsqu'AWS Control Tower crée un nouveau compte dans une AWS région prise en charge, AWS Control Tower supprime automatiquement le AWS VPC par défaut et configure un nouveau VPC configuré par AWS Control Tower.
- Chaque compte AWS Control Tower est autorisé à disposer d'un VPC créé par AWS Control Tower. Un compte peut avoir des AWS VPC supplémentaires dans les limites du compte.
- Chaque VPC AWS Control Tower possède trois zones de disponibilité dans toutes les régions, à l'exception de la région de l'ouest des États-Unis (Californie du Nord)`us-west-1`, et deux zones de disponibilité dans. `us-west-1` Par défaut, chaque zone de disponibilité se voit attribuer un sous-réseau public et deux sous-réseaux privés. Par conséquent, dans les régions à l'exception de l'ouest des États-Unis (Californie du Nord), chaque VPC AWS Control Tower contient neuf sous-réseaux par défaut, répartis sur trois zones de disponibilité. Dans l'ouest des États-Unis (Californie du Nord), six sous-réseaux sont répartis sur deux zones de disponibilité.
- Chacun des sous-réseaux de votre VPC AWS Control Tower se voit attribuer une plage unique, de taille égale.

- Le nombre de sous-réseaux dans un VPC est configurable. Pour plus d'informations sur la modification de la configuration de votre sous-réseau VPC, consultez la rubrique Account Factory.
- Comme les adresses IP ne se chevauchent pas, les six ou neuf sous-réseaux de votre VPC AWS Control Tower peuvent communiquer entre eux sans restriction.

Lorsque vous travaillez avec des VPC, AWS Control Tower ne fait aucune distinction au niveau de la région. Chaque sous-réseau est alloué à partir de la plage d'adresses CIDR exacte que vous spécifiez. Les sous-réseaux VPC peuvent exister dans n'importe quelle région.

Remarques

> **Gérez les coûts des VPC**
>
> Si vous configurez le VPC Account Factory de telle sorte que les sous-réseaux publics soient activés lors de l'approvisionnement d'un nouveau compte, Account Factory configure le VPC pour créer une passerelle NAT. Vous serez facturé pour votre utilisation par Amazon VPC.

> **VPC et paramètres de contrôle**
>
> Si vous configurez des comptes Account Factory avec les paramètres d'accès Internet VPC activés, ce paramètre annule le contrôle Interdire l'accès à Internet pour une instance Amazon VPC gérée par un client. Pour éviter d'activer l'accès à Internet pour les comptes nouvellement provisionnés, vous devez modifier le paramètre dans Account Factory. Pour plus d'informations, consultez Procédure pas à pas : configurer AWS Control Tower sans VPC.

CIDR et peering pour VPC et AWS Control Tower

Cette section est destinée principalement aux administrateurs réseau. L'administrateur réseau de votre entreprise est généralement la personne qui sélectionne la plage d'adresses CIDR globale pour votre organisation AWS Control Tower. L'administrateur réseau alloue ensuite des sous-réseaux à partir de cette plage à des fins spécifiques.

Lorsque vous choisissez une plage d'adresses CIDR pour votre VPC, AWS Control Tower valide les plages d'adresses IP conformément à la spécification RFC 1918. Account Factory autorise un bloc CIDR allant jusqu'/16à une valeur comprise entre :

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16
- 100.64.0.0/10(uniquement si votre fournisseur d'accès Internet autorise l'utilisation de cette plage)

Le délimiteur /16 permet jusqu'à 65 536 adresses IP distinctes.

Vous pouvez attribuer des adresses IP valides à partir des plages suivantes :

- 10.0.x.x to 10.255.x.x
- 172.16.x.x – 172.31.x.x
- 192.168.0.0 – 192.168.255.255 (pas d'IP en dehors de la plage 192.168)

Si la plage que vous spécifiez se situe en dehors de ces valeurs, AWS Control Tower affiche un message d'erreur.

La plage d'adresses CIDR par défaut est 172.31.0.0/16.

Lorsqu'AWS Control Tower crée un VPC à l'aide de la plage d'adresses CIDR que vous sélectionnez, elle attribue la même plage d'adresses CIDR à chaque VPC pour chaque compte que vous créez au sein de l'unité organisationnelle (UO). En raison du chevauchement par défaut des adresses IP, cette implémentation n'autorise initialement pas le peering entre vos VPC AWS Control Tower au sein de l'unité d'organisation.

Sous-réseaux

Au sein de chaque VPC, AWS Control Tower divise la plage de CIDR spécifiée de manière égale en neuf sous-réseaux (sauf dans l'ouest des États-Unis (Californie du Nord), où elle est de six sous-réseaux). Aucun des sous-réseaux au sein d'un VPC ne se chevauche. Ils peuvent donc tous communiquer entre eux, au sein du VPC.

En résumé, par défaut, les communications de sous-réseau au sein du VPC ne sont pas restreintes. La bonne pratique pour contrôler la communication entre vos sous-réseaux VPC, si nécessaire, consiste à configurer les listes de contrôle d'accès avec des règles qui définissent le flux de trafic autorisé. Utilisez des groupes de sécurité pour contrôler le trafic entre des instances spécifiques. Pour plus d'informations sur la configuration des groupes de sécurité et des pare-feux dans AWS

Control Tower, consultez la section Procédure pas à pas : configurer des groupes de sécurité dans AWS Control Tower With AWS Firewall Manager.

Appairage

AWS Control Tower ne limite pas le peering VPC à VPC pour les communications entre plusieurs VPC. Cependant, par défaut, tous les VPC AWS Control Tower ont la même plage d'adresses CIDR par défaut. Pour prendre en charge le peering, vous pouvez modifier la plage CIDR dans les paramètres d'Account Factory afin que les adresses IP ne se chevauchent pas.

Si vous modifiez la plage d'adresses CIDR dans les paramètres d'Account Factory, la nouvelle plage d'adresses CIDR est attribuée à tous les nouveaux comptes créés ultérieurement par AWS Control Tower (à l'aide de Account Factory). Les anciens comptes ne sont pas mis à jour. Par exemple, vous pouvez créer un compte, modifier la plage d'adresses CIDR et créer un nouveau compte, et les VPC alloués à ces deux comptes peuvent être appairés. L'appairage est possible, car leurs plages d'adresses IP ne sont pas identiques.

Rôles et autorisations requis

AWS Control Tower utilise les rôles IAM pour gérer l'accès aux ressources.

Pour des informations générales sur les rôles, voir Groupes d'utilisateurs, rôles et ensembles d'autorisations.

À propos des autorisations

- Pour plus d'informations sur les groupes IAM et leurs autorisations dans AWS Control Tower, consultez la section Groupes IAM Identity Center pour AWS Control Tower.
- Pour plus d'informations sur les autorisations requises pour approvisionner des comptes, consultez la section Autorisations requises pour les comptes.
- Pour plus d'informations sur les autorisations de console requises pour AWS Control Tower, consultez Autorisations requises pour utiliser la console AWS Control Tower.

À propos des rôles

- Pour plus d'informations sur la création d'un rôle, y compris les autorisations conçues pour l'accès programmatique, consultez les sections Création de rôles et attribution d'autorisations, et Rôles programmatiques et relations de confiance pour le compte d'audit AWS Control Tower.
- Pour plus d'informations sur les autres rôles utilisés par AWS Control Tower pour gérer vos comptes, consultez les sections Utilisation de politiques basées sur l'identité (politiques IAM) pour AWS Control Tower et politiques gérées pour AWS Control Tower.
- Pour plus d'informations sur AWS Control Tower et AWS Config ses rôles, consultez AWS Control Tower ConfigRecorderRole.
- Pour plus d'informations sur les rôles utilisés par AWS Control Tower pour agréger les AWS Config informations relatives à vos comptes, consultez Comment AWS Control Tower agrège les AWS Config règles dans les unités d'organisation et les comptes non gérés.
- Pour plus d'informations sur la façon de protéger vos ressources lorsque vous attribuez des rôles et des autorisations, consultez les sections Conditions facultatives relatives aux relations d'approbation de vos rôles, Configuration facultative des AWS KMS clés et Empêcher l'usurpation d'identité entre services.
- Pour des informations spécifiques sur le provisionnement automatique des comptes dans AWS Control Tower avec des rôles IAM, consultez la section Provisionnement de compte automatisé avec des rôles IAM.

- Pour consulter la politique qui protège le sujet AWS Config SNS, voir La politique du sujet AWS Config SNS.

Comment AWS Control Tower utilise les rôles pour créer et gérer des comptes

En général, les rôles font partie de la gestion des identités et des accès (IAM) dans AWS. Pour des informations générales sur IAM et les rôles dans AWS, consultez la rubrique Rôles IAM dans le Guide de l'utilisateur AWS IAM.

Rôles et création de comptes

AWS Control Tower crée le compte d'un client en appelant l'`CreateAccount`API de AWS Organizations. Lors de la AWS Organizations création de ce compte, elle crée un rôle au sein de ce compte, qu'AWS Control Tower nomme en transmettant un paramètre à l'API. Le nom du rôle est `AWSControlTowerExecution`.

AWS Control Tower prend le relais `AWSControlTowerExecution` pour tous les comptes créés par Account Factory. À l'aide de ce rôle, AWS Control Tower définit le compte comme base de référence et applique des contrôles obligatoires (et tout autre contrôle activé), ce qui entraîne la création d'autres rôles. Ces rôles sont à leur tour utilisés par d'autres services, tels que AWS Config.

> **Note**
>
> Pour définir la base de référence d'un compte, il faut configurer ses ressources, notamment les modèles Account Factory, parfois appelés plans, et les contrôles. Le processus de référence définit également les rôles de journalisation et d'audit de sécurité centralisés sur le compte, dans le cadre du déploiement des modèles. Les lignes de base d'AWS Control Tower sont contenues dans les rôles que vous appliquez à chaque compte inscrit.

Pour plus d'informations sur les comptes et les ressources, consultezComptes AWS À propos d'AWS Control Tower.

Le AWSControlTowerExecution rôle, expliqué

Le rôle `AWSControlTowerExecution` doit être présent dans tous les comptes inscrits. Il permet à AWS Control Tower de gérer vos comptes individuels et de communiquer les informations les concernant à vos comptes d'audit et d'archivage des journaux.

Le `AWSControlTowerExecution` rôle peut être ajouté à un compte de différentes manières, comme suit :

- Pour les comptes de l'unité d'organisation de sécurité (parfois appelés comptes principaux), AWS Control Tower crée le rôle au moment de la configuration initiale d'AWS Control Tower.
- Pour un compte Account Factory créé via la console AWS Control Tower, AWS Control Tower crée ce rôle au moment de la création du compte.
- Pour l'inscription d'un compte unique, nous demandons aux clients de créer manuellement le rôle, puis d'inscrire le compte dans AWS Control Tower.
- Lors de l'extension de la gouvernance à une unité d'organisation, AWS Control Tower utilise le StackSet- AWSControlTowerExecutionRole pour créer le rôle dans tous les comptes de cette unité d'organisation.

Objectif du `AWSControlTowerExecution` rôle :

- `AWSControlTowerExecution`vous permet de créer et d'inscrire des comptes, automatiquement, à l'aide de scripts et de fonctions Lambda.
- `AWSControlTowerExecution` permet de configurer la journalisation de votre organisation, de sorte que tous les journaux de chaque compte soient envoyés au compte de journalisation.
- `AWSControlTowerExecution`vous permet d'enregistrer un compte individuel dans AWS Control Tower. Vous devez d'abord ajouter le `AWSControlTowerExecution` rôle à ce compte. Pour savoir comment ajouter le rôle, consultezAjoutez manuellement le rôle IAM requis à un rôle existant Compte AWS et inscrivez-le.

Comment le `AWSControlTowerExecution` rôle fonctionne avec les unités d'organisation :

Ce `AWSControlTowerExecution` rôle garantit que les contrôles AWS Control Tower que vous avez sélectionnés s'appliquent automatiquement à chaque compte individuel, dans chaque unité d'organisation, de votre organisation, ainsi qu'à chaque nouveau compte que vous créez dans AWS Control Tower. En conséquence :

- Vous pouvez fournir des rapports de conformité et de sécurité plus facilement, en vous basant sur les fonctionnalités d'audit et de journalisation intégrées aux contrôles d'AWS Control Tower.
- Vos équipes de sécurité et de conformité peuvent vérifier que toutes les exigences sont satisfaites et qu'aucune dérive organisationnelle ne s'est produite.

Pour plus d'informations sur la dérive, consultez Détecter et résoudre la dérive dans AWS Control Tower.

En résumé, le rôle `AWSControlTowerExecution` et la stratégie qui lui est associée vous offrent un contrôle flexible de la sécurité et de la conformité dans l'ensemble de votre organisation. Par conséquent, les violations de sécurité ou de protocole sont moins susceptibles de se produire.

Conditions facultatives pour vos relations de confiance

Vous pouvez imposer des conditions dans vos politiques de confiance en matière de rôles, afin de restreindre les comptes et les ressources qui interagissent avec certains rôles dans AWS Control Tower. Nous vous recommandons vivement de restreindre l'accès au `AWSControlTowerAdmin` rôle, car il autorise des autorisations d'accès étendues.

Pour empêcher un attaquant d'accéder à vos ressources, modifiez manuellement votre politique de confiance d'AWS Control Tower pour en ajouter au moins une `aws:SourceArn` ou une `aws:SourceAccount` condition à la déclaration de politique. Pour des raisons de sécurité, nous vous recommandons vivement d'ajouter `aws:SourceArn` cette condition, car elle est plus spécifique que `aws:SourceAccount` la limitation de l'accès à un compte et à une ressource spécifiques.

Si vous ne connaissez pas l'ARN complet de la ressource, ou si vous spécifiez plusieurs ressources, vous pouvez utiliser la `aws:SourceArn` condition avec des caractères génériques (*) pour les parties inconnues de l'ARN. Par exemple, `arn:aws:controltower:*:123456789012:*` fonctionne si vous ne souhaitez pas spécifier de région.

L'exemple suivant illustre l'utilisation de la condition `aws:SourceArn` IAM avec vos politiques de confiance des rôles IAM. Ajoutez cette condition à votre relation de confiance pour le AWSControlTowerAdminrôle, car le principal du service AWS Control Tower interagit avec celui-ci.

Comme indiqué dans l'exemple, l'ARN source est au format suivant : `arn:aws:controltower:${HOME_REGION}:${CUSTOMER_AWSACCOUNT_id}:*`

Remplacez `${HOME_REGION}` les chaînes `${CUSTOMER_AWSACCOUNT_id}` par votre propre région d'origine et le numéro de compte du compte appelant.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:controltower:us-west-2:012345678901:*"
        }
      }
    }
  ]
}
```

Dans l'exemple, l'ARN source désigné comme `arn:aws:controltower:us-west-2:012345678901:*` est le seul ARN autorisé à effectuer l'`sts:AssumeRole`action. En d'autres termes, seuls les utilisateurs qui peuvent se connecter à l'identifiant du compte`012345678901`, dans la `us-west-2` région, sont autorisés à effectuer des actions nécessitant ce rôle spécifique et cette relation de confiance pour le service AWS Control Tower, désigné comme`controltower.amazonaws.com`.

L'exemple suivant montre les `aws:SourceArn` conditions `aws:SourceAccount` et appliquées à la politique de confiance dans les rôles.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
```

```
        "StringEquals": {
          "aws:SourceAccount": "012345678901"
        },
        "StringLike": {
          "aws:SourceArn": "arn:aws:controltower:us-west-2:012345678901:*"
        }
      }
    }
  ]
}
```

L'exemple illustre l'instruction de `aws:SourceArn` condition, avec une déclaration de `aws:SourceAccount` condition ajoutée. Pour plus d'informations, consultez Empêchez l'usurpation d'identité entre services.

Pour des informations générales sur les politiques d'autorisation dans AWS Control Tower, consultezGérez l'accès aux ressources.

Recommandations :

Nous vous recommandons d'ajouter des conditions aux rôles créés par AWS Control Tower, car ces rôles sont directement assumés par d'autres services AWS. Pour plus d'informations, consultez l'exemple de AWSControlTowerAdmin, présenté précédemment dans cette section. Pour le rôle d' AWS Config enregistreur, nous recommandons d'ajouter la `aws:SourceArn` condition, en spécifiant l'ARN de l'enregistreur Config comme ARN source autorisé.

Pour les rôles tels que AWSControlTowerExecutionles rôles programmatiques pouvant être assumés par le compte AWS Control Tower Audit dans tous les comptes gérés, nous vous recommandons d'ajouter la `aws:PrincipalOrgID` condition à la politique de confiance relative à ces rôles, qui confirme que le principal accédant à la ressource appartient à un compte de la bonne AWS organisation. N'ajoutez pas l'énoncé de `aws:SourceArn` condition, car il ne fonctionnera pas comme prévu.

> **Note**
>
> En cas de dérive, il est possible qu'un rôle d'AWS Control Tower soit réinitialisé dans certaines circonstances. Il est recommandé de revérifier régulièrement les rôles, si vous les avez personnalisés.

Comment AWS Control Tower agrège les AWS Config règles dans les unités d'organisation et les comptes non gérés

Le compte de gestion AWS Control Tower crée un agrégateur au niveau de l'organisation, qui aide à détecter les AWS Config règles externes, de sorte qu'AWS Control Tower n'a pas besoin d'accéder à des comptes non gérés. La console AWS Control Tower vous indique le nombre de AWS Config règles créées en externe pour un compte donné. Vous pouvez consulter les détails de ces règles externes dans l'onglet External Config Rule Compliance de la page des détails du compte.

Pour créer l'agrégateur, AWS Control Tower ajoute un rôle doté des autorisations requises pour décrire une organisation et répertorier les comptes qui en dépendent. Le `AWSControlTowerConfigAggregatorRoleForOrganizations` rôle nécessite la politique `AWSConfigRoleForOrganizations` gérée et une relation de confiance avec`config.amazonaws.com`.

Voici la politique IAM (artefact JSON) attachée au rôle :

```
{
    "Version": "2012-10-17",
      "Statement": [
       {
        "Effect": "Allow",
        "Action": [
          "organizations:ListAccounts",
          "organizations:DescribeOrganization",
          "organizations:ListAWSServiceAccessForOrganization"
         ],
       "Resource": "*"
      }
    ]
  }
```

Voici la relation de `AWSControlTowerConfigAggregatorRoleForOrganizations` confiance :

```
{
    "Version": "2012-10-17",
      "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
```

```
        "Service": "config.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
      }
    ]
  }
}
```

Pour déployer cette fonctionnalité dans le compte de gestion, les autorisations suivantes sont ajoutées dans la politique géréeAWSControlTowerServiceRolePolicy, qui est utilisée par le AWSControlTowerAdmin rôle lors de la création de l' AWS Config agrégateur :

```
{
  "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "config:PutConfigurationAggregator",
          "config:DeleteConfigurationAggregator",
          "iam:PassRole"
          ],
        "Resource": [
          "arn:aws:iam:::role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations",
          "arn:aws:config:::config-aggregator/"
          ]
        },
      {
        "Effect": "Allow",
        "Action": "organizations:EnableAWSServiceAccess",
        "Resource": "*"
      }
    ]
}
```

Nouvelles ressources créées : AWSControlTowerConfigAggregatorRoleForOrganizations et aws-controltower-ConfigAggregatorForOrganizations

Lorsque vous êtes prêt, vous pouvez inscrire des comptes individuellement ou les inscrire en tant que groupe en enregistrant une unité d'organisation. Lorsque vous avez créé un compte, si vous créez une règle dans AWS Config, AWS Control Tower détecte la nouvelle règle. L'agrégateur indique le

nombre de règles externes et fournit un lien vers la AWS Config console où vous pouvez consulter les détails de chaque règle externe de votre compte. Utilisez les informations de la AWS Config console et de la console AWS Control Tower pour déterminer si les contrôles appropriés sont activés pour le compte.

Rôles programmatiques et relations de confiance pour le compte d'audit AWS Control Tower

Vous pouvez vous connecter au compte d'audit et assumer un rôle pour examiner les autres comptes par programmation. Le compte d'audit ne vous permet pas de vous connecter manuellement à d'autres comptes.

Le compte d'audit vous donne un accès programmatique à d'autres comptes, au moyen de certains rôles attribués uniquement aux fonctions AWS Lambda. Pour des raisons de sécurité, ces rôles entretiennent des relations de confiance avec d'autres rôles, ce qui signifie que les conditions dans lesquelles les rôles peuvent être utilisés sont strictement définies.

Le stack set AWS Control Tower `StackSet-AWSControlTowerBP-BASELINE-ROLES` crée ces rôles inter-comptes uniquement programmatiques dans le compte d'audit :

- aws-control tower- AdministratorExecutionRole
- aws-control tower- AuditAdministratorRole
- aws-control tower- ReadOnlyExecutionRole
- aws-control tower- AuditReadOnlyRole

`ReadOnlyExecutionRole:`Notez que ce rôle permet au compte d'audit de lire des objets dans des compartiments Amazon S3 dans l'ensemble de l'organisation (contrairement à la `SecurityAudit` politique, qui autorise uniquement l'accès aux métadonnées).

aws-controltower- : AdministratorExecutionRole

- Possède des autorisations d'administrateur
- Ne peut pas être supposé depuis la console
- Ne peut être assumé que par un rôle dans le compte d'audit, à savoir le `aws-controltower-AuditAdministratorRole`

L'artefact suivant montre la relation de confiance pour`aws-controltower-AdministratorExecutionRole`. Le numéro d'espace réservé `012345678901` sera remplacé par le `Audit_acct_ID` numéro de votre compte d'audit.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/aws-controltower-AuditAdministratorRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

aws-controltower- : AuditAdministratorRole

- Peut être utilisé uniquement par le AWS service Lambda
- Est autorisé à effectuer des opérations de lecture (Get) et d'écriture (Put) sur des objets Amazon S3 dont le nom commence par la chaîne log

Politiques jointes :

1. AWSLambdaExecute— politique AWS gérée

2. AssumeRole-aws-controltower- AuditAdministratorRole — politique en ligne — Créé par AWS Control Tower, l'artefact suit.

```
{
  "Version": "2012-10-17",
  "Statement": [
 {
 "Action": [
   "sts:AssumeRole"
   ],
 "Resource": [
   "arn:aws:iam::*:role/aws-controltower-AdministratorExecutionRole"
   ],
 "Effect": "Allow"
```

```
 }
   ]
}
```

L'artefact suivant montre la relation de confiance pour `aws-controltower-AuditAdministratorRole` :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

aws-controltower- : ReadOnlyExecutionRole

- Ne peut pas être supposé depuis la console
- Ne peut être assumé que par un autre rôle dans le compte d'audit, à savoir le `AuditReadOnlyRole`

L'artefact suivant montre la relation de confiance pour`aws-controltower-ReadOnlyExecutionRole`. Le numéro d'espace réservé `012345678901` sera remplacé par le `Audit_acct_ID` numéro de votre compte d'audit.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/aws-controltower-AuditReadOnlyRole "
      },
      "Action": "sts:AssumeRole"
    }
  ]
```

```
}
```

aws-controltower- : AuditReadOnlyRole

- Peut être utilisé uniquement par le AWS service Lambda
- Est autorisé à effectuer des opérations de lecture (Get) et d'écriture (Put) sur des objets Amazon S3 dont le nom commence par la chaîne log

Politiques jointes :

1. AWSLambdaExecute— politique AWS gérée

2. AssumeRole-aws-controltower- AuditReadOnlyRole — politique en ligne — Créé par AWS Control Tower, l'artefact suit.

```
{
  "Version": "2012-10-17",
  "Statement": [
 {
 "Action": [
  "sts:AssumeRole"
 ],
 "Resource": [
  "arn:aws:iam::*:role/aws-controltower-ReadOnlyExecutionRole"
 ],
 "Effect": "Allow"
   }
  ]
}
```

L'artefact suivant montre la relation de confiance pour `aws-controltower-AuditAdministratorRole` :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
```

```
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Provisioning automatisé des comptes avec des rôles IAM

Pour configurer les comptes Account Factory de manière plus automatisée, vous pouvez créer des fonctions Lambda dans le compte de gestion AWS Control Tower, qui assume le AWSControlTowerExecutionrôle dans le compte membre. Ensuite, à l'aide du rôle, le compte de gestion exécute les étapes de configuration souhaitées dans chaque compte membre.

Si vous approvisionnez des comptes à l'aide des fonctions Lambda, l'identité qui effectuera cette tâche doit respecter la politique d'autorisation IAM suivante, en plus de. `AWSServiceCatalogEndUserFullAccess`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSControlTowerAccountFactoryAccess",
            "Effect": "Allow",
            "Action": [
                "sso:GetProfile",
                "sso:CreateProfile",
                "sso:UpdateProfile",
                "sso:AssociateProfile",
                "sso:CreateApplicationInstance",
                "sso:GetSSOStatus",
                "sso:GetTrust",
                "sso:CreateTrust",
                "sso:UpdateTrust",
                "sso:GetPeregrineStatus",
                "sso:GetApplicationInstance",
                "sso:ListDirectoryAssociations",
                "sso:ListPermissionSets",
                "sso:GetPermissionSet",
                "sso:ProvisionApplicationInstanceForAWSAccount",
                "sso:ProvisionApplicationProfileForAWSAccountInstance",
                "sso:ProvisionSAMLProvider",
                "sso:ListProfileAssociations",
                "sso-directory:ListMembersInGroup",
```

```
                "sso-directory:AddMemberToGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchGroupsWithGroupName",
                "sso-directory:SearchUsers",
                "sso-directory:CreateUser",
                "sso-directory:DescribeGroups",
                "sso-directory:DescribeDirectory",
                "sso-directory:GetUserPoolInfo",
                "controltower:CreateManagedAccount",
                "controltower:DescribeManagedAccount",
                "controltower:DeregisterManagedAccount",
                "s3:GetObject",
                "organizations:describeOrganization",
                "sso:DescribeRegisteredRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

Les autorisations`sso:GetPeregrineStatus`, `sso:ProvisionApplicationInstanceForAWSAccountsso:ProvisionApplicationProfileForA` et `sso:ProvisionSAMLProvide` sont requises par AWS Control Tower Account Factory pour interagir avec AWS IAM Identity Center.

Ressources disponibles dans AWS Control Tower

- Pour obtenir des informations générales sur la propriété des ressources dans AWS Control Tower, consultezPrésentation de la gestion des autorisations d'accès à vos ressources AWS Control Tower.
- Pour plus d'informations sur les ressources créées par AWS Control Tower dans les comptes partagés, consultezÀ propos des comptes partagés.
- Pour plus d'informations sur les ressources créées par AWS Control Tower lorsqu'elle approvisionne un compte via Account Factory, consultezConsidérations relatives aux ressources pour Account Factory.
- Pour en savoir plus sur les types de AWS ressources définis par AWS Control Tower, à utiliser avec les API AWS Control Tower, consultez la référence relative aux types de ressources AWS Control Tower dans le guide de AWS CloudFormation l'utilisateur.

Comment AWS les régions fonctionnent avec AWS Control Tower

AWS Control Tower est actuellement pris en charge dans les AWS régions suivantes :

- USA Est (Virginie du Nord)
- USA Est (Ohio)
- USA Ouest (Oregon)
- Canada (Centre)
- Asie-Pacifique (Sydney)
- Asie-Pacifique (Singapour)
- Europe (Francfort)
- Europe (Irlande)
- Europe (Londres)
- Europe (Stockholm)
- Asie-Pacifique (Mumbai)
- Asie-Pacifique (Séoul)
- Asie-Pacifique (Tokyo)
- Europe (Paris)
- Amérique du Sud (São Paulo)
- USA Ouest (Californie du Nord)
- Asie-Pacifique (Hong Kong)
- Asie-Pacifique (Jakarta)
- Asie-Pacifique (Osaka)
- Europe (Milan)
- Afrique (Le Cap)
- Moyen-Orient (Bahreïn)
- Israël (Tel Aviv)
- Moyen-Orient (EAU)

- Europe (Espagne)
- Asie-Pacifique (Hyderabad)
- Europe (Zurich)
- Asie-Pacifique (Melbourne)
- Canada Ouest (Calgary)

À propos de votre région d'origine

Lorsque vous créez une zone d'atterrissage, la région que vous utilisez pour accéder à la console AWS de gestion devient votre AWS région d'origine pour AWS Control Tower. Au cours du processus de création, certaines ressources sont mises à disposition dans la région d'origine. Les autres ressources, telles que les unités d'organisation et les AWS comptes, sont mondiales.

Une fois que vous avez sélectionné une région d'origine, vous ne pouvez pas la modifier.

Contrôles et régions

À l'heure actuelle, tous les contrôles préventifs fonctionnent dans le monde entier. Les contrôles Detective et proactifs ne fonctionnent toutefois que dans les régions où AWS Control Tower est pris en charge. Pour plus d'informations sur le comportement des contrôles lorsque vous activez AWS Control Tower dans une nouvelle région, consultezConfigurez vos régions AWS Control Tower.

Configurez vos régions AWS Control Tower

Cette section décrit le comportement auquel vous pouvez vous attendre lorsque vous étendez votre zone d'atterrissage AWS Control Tower à une nouvelle AWS région ou que vous supprimez une région de la configuration de votre zone d'atterrissage. En général, cette action est effectuée par le biais de la fonction Update de la console AWS Control Tower.

> **Note**
>
> Nous vous recommandons d'éviter d'étendre la zone de landing de votre AWS Control Tower à des AWS régions dans lesquelles vous n'avez pas besoin de vos charges de travail pour fonctionner. Le fait de vous désinscrire d'une région ne vous empêche pas de déployer des ressources dans cette région, mais ces ressources resteront en dehors de la gouvernance d'AWS Control Tower.

Lors de la configuration d'une nouvelle région, AWS Control Tower met à jour la zone d'atterrissage, ce qui signifie qu'elle définit votre zone d'atterrissage comme base de référence :

- opérer activement dans toutes les régions nouvellement sélectionnées, et
- pour cesser de gérer les ressources dans les régions désélectionnées.

Les comptes individuels au sein de vos unités organisationnelles (UO) gérés par AWS Control Tower ne sont pas mis à jour dans le cadre de ce processus de mise à jour de la zone de landing zone. Par conséquent, vous devez mettre à jour vos comptes en réenregistrant vos unités d'organisation.

Lorsque vous configurez vos régions AWS Control Tower, tenez compte des recommandations et limites suivantes :

- Sélectionnez les régions dans lesquelles vous prévoyez d'héberger des AWS ressources ou des charges de travail.
- Le fait de vous désinscrire d'une région ne vous empêche pas de déployer des ressources dans cette région, mais ces ressources resteront en dehors de la gouvernance d'AWS Control Tower.

Lorsque vous configurez votre zone d'atterrissage pour de nouvelles régions, les contrôles de détection d'AWS Control Tower respectent les règles suivantes :

- Le comportement reste le même pour les éléments existants. Que ce soit pour la détection ou la prévention, le comportement des barrières de sécurité reste le même pour les comptes existants, dans les unités d'organisation existantes et dans les régions existantes.
- Vous ne pouvez pas appliquer de nouveaux contrôles de détection aux unités d'organisation existantes contenant des comptes qui ne sont pas mis à jour. Lorsque vous avez configuré votre zone d'atterrissage AWS Control Tower dans une nouvelle région (en mettant à jour votre zone d'atterrissage), vous devez mettre à jour les comptes existants dans vos unités d'organisation existantes avant de pouvoir activer de nouveaux contrôles de détection sur ces unités d'organisation et ces comptes.
- Vos contrôles de détection existants commencent à fonctionner dans les régions nouvellement configurées dès que vous mettez à jour les comptes. Lorsque vous mettez à jour votre zone de landing zone AWS Control Tower pour configurer de nouvelles régions, puis que vous mettez à jour un compte, les contrôles de détection déjà activés sur l'unité d'organisation commenceront à fonctionner sur ce compte dans les régions nouvellement configurées.

Configuration des régions AWS Control Tower

1. Connectez-vous à la console AWS Control Tower à l'adresse https://console.aws.amazon.com/controltower
2. Dans le menu de navigation du volet gauche, choisissez Paramètres de la zone d'atterrissage.
3. Sur la page des paramètres de la zone d'atterrissage, dans la section Détails, cliquez sur le bouton Modifier les paramètres en haut à droite. Vous êtes dirigé vers le flux de travail de mise à jour de la zone d'atterrissage, car pour gouverner de nouvelles régions ou supprimer des régions de la gouvernance, vous devez passer à la dernière version de la zone d'atterrissage.
4. Sous AWS Régions supplémentaires pour la gouvernance, recherchez les régions que vous souhaitez gouverner (ou arrêter de gouverner). La colonne État indique les régions que vous gouvernez actuellement et celles que vous ne gouvernez pas.
5. Cochez la case correspondant à chaque région supplémentaire à gouverner. Décochez la case correspondant à chaque région dans laquelle vous supprimez la gouvernance.

   > **Note**
   >
   > Si vous choisissez de ne pas gouverner une région, vous pouvez toujours y déployer des ressources, mais ces ressources resteront en dehors de la gouvernance d'AWS Control Tower.

6. Terminez le reste du flux de travail, puis choisissez Update landing zone.
7. Lorsque la configuration de la zone d'atterrissage est terminée, réenregistrez les UO pour mettre à jour les comptes dans vos nouvelles régions. Pour plus d'informations, consultez Quand mettre à jour les unités d'organisation et les comptes AWS Control Tower.

Une autre méthode pour approvisionner ou mettre à jour des comptes individuels après avoir configuré de nouvelles régions consiste à utiliser le framework d'API de Service Catalog et AWS CLIà mettre à jour les comptes par lots. Pour plus d'informations, consultez Fournir et mettre à jour des comptes à l'aide de l'automatisation.

Évitez la gouvernance mixte lors de la configuration des régions

Il est important de mettre à jour tous les comptes d'une unité d'organisation après avoir étendu la gouvernance d'AWS Control Tower à une nouvelle Région AWS entité et après avoir supprimé la gouvernance d'AWS Control Tower d'une région.

La gouvernance mixte est une situation indésirable qui peut se produire si les contrôles régissant une UO ne correspondent pas totalement aux contrôles régissant chaque compte au sein d'une UO. Une gouvernance mixte se produit dans une unité d'organisation si les comptes ne sont pas mis à jour après qu'AWS Control Tower ait étendu la gouvernance à une nouvelle Région AWS entité ou ait supprimé la gouvernance.

Dans ce cas, certains comptes d'une unité d'organisation peuvent être soumis à des contrôles différents selon les régions, par rapport à d'autres comptes de l'unité d'organisation ou par rapport à la posture de gouvernance globale de la zone d'atterrissage.

Dans une unité d'organisation à gouvernance mixte, si vous créez un nouveau compte, celui-ci bénéficiera de la même posture de gouvernance de région et d'unité organisationnelle (mise à jour) que la zone de landing zone. Toutefois, les comptes existants qui ne sont pas encore mis à jour ne bénéficient pas de la nouvelle posture de gouvernance de la région.

En général, une gouvernance mixte peut créer des indicateurs de statut contradictoires ou inexacts dans la console AWS Control Tower. Par exemple, dans le cadre d'une gouvernance mixte, les régions optionnelles apparaissent avec le statut Non gouvernée, dans les unités d'organisation enregistrées, pour les comptes qui ne sont pas encore mis à jour.

> **Note**
>
> AWS Control Tower n'autorise pas l'activation des contrôles dans un état de gouvernance mixte.

Comportement des contrôles lors d'une gouvernance mixte

- Dans le cadre d'une gouvernance mixte, AWS Control Tower ne peut pas déployer de manière cohérente des contrôles basés sur des AWS Config règles (c'est-à-dire des contrôles de détection) dans les régions que l'unité d'organisation indique déjà comme étant gouvernées, car certains comptes de l'unité d'organisation n'ont pas été mis à jour. Il est possible que vous receviez un message `FAILED_TO_ENABLE` d'erreur.
- Dans le cadre d'une gouvernance mixte, si vous étendez la gouvernance de la zone d'atterrissage à une région optionnelle alors qu'aucun compte de l'unité d'organisation n'a encore été mis à jour, le fonctionnement de l'`EnableControl`API sur l'unité d'organisation échoue pour les contrôles détectifs et proactifs. Vous recevrez un message d'`FAILED_TO_ENABLE`erreur, car les comptes de membres non mis à jour au sein de l'UO n'ont pas encore été ajoutés à ces régions.

- Dans le cadre d'une gouvernance mixte, les contrôles qui font partie de la norme gérée par le Security Hub Service : AWS Control Tower ne peuvent pas signaler avec précision la conformité dans les régions où la configuration de la zone de landing zone ne correspond pas à celle des comptes qui ne sont pas mis à jour.
- La gouvernance mixte ne modifie pas le comportement des contrôles basés sur les SCP (contrôles préventifs), qui s'appliquent uniformément à tous les comptes d'une unité d'organisation, dans chaque région gouvernée.

> **Note**
>
> La gouvernance mixte n'est pas la même chose que la dérive, et elle n'est pas signalée comme telle.

Pour réparer la gouvernance mixte

- Choisissez Mettre à jour le compte pour chaque compte de l'unité d'organisation dont le statut de mise à jour est disponible sur la page Organizations de la console.
- Choisissez Re-Register OU sur la page Organizations, qui met automatiquement à jour tous les comptes de l'unité d'organisation, pour les unités d'organisation comptant moins de 300 comptes.

Considérations relatives à l'activation des AWS régions optionnelles

Bien que la plupart Régions AWS soient actives par défaut pour vous Compte AWS, certaines régions ne sont activées que lorsque vous les sélectionnez manuellement. Dans le présent document, ces régions sont appelées « régions optionnelles ». En revanche, les régions actives par défaut, dès que la vôtre Compte AWS est créée, sont appelées régions commerciales, ou simplement régions.

Le terme « opt-in » a une base historique. Toute région Régions AWS introduite après le 20 mars 2019 est considérée comme une région optionnelle. Les régions optionnelles ont des exigences de sécurité plus strictes que les régions commerciales, en ce qui concerne le partage des données IAM via des comptes actifs dans les régions optionnelles. Toutes les données gérées via le service IAM sont considérées comme des données d'identité, y compris les utilisateurs, les groupes, les rôles, les politiques, les fournisseurs d'identité, leurs données associées (par exemple, les certificats de

signature X.509 ou les informations d'identification spécifiques au contexte) et les autres paramètres au niveau du compte, tels que la politique de mot de passe et l'alias du compte.

Vous pouvez activer automatiquement les régions optionnelles lors de la configuration de la zone d'atterrissage, en les sélectionnant. Votre zone de landing devient active dans toutes les régions sélectionnées.

Si vous choisissez de sélectionner une région optionnelle comme région d'origine de votre AWS Control Tower, activez-la d'abord en suivant les étapes décrites dans Enabling a Region, une fois connecté à la console AWS de gestion. Pour transférer vos propres comptes d'archivage de journaux et d'audit existants depuis une région optionnelle, activez d'abord manuellement cette région.

Les régions AWS optionnelles incluent plusieurs régions dans lesquelles AWS Control Tower est disponible :

- Région Asie-Pacifique (Hong Kong), ap-east-1
- Région Asie-Pacifique (Jakarta), ap-southeast-3
- Région Europe (Milan), eu-south-1
- Région Afrique (Cape Town), af-south-1
- Région du Moyen-Orient (Bahreïn), me-south-1
- Israël (Tel Aviv), il-central-1
- Région du Moyen-Orient (EAU), me-central-1
- Région Europe (Espagne), eu-south-2
- Région Asie-Pacifique (Hyderabad), ap-south-2
- Région Europe (Zurich), eu-central-2
- Région Asie-Pacifique (Melbourne), ap-southeast-4
- Région du Canada Ouest (Calgary), ca-west-1

AWS Control Tower dispose de certains contrôles qui fonctionnent différemment dans les régions optionnelles et dans les régions commerciales. Pour plus d'informations, consultez Limites de contrôle. Voici quelques points à prendre en compte lorsque vous déployez des charges de travail dans des régions optionnelles.

> **Gouverner ou activer ?**
>
> N'oubliez pas que gouverner une région est une action que vous pouvez sélectionner depuis la console AWS Control Tower, afin que les contrôles puissent être appliqués dans la région. L'activation ou la désactivation d'une région optionnelle est une action différente que vous pouvez choisir dans la AWS console, qui ouvre la région à votre compte, afin que vous puissiez y déployer des ressources et des charges de travail.

Considérations comportementales

- Si vous choisissez de gérer les régions optionnelles, nous vous recommandons de ne désactiver (de vous désinscrire) aucune de vos régions optionnelles gouvernées, car cela pourrait entraîner l'échec de vos charges de travail. AWS Control Tower n'autorise pas la désactivation d'une région gouvernée depuis la console AWS Control Tower, mais assurez-vous de ne pas désactiver les régions gouvernées depuis une source extérieure à AWS Control Tower, telle que la console de AWS facturation ou AWS le SDK.
- Lorsqu'AWS Control Tower étend la gouvernance à une région optionnelle, elle active (opts-in) la région dans tous les comptes membres. Lorsque vous supprimez une région de la gouvernance, AWS Control Tower ne la désactive pas (ne désactive pas) la région dans les comptes des membres.
- Lors de la désélection d'une région, AWS Control Tower ne supprime pas les ressources d'une région optionnelle si cette région a été désactivée manuellement pour un compte provenant d'une source extérieure à AWS Control Tower, telle que la console de AWS facturation ou le SDK. AWS Nous vous recommandons de supprimer les ressources des régions que vous avez désactivées, sous peine de recevoir des frais de facturation imprévus pour ces ressources.
- Si votre zone de landing zone est mise hors service, AWS Control Tower nettoie les ressources dans toutes les régions gouvernées, y compris les régions optionnelles. Cependant, AWS Control Tower ne désactive pas les régions optionnelles. Vous pouvez désactiver les régions optionnelles comme étape supplémentaire après la mise hors service.
- Si votre région d'origine est une région optionnelle, et si vous avez l'intention d'inscrire des comptes existants en tant que comptes d'archivage des journaux et d'audit, vous devez activer manuellement la région optionnelle avant de pouvoir la sélectionner comme région d'origine pour votre zone d'atterrissage. Voir Activation d'une région.

- Si AWS Control Tower est configurée avec une région optionnelle comme région d'origine, et si vous visitez le service AWS Control Tower depuis la AWS console d'une autre région, la console ne vous redirige pas automatiquement vers la région d'origine.
- L'API sous-jacente comporte des limites de capacité, ce qui peut augmenter le temps de latence de quelques minutes à plusieurs heures, en fonction du nombre de régions, de comptes et de la charge de service. Il est recommandé de n'opter que pour celles dans Régions AWS lesquelles vous allez exécuter les charges de travail, et d'opter pour une région à la fois.

Limitations importantes en matière de gouvernance et de contrôles

- Si vous avez actuellement activé un contrôle AWS Control Tower qui n'est pas pris en charge dans une région optionnelle, vous ne pourrez pas étendre la gouvernance d'AWS Control Tower à cette région optionnelle tant que le contrôle ne sera pas pris en charge dans cette région. Pour plus d'informations, consultez Limites de contrôle.
- Si vous étendez la gouvernance d'AWS Control Tower à une région optionnelle dans laquelle aucun contrôle spécifique n'est pris en charge, vous ne pourrez activer ce contrôle dans aucune région tant que le contrôle n'est pas pris en charge dans toutes les régions que vous gérez avec AWS Control Tower. Pour plus d'informations, consultez Limites de contrôle
- Si les 22 régions commerciales dans lesquelles AWS Control Tower est disponible sont activées, y compris les régions optionnelles, la limite supérieure du nombre de comptes par unité organisationnelle (UO), lors de l'extension de la gouvernance à une UO, est réduite. La limite est de 220 comptes au lieu de 300. Cette réduction est due à StackSet des limitations. Si vous souhaitez étendre la gouvernance aux unités d'organisation comptant plus de 220 comptes, réduisez le nombre de régions activées.

Configurer le contrôle de refus des régions

AWS Control Tower propose deux contrôles de refus régionaux. Une commande`GRREGIONDENY`, lorsqu'elle est activée, s'applique à l'ensemble de la zone d'atterrissage. Une autre commande`CTMULTISERVICEPV1`, lorsqu'elle est activée, peut s'appliquer à des unités d'organisation spécifiques que vous spécifiez. Pour plus d'informations, consultez la section Refuser l'accès en AWS fonction de la demande Région AWS et le contrôle de refus régional appliqué à l'unité d'organisation.

La Région de refus de contrôle `GRREGIONDENY` est unique, car elle s'applique à la zone d'atterrissage dans son ensemble, plutôt qu'à une unité d'organisation spécifique. Pour configurer

le refus de contrôle par région, rendez-vous sur la page des paramètres de la zone d'atterrissage et sélectionnez Modifier les paramètres.

- Ce paramètre peut être modifié ultérieurement.
- Lorsqu'elle est activée, cette commande s'applique à toutes les unités d'organisation enregistrées.
- Ce contrôle ne peut pas être configuré pour des unités d'organisation individuelles.

> **Note**
>
> Avant d'activer le refus de contrôle par région, assurez-vous que vous ne disposez pas de ressources existantes dans ces régions, car vous n'aurez pas accès à vos ressources une fois le contrôle appliqué. Tant que le contrôle est activé, vous ne pourrez pas déployer de ressources dans les régions interdites.

Le refus de contrôle de la région interdit l'accès aux AWS services, en fonction de la configuration de votre région AWS Control Tower. Il refuse l'accès aux AWS régions dont le statut est Non gouverné. Le refus de contrôle de la région refuse également l'accès aux régions dans lesquelles AWS Control Tower n'est pas disponible. Vous ne pouvez pas refuser l'accès à votre région d'origine. Certains AWS services internationaux, tels que IAM et AWS Organizations, sont exemptés du refus de contrôle de la Région. Pour en savoir plus, consultez la section Refuser l'accès AWS en fonction de la demande Région AWS.

Lorsque vous activez le contrôle, il s'applique à toutes les unités d'organisation de niveau supérieur enregistrées dans votre hiérarchie, et il est hérité par les unités d'organisation situées plus bas dans la chaîne. Lorsque vous supprimez le contrôle, il est supprimé sur toutes les unités d'organisation enregistrées, toutes les régions non gouvernées d'AWS Control Tower conservent le statut Non gouvernées et vous pouvez déployer des ressources dans des régions où AWS Control Tower n'est pas disponible.

- Nom du contrôle complet : refuser l'accès AWS en fonction de la AWS région demandée
- Description du garde-corps : interdit l'accès aux opérations non répertoriées dans les services mondiaux et régionaux en dehors des régions spécifiées.
- Il s'agit d'un contrôle électif avec des conseils préventifs.

Pour consulter le modèle du SCP de refus de contrôle régional, consultez la section Refuser l'accès en AWS fonction de ce qui est demandé Région AWS dans la référence AWS Control Tower Control. Le SCP d'AWS Control Tower est similaire au SCP de AWS Organizations, mais il n'est pas identique.

Vous pouvez déterminer les points de terminaison des services régionaux sur la page des services régionaux.

Considérations relatives au refus de contrôle des régions au niveau de l'UO

La principale considération concernant le refus de contrôle de la région au niveau de l'OU est de déterminer comment il interagira avec le contrôle de refus de la région de la zone d'atterrissage, si les deux sont activés. Pour plus d'informations, consultez la section Contrôle de refus de région appliqué à l'unité d'organisation.

Approvisionnement et gestion de comptes dans AWS Control Tower

Ce chapitre inclut une présentation et des procédures de mise en service et de gestion des comptes membres dans votre zone de landing zone AWS Control Tower.

Il inclut également une présentation et les procédures d'inscription d'un AWS compte existant dans AWS Control Tower.

Pour plus d'informations sur les comptes dans AWS Control Tower, consultezComptes AWS À propos d'AWS Control Tower. Pour plus d'informations sur l'inscription de plusieurs comptes dans AWS Control Tower, consultez. Enregistrer une unité organisationnelle existante auprès d'AWS Control Tower

> **Note**
>
> Vous pouvez effectuer jusqu'à cinq (5) opérations liées au compte simultanément, notamment le provisionnement, la mise à jour et l'inscription.

Méthodes de provisionnement

AWS Control Tower propose plusieurs méthodes pour créer et mettre à jour les comptes des membres. Certaines méthodes sont principalement basées sur la console, tandis que d'autres sont principalement automatisées.

Présentation

La méthode standard pour créer des comptes membres consiste à utiliser Account Factory, un produit basé sur une console qui fait partie du Service Catalog. Si votre zone de landing zone n'est pas en état de dérive, vous pouvez utiliser Create account pour ajouter de nouveaux comptes depuis la console, ou Enroll account pour inscrire des AWS comptes existants dans AWS Control Tower.

Avec Account Factory, vous pouvez configurer des comptes de base en vous basant sur les paramètres par défaut d'AWS Control Tower. Vous pouvez également créer des comptes personnalisés répondant aux exigences des cas d'utilisation spécialisés.

Account Factory Customization (AFC) est un moyen de configurer des comptes personnalisés à partir de la console AWS Control Tower. Il automatise la personnalisation et le déploiement de vos

comptes. Il permet un provisionnement automatisé basé sur la console, après quelques étapes de configuration uniques, ce qui élimine le besoin d'écrire des scripts ou de configurer des pipelines. Pour plus d'informations, consultez Personnalisez les comptes avec Account Factory Customization (AFC).

Méthodes basées sur la console :

- Par le biais de la console Account Factory qui en fait partie AWS Service Catalog, pour les comptes de base ou personnalisés. Consultez Provisionner et gérer des comptes avec Account Factory les détails et les instructions.
- Grâce à la fonctionnalité d'inscription d'un compte dans AWS Control Tower, si votre zone d'atterrissage n'est pas en état de dérive. veuillez consulter Inscrire un compte existant.
- Dans la console AWS Control Tower, vous pouvez utiliser Account Factory pour créer, mettre à jour ou inscrire jusqu'à cinq comptes simultanément.

Méthodes automatisées :

- Code Lambda : depuis le compte de gestion de votre zone d'atterrissage AWS Control Tower, à l'aide du code Lambda et des rôles IAM appropriés. Consultez la section Provisionnement automatique des comptes avec les rôles IAM.
- Terraform : de l'AWS Control Tower Account Factory for Terraform (AFT), qui s'appuie sur Account Factory et un GitOps modèle permettant d'automatiser le provisionnement et la mise à jour des comptes. veuillez consulter Provisionner des comptes avec AWS Control Tower Account Factory for Terraform (AFT) .
- Personnalisation d'Account Factory dans la console AWS Control Tower : après les étapes de configuration, le futur provisionnement de comptes personnalisés ne nécessite aucune configuration supplémentaire ni aucune maintenance du pipeline. Les comptes sont approvisionnés au moyen d'un AWS Service Catalog produit appelé Blueprint. Un plan peut utiliser des modèles ou AWS CloudFormation des modèles Terraform.

> **Note**
>
> AWS CloudFormation les plans peuvent déployer des ressources dans plusieurs régions. Les plans Terraform ne peuvent déployer des ressources que dans une seule région. Par défaut, il s'agit de la région d'origine.

Que se passe-t-il lorsque AWS Control Tower crée un compte

Les nouveaux comptes dans AWS Control Tower sont créés puis provisionnés par une interaction entre AWS Control Tower AWS Organizations, et AWS Service Catalog. Pour savoir comment inscrire un appareil existant à Compte AWS l'aide de la console AWS Control Tower, consultezInscrire un compte existant.

Dans les coulisses de la création de compte

1. Vous lancez la demande, par exemple, depuis la page AWS Control Tower Account Factory, directement depuis la AWS Service Catalog console ou en appelant l'`ProvisionProduct`API Service Catalog.
2. AWS Service Catalog appelle AWS Control Tower.
3. AWS Control Tower lance un flux de travail qui, dans un premier temps, appelle l' AWS Organizations `CreateAccount`API.
4. Après avoir AWS Organizations créé le compte, AWS Control Tower termine le processus de provisionnement en appliquant des plans et des contrôles.
5. Service Catalog continue d'interroger AWS Control Tower pour vérifier si le processus de mise en service est terminé.
6. Lorsque le flux de travail dans AWS Control Tower est terminé, Service Catalog finalise l'état du compte et vous informe (le demandeur) du résultat.

Autorisations requises pour les comptes

Les autorisations requises pour chaque méthode de provisionnement et de mise à jour des comptes sont décrites dans chaque section, respectivement. Avec les autorisations de groupe d'utilisateurs appropriées, les fournisseurs peuvent spécifier des lignes de base normalisées et des configurations réseau pour tous les comptes de leur organisation.

> **Note**
>
> Lors de la mise en service d'un compte, le demandeur du compte doit toujours disposer des autorisations `CreateAccount` et des `DescribeCreateAccountStatus` autorisations. Cet ensemble d'autorisations fait partie du rôle d'administrateur, et il est accordé automatiquement lorsqu'un demandeur assume le rôle d'administrateur. Si vous déléguez

l'autorisation de provisionner des comptes, vous devrez peut-être ajouter ces autorisations directement aux demandeurs de comptes.

Lorsque vous créez des comptes à partir de la console AWS Control Tower avec Account Factory, vous devez être connecté à un compte avec un utilisateur IAM dont la `AWSServiceCatalogEndUserFullAccess` politique est activée, ainsi que les autorisations nécessaires pour utiliser la console AWS Control Tower, et vous ne pouvez pas être connecté en tant qu'utilisateur root.

Pour obtenir des informations générales sur les autorisations requises dans AWS Control Tower, consultezUtilisation de politiques basées sur l'identité (politiques IAM) pour AWS Control Tower. Pour plus d'informations sur les rôles et les comptes dans AWS Control Tower, consultez la section Rôles et comptes.

Sécurité de vos comptes

Vous trouverez des conseils sur les meilleures pratiques pour protéger la sécurité de votre compte de gestion AWS Control Tower et de vos comptes membres dans la AWS Organizations documentation.

- Bonnes pratiques pour le compte de gestion
- Bonnes pratiques pour les comptes des membres

Comptes AWS À propos d'AWS Control Tower

An Compte AWS est le conteneur pour toutes vos propres ressources. Ces ressources incluent les identités AWS Identity and Access Management (IAM) acceptées par le compte, qui déterminent qui a accès à ce compte. Les identités IAM peuvent inclure des utilisateurs, des groupes, des rôles, etc. Pour plus d'informations sur l'utilisation de l'IAM, les utilisateurs, les rôles et les politiques dans AWS Control Tower, consultez la section Gestion des identités et des accès dans AWS Control Tower.

Ressources et délai de création du compte

Lorsqu'AWS Control Tower crée ou inscrit un compte, elle déploie la configuration de ressources minimale nécessaire pour le compte, y compris des ressources sous la forme de modèles Account Factory et d'autres ressources dans votre zone de landing zone. Ces ressources peuvent inclure des

rôles IAM, des AWS CloudTrail pistes, des produits fournis par Service Catalog et des utilisateurs d'IAM Identity Center. AWS Control Tower déploie également des ressources, conformément à la configuration de contrôle, pour l'unité organisationnelle (UO) dans laquelle le nouveau compte est destiné à devenir un compte membre.

AWS Control Tower orchestre le déploiement de ces ressources en votre nom. Le déploiement peut prendre plusieurs minutes par ressource. Tenez donc compte du temps total avant de créer ou d'inscrire un compte. Pour plus d'informations sur la gestion des ressources de vos comptes, consultezConseils pour créer et modifier les ressources AWS Control Tower.

Considérations relatives à l'ajout de comptes de sécurité ou de journalisation existants

Avant d'accepter un compte Compte AWS en tant que compte de sécurité ou de connexion, AWS Control Tower vérifie si le compte contient des ressources en conflit avec les exigences d'AWS Control Tower. Par exemple, vous pouvez avoir un bucket de journalisation portant le même nom que celui requis par AWS Control Tower. AWS Control Tower vérifie également que le compte peut fournir des ressources ; par exemple, en s'assurant que AWS Security Token Service (AWS STS) est activé, que le compte n'est pas suspendu et qu'AWS Control Tower est autorisée à fournir des ressources au sein du compte.

AWS Control Tower ne supprime aucune ressource existante dans les comptes de journalisation et de sécurité que vous fournissez. Toutefois, si vous choisissez d'activer la fonctionnalité de Région AWS refus, le contrôle de refus par région empêche l'accès aux ressources dans les régions interdites.

Consultez vos comptes

La page Organisation répertorie toutes les unités d'organisation et tous les comptes de votre organisation, quel que soit l'unité d'organisation ou le statut d'inscription dans AWS Control Tower. Vous pouvez consulter et inscrire les comptes membres dans AWS Control Tower, individuellement ou par groupes d'unités d'organisation, si chaque compte répond aux conditions requises pour l'inscription.

Pour consulter un compte spécifique sur la page Organisation, vous pouvez sélectionner Comptes uniquement dans le menu déroulant en haut à droite, puis sélectionner le nom de votre compte dans le tableau. Vous pouvez également sélectionner le nom de l'unité d'organisation parent dans le tableau et consulter la liste de tous les comptes de cette unité d'organisation sur la page Détails de cette unité d'organisation.

Sur les pages Organisation et Détails du compte, vous pouvez voir l'état du compte, qui est l'un des suivants :

- Non inscrit : le compte est membre de l'unité d'organisation parent, mais il n'est pas entièrement géré par AWS Control Tower. Si l'unité d'organisation parent est enregistrée, le compte est régi par les contrôles préventifs configurés pour son unité d'organisation parent enregistrée, mais les contrôles de détection de l'unité d'organisation ne s'appliquent pas à ce compte. Si l'unité d'organisation parent n'est pas enregistrée, aucun contrôle ne s'applique à ce compte.
- Inscription — Le compte est intégré à la gouvernance par AWS Control Tower. Nous alignons le compte sur la configuration de contrôle de l'unité d'organisation parent. Ce processus peut nécessiter plusieurs minutes par ressource du compte.
- Inscrit — Le compte est régi par les contrôles configurés pour son unité d'organisation parent. Il est entièrement géré par AWS Control Tower.
- Échec de l'inscription : le compte n'a pas pu être inscrit dans AWS Control Tower. Pour plus d'informations, consultez Causes courantes d'échec de l'inscription.
- Mise à jour disponible — Une mise à jour est disponible sur le compte. Les comptes dans cet état sont toujours inscrits, mais ils doivent être mis à jour pour refléter les modifications récentes apportées à votre environnement. Pour mettre à jour un seul compte, accédez à la page détaillée du compte et sélectionnez Mettre à jour le compte.

  Si vous avez plusieurs comptes dotés de cet état dans une seule unité d'organisation, vous pouvez choisir de réenregistrer l'unité d'organisation et de mettre à jour ces comptes ensemble.

Ressources créées dans les comptes partagés

Cette section présente les ressources créées par AWS Control Tower dans les comptes partagés lorsque vous configurez votre zone de landing zone.

Pour plus d'informations sur les ressources relatives aux comptes de membres, consultezConsidérations relatives aux ressources pour Account Factory.

Ressources du compte de gestion

Lorsque vous configurez votre zone de landing zone, les AWS ressources suivantes sont créées dans votre compte de gestion.

Service AWS	Type de ressource	Nom de la ressource
AWS Organizations	Comptes	audit log archive
AWS Organizations	Unités d'organisation	Security Sandbox
AWS Organizations	Politiques de contrôle de service	aws-guardrails-*
AWS CloudFormation	Piles	AWSControlTowerBP-BASELINE-CLOUDTRAIL-MASTER AWSControlTowerBP-BASELINE-CONFIG-MASTER(dans la version 2.6 et versions ultérieures)
AWS CloudFormation	StackSets	AWSControlTowerBP-BASELINE-CLOUDTRAIL(Non déployé dans la version 3.0 et versions ultérieures) AWSControlTowerBP_BASELINE_SERVICE_LINKED_ROLE (Deployed in 3.2 and later) AWSControlTowerBP-BASELINE-CLOUDWATCH AWSControlTowerBP-BASELINE-CONFIG AWSControlTowerBP-BASELINE-ROLES

Service AWS	Type de ressource	Nom de la ressource
		AWSControlTowerBP-BASELINE-SERVICE-ROLES AWSControlTowerBP-SECURITY-TOPICS AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED AWSControlTowerLoggingResources AWSControlTowerSecurityResources AWSControlTowerExecutionRole
AWS Service Catalog	Produit (langue française non garantie)	AWS Control Tower Account Factory
AWS Config	Agrégateur	aws-controltower-ConfigAggregatorForOrganizations
AWS CloudTrail	Journal d'activité	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch Journaux	aws-controltower/CloudTrail Logs

Service AWS	Type de ressource	Nom de la ressource
AWS Identity and Access Management	Rôles	AWSControlTowerAdmin AWSControlTowerStackSetRole AWSControlTowerCloudTrailRolePolicy
AWS Identity and Access Management	Politiques	AWSControlTowerServiceRolePolicy AWSControlTowerAdminPolicy AWSControlTowerCloudTrailRolePolicy AWSControlTowerStackSetRolePolicy
AWS IAM Identity Center	Groupes d'annuaires	AWSAccountFactory AWSAuditAccountAdmins AWSControlTowerAdmins AWSLogArchiveAdmins AWSLogArchiveViewers AWSSecurityAuditors AWSSecurityAuditPowerUsers AWSServiceCatalogAdmins

Service AWS	Type de ressource	Nom de la ressource
AWS IAM Identity Center	Jeux d'autorisations	AWSAdministratorAccess AWSPowerUserAccess AWSServiceCatalogAdminFullAccess AWSServiceCatalogEndUserAccess AWSReadOnlyAccess AWSOrganizationsFullAccess

> **Note**
>
> AWS CloudFormation StackSet `BP_BASELINE_CLOUDTRAIL` n'est pas déployé dans les versions 3.0 ou ultérieures de la zone d'atterrissage. Toutefois, elle continue d'exister dans les versions antérieures de la zone d'atterrissage, jusqu'à ce que vous mettiez à jour votre zone d'atterrissage.

Archiver les ressources du compte

Lorsque vous configurez votre zone de landing zone, les AWS ressources suivantes sont créées dans votre compte d'archive de journaux.

Service AWS	Type de ressource	Nom de la ressource
AWS CloudFormation	Piles	StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED- StackSet-AWSControlTowerGuardrailAWS-GR-

Service AWS	Type de ressource	Nom de la ressource
		AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH- StackSet-AWSControlTowerBP-BASELINE-CONFIG- StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL- StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES- StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In 3.2 and later) StackSet-AWSControlTowerBP-BASELINE-ROLES- StackSet-AWSControlTowerLoggingResources-
AWS Config	AWS Config Rules	AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIBIT

Service AWS	Type de ressource	Nom de la ressource
AWS CloudTrail	Journaux de suivi	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch Règles de l'événement	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch Journaux	/aws/lambda/aws-controltower-NotificationForwarder
AWS Identity and Access Management	Rôles	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole AWSControlTowerExecution
AWS Identity and Access Management	Politiques	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	Rubriques	aws-controltower-SecurityNotifications
AWS Lambda	Applications	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*
AWS Lambda	Fonctions	aws-controltower-NotificationForwarder

Service AWS	Type de ressource	Nom de la ressource
Amazon Simple Storage Service	Compartiments	aws-controltower-logs-* aws-controltower-s3-access-logs-*

Ressources du compte d'audit

Lorsque vous configurez votre zone de landing zone, les AWS ressources suivantes sont créées dans votre compte d'audit.

Service AWS	Type de ressource	Nom de la ressource
AWS CloudFormation	Piles	StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED- StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED- StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH- StackSet-AWSControlTowerBP-BASELINE-CONFIG- StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL-

Service AWS	Type de ressource	Nom de la ressource
		StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES- StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In 3.2 and later) StackSet-AWSControlTowerBP-SECURITY-TOPICS- StackSet-AWSControlTowerBP-BASELINE-ROLES- StackSet-AWSControlTowerSecurityResources-*
AWS Config	Agrégateur	aws-controltower-GuardrailsComplianceAggregator
AWS Config	AWS Config Rules	AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIBITED
AWS CloudTrail	Journal d'activité	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch Règles de l'événement	aws-controltower-ConfigComplianceChangeEventRule

Service AWS	Type de ressource	Nom de la ressource
Amazon CloudWatch	CloudWatch Journaux	/aws/lambda/aws-controltower-NotificationForwarder
AWS Identity and Access Management	Rôles	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole aws-controltower-AuditAdministratorRole aws-controltower-AuditReadOnlyRole AWSControlTowerExecution
AWS Identity and Access Management	Politiques	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	Rubriques	aws-controltower-AggregateSecurityNotifications aws-controltower-AllConfigNotifications aws-controltower-SecurityNotifications

Service AWS	Type de ressource	Nom de la ressource
AWS Lambda	Fonctions	aws-controltower-NotificationForwarder

À propos des comptes partagés

Trois offres spéciales Comptes AWS sont associées à AWS Control Tower : le compte de gestion, le compte d'audit et le compte d'archivage des journaux. Ces comptes sont généralement appelés comptes partagés, ou parfois comptes principaux.

- Vous pouvez sélectionner des noms personnalisés pour les comptes d'audit et d'archivage des journaux lorsque vous configurez votre zone de landing zone. Pour plus d'informations sur la modification du nom d'un compte, consultez Modification externe des noms de ressources AWS Control Tower.
- Vous pouvez également spécifier un compte existant Compte AWS en tant que compte de sécurité ou de journalisation AWS Control Tower, lors du processus de configuration initiale de la zone de landing zone. Grâce à cette option, AWS Control Tower n'a plus besoin de créer de nouveaux comptes partagés. (Il s'agit d'une sélection unique.)

Pour plus d'informations sur les comptes partagés et leurs ressources associées, consultezRessources créées dans les comptes partagés.

Compte de gestion

Cela Compte AWS lance AWS Control Tower. Par défaut, l'utilisateur root de ce compte et l'utilisateur IAM ou l'utilisateur administrateur IAM de ce compte ont un accès complet à toutes les ressources de votre zone de landing zone.

> **Note**
>
> Il est recommandé de vous connecter en tant qu'utilisateur IAM Identity Center avec des privilèges d'administrateur lorsque vous effectuez des tâches administratives dans la console AWS Control Tower, au lieu de vous connecter en tant qu'utilisateur root ou administrateur IAM pour ce compte.

Pour plus d'informations sur les rôles et les ressources disponibles dans le compte de gestion, consultezRessources créées dans les comptes partagés.

Compte d'archivage des journaux

Le compte partagé d'archivage du journal est configuré automatiquement lorsque vous créez votre zone de landing zone.

Ce compte contient un compartiment Amazon S3 central permettant de stocker une copie de tous les comptes AWS CloudTrail et les fichiers AWS Config journaux de tous les autres comptes de votre zone de landing zone. À titre de bonne pratique, nous recommandons de restreindre l'accès aux comptes d'archivage des journaux aux équipes chargées de la conformité et des enquêtes, ainsi qu'à leurs outils de sécurité ou d'audit associés. Ce compte peut être utilisé pour des audits de sécurité automatisés ou pour héberger des fonctionnalités personnalisées AWS Config Rules, telles que des fonctions Lambda, afin d'effectuer des actions correctives.

> **Politique relative aux compartiments Amazon S3**
>
> Pour la version 3.3 et les versions ultérieures d'AWS Control Tower landing zone, les comptes doivent remplir une `aws:SourceOrgID` condition pour toute autorisation d'écriture dans votre compartiment d'audit. Cette condition garantit que CloudTrail seuls les journaux peuvent être écrits pour le compte de comptes au sein de votre organisation dans votre compartiment S3 ; elle empêche CloudTrail les journaux extérieurs à votre organisation d'écrire dans votre compartiment AWS Control Tower S3. Pour plus d'informations, consultez Zone de landing zone d'AWS Control Tower, version 3.3.

Pour plus d'informations sur les rôles et les ressources disponibles dans le compte d'archivage des journaux, voir Archiver les ressources du compte

> **Note**
>
> Ces journaux ne peuvent pas être modifiés. Tous les journaux sont conservés à des fins d'audit et d'enquêtes de conformité liées à l'activité du compte.

Compte d'audit

Ce compte partagé est configuré automatiquement lorsque vous créez votre zone de landing zone.

Le compte d'audit doit être réservé aux équipes chargées de la sécurité et de la conformité ayant des rôles intercomptes d'auditeur (lecture seule) et d'administrateur (accès complet) pour tous les comptes de la zone de landing zone. Ces rôles sont destinés à être utilisés par les équipes de sécurité et de conformité pour :

- Réalisez des audits par le biais de AWS mécanismes tels que l'hébergement de fonctions Lambda basées sur des AWS Config règles personnalisées.
- Effectuez des opérations de sécurité automatisées, telles que des actions correctives.

Le compte d'audit reçoit également des notifications via le service Amazon Simple Notification Service (Amazon SNS). Trois catégories de notifications peuvent être reçues :

- Tous les événements de configuration : cette rubrique regroupe toutes les AWS Config notifications CloudTrail de tous les comptes de votre zone de landing zone.
- Notifications de sécurité agrégées : cette rubrique regroupe toutes les notifications de sécurité relatives à des CloudWatch événements spécifiques, à des événements de modification du statut de AWS Config Rules conformité et à des GuardDuty résultats.
- Notifications de dérive : cette rubrique regroupe tous les avertissements de dérive découverts sur tous les comptes, utilisateurs, unités d'organisation et SCP de votre zone d'atterrissage. Pour plus d'informations sur la dérive, voirDétectez et corrigez les dérives dans AWS Control Tower.

Les notifications d'audit déclenchées au sein d'un compte membre peuvent également envoyer des alertes à une rubrique Amazon SNS locale. Cette fonctionnalité permet aux administrateurs de compte de s'abonner aux notifications d'audit spécifiques à un compte de membre individuel. Les administrateurs peuvent ainsi résoudre les problèmes qui concernent un compte individuel, tout en regroupant toutes les notifications de compte sur votre compte d'audit centralisé. Pour plus d'informations, consultez le Guide du développeur Amazon Simple Notification Service.

Pour plus d'informations sur les rôles et les ressources disponibles dans le compte d'audit, consultezRessources du compte d'audit.

Pour plus d'informations sur l'audit programmatique, consultez la section Rôles programmatiques et relations de confiance pour le compte d'audit AWS Control Tower.

> **Important**
>
> L'adresse e-mail que vous fournissez pour le compte d'audit reçoit des e-mails de AWS notification et de confirmation d'abonnement de la part de toutes les Région AWS entreprises prises en charge par AWS Control Tower. Pour recevoir des e-mails de conformité sur votre compte d'audit, vous devez choisir le lien de confirmation d'abonnement contenu dans chaque e-mail provenant de chaque e-mail Région AWS pris en charge par AWS Control Tower.

À propos des comptes des membres

Les comptes membres sont les comptes par le biais desquels vos utilisateurs exécutent leur AWS charge de travail. Ces comptes membres peuvent être créés dans Account Factory, par les utilisateurs d'IAM Identity Center dotés de privilèges d'administrateur dans la console Service Catalog ou par des méthodes automatisées. Une fois créés, ces comptes membres existent dans une unité d'organisation créée dans la console AWS Control Tower ou enregistrée auprès d'AWS Control Tower. Pour plus d'informations, consultez les rubriques connexes suivantes :

- Provisionner et gérer des comptes avec Account Factory
- Automatisez les tâches dans AWS Control Tower
- AWS Organisations : terminologie et concepts dans le guide de AWS Organizations l'utilisateur.

Voir aussi Provisionner des comptes avec AWS Control Tower Account Factory for Terraform (AFT) .

> **Comptes et contrôles**
>
> Les comptes des membres peuvent être inscrits dans AWS Control Tower, ou ils peuvent être désinscrits. Les contrôles s'appliquent différemment aux comptes inscrits et non inscrits, et les contrôles peuvent s'appliquer aux comptes des unités d'organisation imbriquées sur la base de l'héritage.

Pour plus d'informations sur les ressources allouées aux comptes membres par AWS Control Tower, consultez. Considérations relatives aux ressources pour Account Factory

Inscrire un existant Compte AWS

Vous pouvez étendre la gouvernance d'AWS Control Tower à un individu, existant Compte AWS lorsque vous l'inscrivez dans une unité organisationnelle (UO) déjà régie par AWS Control Tower. Les comptes éligibles existent dans des unités d'organisation non enregistrées qui font partie de la même AWS Organizations organisation que l'unité d'organisation AWS Control Tower.

> **Note**
>
> Vous ne pouvez pas enregistrer un compte existant comme compte d'audit ou d'archivage des journaux, sauf lors de la configuration initiale de la zone d'atterrissage.

Configurez d'abord un accès sécurisé

Avant de pouvoir inscrire un Compte AWS compte existant dans AWS Control Tower, vous devez autoriser AWS Control Tower à gérer ou à gouverner le compte. Plus précisément, AWS Control Tower a besoin d'une autorisation pour établir un accès fiable entre vous AWS CloudFormation et en votre nom, afin de AWS CloudFormation pouvoir déployer automatiquement votre stack AWS Organizations sur les comptes de l'organisation que vous avez sélectionnée. Grâce à cet accès fiable, le `AWSControlTowerExecution` rôle mène les activités nécessaires à la gestion de chaque compte. C'est pourquoi vous devez ajouter ce rôle à chaque compte avant de l'inscrire.

Lorsque l'accès sécurisé est activé, AWS CloudFormation vous pouvez créer, mettre à jour ou supprimer des piles sur plusieurs comptes et Régions AWS en une seule opération. AWS Control Tower s'appuie sur cette capacité de confiance pour appliquer des rôles et des autorisations aux comptes existants avant de les transférer dans une unité organisationnelle enregistrée, et de les placer ainsi sous gouvernance.

Pour en savoir plus sur l'accès sécurisé AWS CloudFormation StackSets, consultez AWS CloudFormationStackSetset AWS Organizations.

Que se passe-t-il lors de l'inscription au compte

Au cours du processus d'inscription, AWS Control Tower effectue les actions suivantes :

- Établit la référence du compte, ce qui inclut le déploiement de ces ensembles de piles :
  - `AWSControlTowerBP-BASELINE-CLOUDTRAIL`

- `AWSControlTowerBP-BASELINE-CLOUDWATCH`
- `AWSControlTowerBP-BASELINE-CONFIG`
- `AWSControlTowerBP-BASELINE-ROLES`
- `AWSControlTowerBP-BASELINE-SERVICE-ROLES`
- `AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLES`
- `AWSControlTowerBP-VPC-ACCOUNT-FACTORY-V1`

Il est conseillé de passer en revue les modèles de ces ensembles de piles et de s'assurer qu'ils ne sont pas en conflit avec vos stratégies existantes.

- Identifie le compte par le biais de AWS IAM Identity Center ou AWS Organizations.
- Place le compte dans l'unité d'organisation que vous avez spécifiée. Veillez à appliquer tous les SCP qui sont appliqués dans l'unité d'organisation actuelle, afin que votre situation de sécurité reste cohérente.
- Applique les contrôles obligatoires au compte au moyen des SCP qui s'appliquent à l'unité d'organisation sélectionnée dans son ensemble.
- Active AWS Config et configure le système pour enregistrer toutes les ressources du compte.
- Ajoute les AWS Config règles qui appliquent les contrôles de détection d'AWS Control Tower au compte.

Comptes et parcours au niveau de l'organisation CloudTrail

Tous les comptes des membres d'une UO sont régis par l' AWS CloudTrail historique de l'UO, qu'ils soient inscrits ou non :

- Lorsque vous enregistrez un compte dans AWS Control Tower, celui-ci est régi par le AWS CloudTrail parcours de la nouvelle organisation. Si vous avez déjà déployé une version d'essai CloudTrail , des frais supplémentaires peuvent être facturés, sauf si vous supprimez la version d'essai existante pour le compte avant de l'inscrire dans AWS Control Tower.
- Si vous transférez un compte vers une unité d'organisation enregistrée, par exemple au moyen de la AWS Organizations console, et que vous ne procédez pas à l'inscription du compte dans AWS Control Tower, vous souhaiterez peut-être supprimer les traces restantes au niveau du compte. Si vous avez déjà déployé un CloudTrail trail, vous devrez payer des CloudTrail frais supplémentaires.

Si vous mettez à jour votre zone d'atterrissage et que vous choisissez de ne plus participer aux pistes au niveau de l'organisation, ou si votre zone d'atterrissage est antérieure à la version 3.0, les CloudTrail pistes au niveau de l'organisation ne s'appliquent pas à vos comptes.

Inscription de comptes existants auprès de VPC

AWS Control Tower gère les VPC différemment lorsque vous créez un nouveau compte dans Account Factory ou lorsque vous enregistrez un compte existant.

- Lorsque vous créez un nouveau compte, AWS Control Tower supprime automatiquement le VPC AWS par défaut et crée un nouveau VPC pour ce compte.
- Lorsque vous enregistrez un compte existant, AWS Control Tower ne crée pas de nouveau VPC pour ce compte.
- Lorsque vous enregistrez un compte existant, AWS Control Tower ne supprime aucun VPC existant ou VPC AWS par défaut associé au compte.

Tip

Vous pouvez modifier le comportement par défaut des nouveaux comptes en configurant Account Factory, afin qu'il ne configure pas de VPC par défaut pour les comptes de votre organisation sous AWS Control Tower. Pour plus d'informations, consultez Créez un compte dans AWS Control Tower sans VPC.

Conditions préalables à l'inscription

Les conditions préalables suivantes sont requises avant de pouvoir inscrire une personne existante Compte AWS dans AWS Control Tower :

1. Pour inscrire un poste existant Compte AWS, le `AWSControlTowerExecution` rôle doit être présent dans le compte que vous inscrivez. Vous pouvez consulter Enregistrer un compte pour obtenir des informations et des instructions.

2. Outre le `AWSControlTowerExecution` rôle, le titulaire que Compte AWS vous souhaitez inscrire doit disposer des autorisations et des relations de confiance suivantes. Sinon, l'inscription échouera.

   Autorisation de rôle : `AdministratorAccess` (politique AWS gérée)

   Relation d'approbation de rôle :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::Management Account ID:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

3. Nous recommandons que le compte ne dispose pas d'un enregistreur AWS Config de configuration ou d'un canal de diffusion. Ils peuvent être supprimés ou modifiés AWS CLI avant de pouvoir créer un compte. Sinon, consultez les comptes d'inscription dotés de AWS Config ressources existantes pour obtenir des instructions sur la manière dont vous pouvez modifier vos ressources existantes.
4. Le compte que vous souhaitez inscrire doit exister dans la même AWS Organizations organisation que le compte de gestion AWS Control Tower. Le compte existant ne peut être inscrit que dans la même organisation que le compte de gestion AWS Control Tower, dans une unité d'organisation déjà enregistrée auprès d'AWS Control Tower.

Pour vérifier les autres conditions préalables à l'inscription, consultez Getting Started with AWS Control Tower.

> **Note**
>
> Lorsque vous créez un compte dans AWS Control Tower, celui-ci est régi par le AWS CloudTrail parcours de l'organisation AWS Control Tower. Si vous avez déjà déployé une version d'essai CloudTrail, des frais supplémentaires peuvent être facturés, sauf si vous

supprimez la version d'essai existante pour le compte avant de l'inscrire dans AWS Control Tower.

Inscrire un compte existant

La fonctionnalité d'inscription d'un compte est disponible dans la console AWS Control Tower. Elle permet d'inscrire des comptes existants Comptes AWS afin qu'ils soient régis par AWS Control Tower. Pour plus d'informations, voir Inscrire un existant Compte AWS.

La fonction Inscrire un compte est disponible lorsque votre zone de destination n'est pas en état de dérive. Pour afficher cette fonctionnalité dans la console :

- Accédez à la page Organisation dans AWS Control Tower.
- Trouvez le nom du compte que vous souhaitez enregistrer. Pour le trouver, choisissez Comptes uniquement dans le menu déroulant en haut à droite, puis recherchez le nom du compte dans le tableau filtré.
- Suivez les étapes pour créer un compte individuel, comme indiqué dans la Étapes pour créer un compte section.

> **Note**
>
> Lorsque vous inscrivez une adresse e-mail existante Compte AWS, assurez-vous de vérifier l'adresse e-mail existante. Dans le cas contraire, un nouveau compte peut être créé.

Certaines erreurs peuvent nécessiter que vous actualisiez la page et que vous réessayiez. Si votre zone de destination est en état de dérive, il se peut que vous ne puissiez pas utiliser la fonction Inscrire un compte avec succès. Vous devrez créer de nouveaux comptes via Account Factory jusqu'à ce que votre problème de dérive de la zone d'atterrissage soit résolu.

Lorsque vous enregistrez des comptes depuis la console AWS Control Tower, vous devez être connecté à un compte dont la `AWSServiceCatalogEndUserFullAccess` politique est activée, ainsi que des autorisations d'accès d'administrateur pour utiliser la console AWS Control Tower, et vous ne pouvez pas être connecté en tant qu'utilisateur root.

Les comptes que vous inscrivez peuvent être mis à jour par le biais AWS Service Catalog de l'usine de comptes AWS Control Tower, comme vous le feriez pour tout autre compte. Les procédures de

mise à jour sont indiquées dans la section appelée Mettez à jour et déplacez les comptes Account Factory avec AWS Control Tower ou avec AWS Service Catalog.

Étapes pour créer un compte

Une fois que l'AdministratorAccessautorisation (politique) est en place sur votre compte existant, procédez comme suit pour enregistrer le compte :

Pour créer un compte individuel dans AWS Control Tower

- Accédez à la page d'organisation d'AWS Control Tower.
- Sur la page Organisation, les comptes éligibles à l'inscription vous permettent de sélectionner S'inscrire dans le menu déroulant Actions en haut de la section. Ces comptes affichent également un bouton d'inscription lorsque vous les consultez sur la page des détails du compte.
- Lorsque vous choisissez Enregistrer un compte, vous verrez une page d'inscription sur laquelle vous êtes invité à ajouter le **`AWSControlTowerExecution`** rôle au compte. Pour obtenir des instructions, voirAjoutez manuellement le rôle IAM requis à un rôle existant Compte AWS et inscrivez-le.
- Sélectionnez ensuite une unité d'organisation enregistrée dans la liste déroulante. Si le compte se trouve déjà dans une unité d'organisation enregistrée, cette liste affichera l'unité d'organisation.
- Choisissez Inscrire un compte.
- Vous verrez un rappel modal vous demandant d'ajouter le `AWSControlTowerExecution` rôle et de confirmer l'action.
- Choisissez S'inscrire.
- AWS Control Tower lance le processus d'inscription et vous êtes redirigé vers la page des détails du compte.

Causes courantes d'échec de l'inscription

- Pour inscrire un compte existant, le `AWSControlTowerExecution` rôle doit être présent dans le compte que vous inscrivez.
- Votre principal IAM peut ne pas disposer des autorisations nécessaires pour provisionner un compte.
- AWS Security Token Service (AWS STS) est désactivé Compte AWS dans votre région d'origine ou dans toute région prise en charge par AWS Control Tower.

- Vous êtes peut-être connecté à un compte qui doit être ajouté à Account Factory Portfolio in AWS Service Catalog. Le compte doit être ajouté pour que vous puissiez accéder à Account Factory afin que vous puissiez créer ou enregistrer un compte dans AWS Control Tower. Si l'utilisateur ou le rôle approprié n'est pas ajouté au portefeuille Account Factory, vous recevrez un message d'erreur lorsque vous tenterez d'ajouter un compte. Pour savoir comment accorder l'accès aux AWS Service Catalog portefeuilles, consultez la section Accorder l'accès aux utilisateurs.
- Vous pouvez être connecté en tant que racine.
- Le compte que vous essayez d'enregistrer comporte peut-être des AWS Config paramètres résiduels. En particulier, le compte peut disposer d'un enregistreur de configuration ou d'un canal de diffusion. Vous devez les supprimer ou les modifier AWS CLI avant de pouvoir créer un compte. Pour plus d'informations, consultez Inscrire des comptes disposant de ressources existantes AWS Config et Interagir avec AWS Control Tower l'utilisation AWS CloudShell.
- Si le compte appartient à une autre unité d'organisation dotée d'un compte de gestion, y compris une autre unité d'organisation AWS Control Tower, vous devez résilier le compte dans son unité d'organisation actuelle avant qu'il ne puisse rejoindre une autre unité d'organisation. Les ressources existantes doivent être supprimées dans l'unité d'organisation d'origine. Sinon, l'inscription échouera.
- Le provisionnement et l'inscription du compte échouent si les SCP de l'unité organisationnelle de destination ne vous permettent pas de créer toutes les ressources requises pour ce compte. Par exemple, un SCP dans votre unité d'organisation de destination peut bloquer la création de ressources sans certaines balises. Dans ce cas, le provisionnement ou l'inscription du compte échouent, car AWS Control Tower ne prend pas en charge le balisage des ressources. Pour obtenir de l'aide, contactez le représentant de votre compte, ou AWS Support.

Pour plus d'informations sur la façon dont AWS Control Tower utilise les rôles lorsque vous créez de nouveaux comptes ou que vous inscrivez des comptes existants, consultez la section Rôles et comptes.

> **Tip**
>
> Si vous ne pouvez pas confirmer qu'une unité existante Compte AWS répond aux conditions d'inscription, vous pouvez configurer une unité d'inscription et inscrire le compte dans cette unité d'organisation. Une fois l'inscription réussie, vous pouvez déplacer le compte vers l'unité d'organisation souhaitée. En cas d'échec de l'inscription, aucun autre compte ou unité d'organisation n'est affecté par l'échec.

Si vous avez des doutes quant à la compatibilité de vos comptes existants et de leurs configurations avec AWS Control Tower, vous pouvez suivre les bonnes pratiques recommandées dans la section suivante.

Recommandé : vous pouvez configurer une approche en deux étapes pour l'inscription de compte

- Tout d'abord, utilisez un pack de AWS Config conformité pour évaluer dans quelle mesure vos comptes peuvent être affectés par certains contrôles de l'AWS Control Tower. Pour déterminer dans quelle mesure l'inscription à AWS Control Tower peut affecter vos comptes, consultez Étendre la gouvernance d'AWS Control Tower à l'aide de packs de AWS Config conformité.
- Ensuite, vous pouvez inscrire le compte. Si les résultats de conformité sont satisfaisants, le chemin de migration est plus facile car vous pouvez inscrire le compte sans conséquences inattendues.
- Une fois votre évaluation terminée, si vous décidez de configurer une zone d'atterrissage AWS Control Tower, vous devrez peut-être supprimer le canal de AWS Config diffusion et l'enregistreur de configuration créés pour votre évaluation. Vous serez alors en mesure de configurer AWS Control Tower avec succès.

> **Note**
>
> Le pack de conformité fonctionne également dans les situations où les comptes sont situés dans des unités d'organisation enregistrées par AWS Control Tower, mais où les charges de travail sont exécutées dans des AWS régions qui ne sont pas prises en charge par AWS Control Tower. Vous pouvez utiliser le pack de conformité pour gérer les ressources des comptes qui existent dans les régions où AWS Control Tower n'est pas déployée.

Et si le compte ne répond pas aux prérequis ?

N'oubliez pas que, comme condition préalable, les comptes éligibles à l'inscription à la gouvernance d'AWS Control Tower doivent faire partie de la même organisation globale. Pour remplir cette condition préalable à l'enregistrement d'un compte, vous pouvez suivre ces étapes préparatoires pour transférer un compte dans la même organisation qu'AWS Control Tower.

Étapes préparatoires à l'intégration d'un compte dans la même organisation qu'AWS Control Tower

1. Supprimez le compte de son organisation existante. Vous devez fournir un mode de paiement distinct si vous utilisez cette approche.

2. Invitez le compte à rejoindre l'organisation AWS Control Tower. Pour plus d'informations, voir Inviter un AWS compte à rejoindre votre organisation dans le Guide de AWS Organizations l'utilisateur.
3. Acceptez l'invitation. Le compte apparaît à la racine de l'organisation. Cette étape déplace le compte vers la même organisation qu'AWS Control Tower et établit les SCP et la facturation consolidée.

> **Tip**
>
> Vous pouvez envoyer l'invitation à la nouvelle organisation avant que le compte ne soit supprimé de l'ancienne organisation. L'invitation sera en attente lorsque le compte sera officiellement retiré de son organisation existante.

Étapes pour remplir les autres conditions préalables :

1. Créez le `AWSControlTowerExecution` rôle nécessaire.
2. Supprimez le VPC par défaut. (Cette partie est facultative. AWS Control Tower ne modifie pas votre VPC par défaut existant.)
3. Supprimez ou modifiez tout enregistreur AWS Config de configuration ou canal de distribution existant via le AWS CLI ou AWS CloudShell. Pour plus d'informations, consultez Exemples de commandes AWS Config CLI pour l'état des ressources et Inscrire des comptes disposant de ressources existantes AWS Config

Une fois ces étapes préparatoires terminées, vous pouvez inscrire le compte dans AWS Control Tower. Pour plus d'informations, consultez Étapes pour créer un compte. Cette étape intègre le compte à la gouvernance complète d'AWS Control Tower.

Étapes facultatives pour déprovisionner un compte, afin qu'il puisse être inscrit et conserver sa pile

1. Pour conserver la AWS CloudFormation pile appliquée, supprimez l'instance de pile des ensembles de piles et choisissez Conserver les piles pour l'instance.
2. Résiliez le produit approvisionné par le AWS Service Catalog compte dans Account Factory. (Cette étape supprime uniquement le produit provisionné d'AWS Control Tower. Cela ne supprime pas le compte.)

3. Configurez le compte avec les informations de facturation nécessaires, comme c'est le cas pour tout compte n'appartenant pas à une organisation. Supprimez ensuite le compte de l'organisation. (Vous faites cela pour que le compte ne soit pas pris en compte dans le total de votre AWS Organizations quota.)
4. Nettoyez le compte s'il reste des ressources, puis fermez-le en suivant les étapes de fermeture du compte indiquéesAnnuler la gestion d'un compte.
5. Si vous avez une unité d'organisation suspendue avec des commandes définies, vous pouvez y déplacer le compte au lieu de passer à l'étape 1.

Exemples de commandes AWS Config CLI pour l'état des ressources

Voici quelques exemples de commandes AWS Config CLI que vous pouvez utiliser pour déterminer l'état de votre enregistreur de configuration et de votre canal de diffusion.

Commandes d'affichage :

- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-recorders`

La réponse normale est quelque chose comme `"name": "default"`

Commandes de suppression :

- `aws configservice stop-configuration-recorder --configuration-recorder-name` *`NAME-FROM-DESCRIBE-OUTPUT`*
- `aws configservice delete-delivery-channel --delivery-channel-name` *`NAME-FROM-DESCRIBE-OUTPUT`*
- `aws configservice delete-configuration-recorder --configuration-recorder-name` *`NAME-FROM-DESCRIBE-OUTPUT`*

Ajoutez manuellement le rôle IAM requis à un rôle existant Compte AWS et inscrivez-le

Si vous avez déjà configuré la zone de landing de votre AWS Control Tower, vous pouvez commencer à inscrire les comptes de votre organisation dans une unité d'organisation enregistrée

auprès d'AWS Control Tower. Si vous n'avez pas configuré votre zone de landing zone, suivez les étapes décrites dans le guide de l'utilisateur d'AWS Control Tower sur Getting Started, étape 2. Une fois la zone de landing zone prête, suivez les étapes ci-dessous pour intégrer manuellement les comptes existants à la gouvernance d'AWS Control Tower.

N'oubliez pas de consulter ce qui est Conditions préalables à l'inscription indiqué précédemment dans ce chapitre.

Avant de créer un compte auprès d'AWS Control Tower, vous devez autoriser AWS Control Tower à gérer ce compte. Pour ce faire, vous allez ajouter un rôle disposant d'un accès complet au compte, comme indiqué dans les étapes suivantes. Ces étapes doivent être effectuées pour chaque compte que vous inscrivez.

Pour chaque compte :

Étape 1 : Connectez-vous avec un accès administrateur au compte de gestion de l'organisation qui contient actuellement le compte que vous souhaitez inscrire.

Par exemple, si vous avez créé ce compte à partir de AWS Organizations et que vous utilisez un rôle IAM entre comptes pour vous connecter, vous pouvez suivre les étapes suivantes :

1. Connectez-vous au compte de gestion de votre organisation.
2. Accédez à AWS Organizations.
3. Sous Comptes, sélectionnez le compte que vous souhaitez enregistrer et copiez son numéro de compte.
4. Ouvrez le menu déroulant du compte dans la barre de navigation supérieure et choisissez Changer de rôle.
5. Sur le formulaire Switch role, renseignez les champs suivants :
   - Sous Compte, entrez le numéro de compte que vous avez copié.
   - Sous Rôle, entrez le nom du rôle IAM qui permet l'accès entre comptes à ce compte. Le nom de ce rôle a été défini lors de la création du compte. Si vous n'avez pas spécifié de nom de rôle lors de la création du compte, entrez le nom de rôle par défaut,`OrganizationAccountAccessRole`.
6. Choisissez Changer de rôle.
7. Vous devriez maintenant être connecté au compte en AWS Management Console tant qu'enfant.
8. Lorsque vous avez terminé, restez dans le compte enfant pour la prochaine étape de la procédure.

9. Prenez note de l'identifiant du compte de gestion, car vous devrez le saisir à l'étape suivante.

Étape 2 : autorisez AWS Control Tower à gérer le compte.

1. Accédez à IAM.
2. Accédez à Rôles.
3. Sélectionnez Créer un rôle.
4. Lorsque vous êtes invité à sélectionner le service auquel le rôle est destiné, choisissez Politique de confiance personnalisée.
5. Copiez l'exemple de code présenté ici et collez-le dans le document de politique. Remplacez la chaîne *`Management Account ID`*par l'identifiant de compte de gestion réel de votre compte de gestion. Voici la politique à coller :

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
      "Effect":"Allow",
      "Principal":{
         "AWS": "arn:aws:iam::Management Account ID:root"
         },
         "Action": "sts:AssumeRole",
         "Condition": {}
      }
   ]
  }
```

6. Lorsque vous êtes invité à joindre des politiques, sélectionnez AdministratorAccess.
7. Choisissez Suivant : balises.
8. Vous pouvez voir un écran facultatif intitulé Ajouter des balises. Ignorez cet écran pour le moment en choisissant Next:Review
9. Sur l'écran de révision, dans le champ Nom du rôle, entrez`AWSControlTowerExecution`.
10. Entrez une brève description dans le champ Description, telle que Autorise l'accès complet au compte pour l'inscription.
11. Sélectionnez Créer un rôle.

Étape 3 : Enregistrez le compte en le transférant dans une unité d'organisation enregistrée et vérifiez l'inscription.

Après avoir configuré les autorisations nécessaires en créant le rôle, suivez ces étapes pour enregistrer le compte et vérifier l'inscription.

1. Connectez-vous à nouveau en tant qu'administrateur et accédez à AWS Control Tower.
2. Enregistrez le compte.
   - Sur la page Organisation d'AWS Control Tower, sélectionnez votre compte, puis choisissez S'inscrire dans le menu déroulant Actions en haut à droite.
   - Suivez les étapes pour créer un compte individuel, comme indiqué sur la Étapes pour créer un compte page.
3. Vérifiez l'inscription.
   - Dans AWS Control Tower, choisissez Organization dans le menu de navigation de gauche.
   - Recherchez le compte que vous avez récemment ouvert. Son état initial indiquera le statut d'inscription.
   - Lorsque l'état passe à Inscrit, le transfert a été effectué avec succès.

Pour poursuivre ce processus, connectez-vous à chaque compte de votre organisation que vous souhaitez inscrire à AWS Control Tower. Répétez les étapes préalables et les étapes d'inscription pour chaque compte.

Inscription automatique des AWS Organizations comptes

Vous pouvez utiliser la méthode d'inscription décrite dans un billet de blog intitulé Enroll existing AWS accounts into AWS Control Tower pour inscrire vos AWS Organizations comptes dans AWS Control Tower par le biais d'un processus programmatique.

Le modèle YAML suivant peut vous aider à créer le rôle requis dans un compte, afin qu'il puisse être inscrit par programme.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure the AWSControlTowerExecution role to enable use of your
  account as a target account in AWS CloudFormation StackSets.
Parameters:
  AdministratorAccountId:
```

```
    Type: String
    Description: AWS Account Id of the administrator account (the account in which
      StackSets will be created).
    MaxLength: 12
    MinLength: 12
Resources:
  ExecutionRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: AWSControlTowerExecution
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              AWS:
                - !Ref AdministratorAccountId
            Action:
              - sts:AssumeRole
      Path: /
      ManagedPolicyArns:
        - !Sub arn:${AWS::Partition}:iam::aws:policy/AdministratorAccess
```

Inscrire des comptes disposant de ressources existantes AWS Config

Cette rubrique explique step-by-step comment inscrire des comptes dotés de AWS Config ressources existantes. Pour obtenir des exemples de vérification de vos ressources existantes, consultezExemples de commandes AWS Config CLI pour l'état des ressources.

> **Note**
>
> Si vous envisagez d'intégrer AWS des comptes existants dans AWS Control Tower en tant que comptes d'audit et d'archivage de journaux, et si ces comptes disposent de AWS Config ressources existantes, vous devez supprimer complètement les AWS Config ressources existantes avant de pouvoir inscrire ces comptes dans AWS Control Tower à cette fin. Pour les comptes qui ne sont pas destinés à devenir des comptes d'archive d'audit et de journal, vous pouvez modifier les ressources Config existantes.

Exemples de AWS Config ressources

Voici quelques types de AWS Config ressources que votre compte pourrait déjà avoir. Ces ressources devront peut-être être modifiées afin que vous puissiez inscrire votre compte dans AWS Control Tower.

- AWS Config enregistreur
- AWS Config canal de livraison
- AWS Config autorisation d'agrégation

Hypothèses

- Vous avez déployé une zone de landing zone AWS Control Tower
- Votre compte n'est pas encore inscrit à AWS Control Tower.
- Votre compte possède au moins une AWS Config ressource préexistante dans au moins l'une des régions AWS Control Tower régies par le compte de gestion.
- Votre compte n'est pas le compte de gestion d'AWS Control Tower.
- Votre compte n'est pas en situation de dérive en matière de gouvernance.

Pour consulter un blog qui décrit une approche automatisée pour inscrire des comptes avec des AWS Config ressources existantes, consultez Automatiser l'inscription de comptes avec des AWS Config ressources existantes dans AWS Control Tower. Vous pourrez soumettre un seul ticket d'assistance pour tous les comptes que vous souhaitez inscrire, comme décrit dans Étape 1 : contactez le support client avec un ticket, pour ajouter le compte à la liste d'autorisation d'AWS Control Tower ce qui suit.

Limites

- Le compte ne peut être inscrit qu'en utilisant le flux de travail AWS Control Tower pour étendre la gouvernance.
- Si les ressources sont modifiées et créent une dérive sur le compte, AWS Control Tower ne les met pas à jour.
- AWS Config les ressources des régions qui ne sont pas régies par AWS Control Tower ne sont pas modifiées.

> **Note**
>
> Si vous essayez d'inscrire un compte qui possède des ressources Config existantes, sans que le compte soit ajouté à la liste d'autorisation, l'inscription échouera. Par la suite, si vous essayez par la suite d'ajouter ce même compte à la liste d'autorisation, AWS Control Tower ne pourra pas vérifier que le compte est correctement configuré. Vous devez déprovisionner le compte auprès d'AWS Control Tower avant de pouvoir demander la liste d'autorisations, puis l'inscrire. Si vous déplacez le compte uniquement vers une autre unité d'organisation AWS Control Tower, cela entraîne une dérive de la gouvernance, ce qui empêche également l'ajout du compte à la liste des autorisations.

Ce processus comporte 5 étapes principales.

1. Ajoutez le compte à la liste d'autorisation d'AWS Control Tower.
2. Créez un nouveau rôle IAM dans le compte.
3. Modifiez les AWS Config ressources préexistantes.
4. Créez AWS Config des ressources dans AWS des régions où elles n'existent pas.
5. Enregistrez le compte auprès d'AWS Control Tower.

Avant de poursuivre, tenez compte des attentes suivantes concernant ce processus.

- AWS Control Tower ne crée aucune AWS Config ressource sur ce compte.
- Après l'inscription, les contrôles d'AWS Control Tower protègent automatiquement les AWS Config ressources que vous avez créées, y compris le nouveau rôle IAM.
- Si des modifications sont apportées aux AWS Config ressources après l'inscription, celles-ci doivent être mises à jour pour s'aligner sur les paramètres d'AWS Control Tower avant de pouvoir réinscrire le compte.

Étape 1 : contactez le support client avec un ticket, pour ajouter le compte à la liste d'autorisation d'AWS Control Tower

Incluez cette phrase dans l'objet de votre billet :

Inscrire des comptes disposant de AWS Config ressources existantes dans AWS Control Tower

Incluez les informations suivantes dans le corps de votre billet :

- Numéro de compte de gestion
- Numéros de compte des comptes membres disposant de AWS Config ressources existantes
- La région d'origine que vous avez sélectionnée pour la configuration d'AWS Control Tower

> **Note**
>
> Le délai requis pour ajouter votre compte à la liste d'autorisation est de 2 jours ouvrables.

Étape 2 : créer un nouveau rôle IAM dans le compte membre

1. Ouvrez la AWS CloudFormation console du compte membre.
2. Créez une nouvelle pile à l'aide du modèle suivant

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config

Resources:
  CustomerCreatedConfigRecorderRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: aws-controltower-ConfigRecorderRole-customer-created
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AWS_ConfigRole
        - arn:aws:iam::aws:policy/ReadOnlyAccess
```

3. Entrez le nom de la pile en tant que CustomerCreatedConfigRecorderRoleForControltour
4. Créez la pile.

> **Note**
>
> Tout SCP que vous créez doit exclure un `aws-controltower-ConfigRecorderRole*` rôle. Ne modifiez pas les autorisations qui limitent la capacité des AWS Config règles à effectuer des évaluations.
> Suivez ces directives afin de ne pas recevoir de message `AccessDeniedException` lorsque vous avez des SCP qui vous empêchent `aws-controltower-ConfigRecorderRole*` d'appeler Config.

Étape 3 : Identifier les AWS régions disposant de ressources préexistantes

Pour chaque région gouvernée (régie par AWS Control Tower) du compte, identifiez et notez les régions qui possèdent au moins l'un des types de AWS Config ressources existants présentés précédemment.

Étape 4 : Identifier les AWS régions dépourvues de AWS Config ressources

Pour chaque région gouvernée (régie par AWS Control Tower) dans le compte, identifiez et notez les régions dans lesquelles il n'existe aucune AWS Config ressource du type illustré précédemment.

Étape 5 : Modifier les ressources existantes dans chaque AWS région

Pour cette étape, les informations suivantes sont nécessaires concernant la configuration de votre AWS Control Tower.

- `LOGGING_ACCOUNT`- l'identifiant du compte de journalisation
- `AUDIT_ACCOUNT`- l'identifiant du compte d'audit
- `IAM_ROLE_ARN`- l'ARN du rôle IAM créé à l'étape 1
- `ORGANIZATION_ID`- l'identifiant de l'organisation pour le compte de gestion
- `MEMBER_ACCOUNT_NUMBER`- le compte membre en cours de modification
- `HOME_REGION`- la région d'origine pour la configuration d'AWS Control Tower.

Modifiez chaque ressource existante en suivant les instructions données dans les sections 5a à 5c, qui suivent.

Étape 5a. AWS Config ressources pour les enregistreurs

Il ne peut y avoir qu'un seul AWS Config enregistreur par AWS région. S'il en existe un, modifiez les paramètres comme indiqué. Remplacez l'article `GLOBAL_RESOURCE_RECORDING` par true dans votre région d'origine. Remplacez l'élément par false pour les autres régions où un AWS Config enregistreur existe.

- Nom : DON'T CHANGE
- ROLearn : `IAM_ROLE_ARN`
  - RecordingGroup:
  - AllSupported: vrai
  - IncludeGlobalResourceTypes: `GLOBAL_RESOURCE_RECORDING`
  - ResourceTypes: Vide

Cette modification peut être effectuée via la AWS CLI à l'aide de la commande suivante. Remplacez la chaîne `RECORDER_NAME` par le nom de l' AWS Config enregistreur existant.

```
aws configservice put-configuration-recorder --configuration-recorder
  name=RECORDER_NAME,roleARN=arn:aws:iam::MEMBER_ACCOUNT_NUMBER:role/
aws-controltower-ConfigRecorderRole-customer-created --recording-group
 allSupported=true,includeGlobalResourceTypes=GLOBAL_RESOURCE_RECORDING --
region CURRENT_REGION
```

Étape 5b. Modifier les ressources du canal de AWS Config distribution

Il ne peut exister qu'un seul canal de AWS Config distribution par région. S'il en existe un autre, modifiez les paramètres comme indiqué.

- Nom : DON'T CHANGE
- ConfigSnapshotDeliveryProperties: TwentyFour _Heures
- S3 BucketName : nom du compartiment de journalisation indiqué dans le compte de journalisation AWS Control Tower

  `aws-controltower-logs-LOGGING_ACCOUNT-HOME_REGION`
- S3 KeyPrefix : IDENTIFIANT DE *L'ORGANISATION*

- SnsTopicARN : l'ARN de la rubrique SNS issu du compte d'audit, au format suivant :

  `arn:aws:sns:CURRENT_REGION:AUDIT_ACCOUNT:aws-controltower-AllConfigNotifications`

Cette modification peut être effectuée via la AWS CLI à l'aide de la commande suivante. Remplacez la chaîne *DELIVERY_CHANNEL_NAME* par le nom de l' AWS Config enregistreur existant.

```
aws configservice put-delivery-channel --delivery-channel
 name=DELIVERY_CHANNEL_NAME,s3BucketName=aws-controltower-
logs-LOGGING_ACCOUNT_ID-
HOME_REGION,s3KeyPrefix="ORGANIZATION_ID",configSnapshotDeliveryProperties={deliveryFrequency=T
controltower-AllConfigNotifications --region CURRENT_REGION
```

Étape 5c. Modifier les ressources AWS Config d'autorisation d'agrégation

Plusieurs autorisations d'agrégation peuvent exister par région. AWS Control Tower nécessite une autorisation d'agrégation qui indique que le compte d'audit est le compte autorisé, et que la région d'origine d'AWS Control Tower est la région autorisée. S'il n'existe pas, créez-en un nouveau avec les paramètres suivants :

- AuthorizedAccountId: ID du compte d'audit
- AuthorizedAwsRegion: région d'origine pour la configuration d'AWS Control Tower

Cette modification peut être effectuée via la AWS CLI à l'aide de la commande suivante :

`aws configservice put-aggregation-authorization --authorized-account-id AUDIT_ACCOUNT_ID --authorized-aws-region HOME_REGION --region CURRENT_REGION`

Étape 6 : créer des ressources là où elles n'existent pas, dans les régions régies par AWS Control Tower

Révisez le AWS CloudFormation modèle de manière à ce que le IncludeGlobalResourcesTypesparamètre ait la valeur voulue dans votre région

d'origine`GLOBAL_RESOURCE_RECORDING`, comme indiqué dans l'exemple suivant. Mettez également à jour les champs obligatoires dans le modèle, comme indiqué dans cette section.

Remplacez l'article `GLOBAL_RESOURCE_RECORDING` par true dans votre région d'origine. Remplacez l'élément par false pour les autres régions où un AWS Config enregistreur existe.

1. Accédez à la AWS CloudFormation console du compte de gestion.
2. Créez-en un nouveau StackSet avec ce nom CustomerCreatedConfigResourcesForControlTower.
3. Copiez et mettez à jour le modèle suivant :

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config
Resources:
  CustomerCreatedConfigRecorder:
    Type: AWS::Config::ConfigurationRecorder
    Properties:
      Name: aws-controltower-BaselineConfigRecorder-customer-created
      RoleARN: !Sub arn:aws:iam::${AWS::AccountId}:role/aws-controltower-
ConfigRecorderRole-customer-created
      RecordingGroup:
        AllSupported: true
        IncludeGlobalResourceTypes: GLOBAL_RESOURCE_RECORDING
        ResourceTypes: []
  CustomerCreatedConfigDeliveryChannel:
    Type: AWS::Config::DeliveryChannel
    Properties:
      Name: aws-controltower-BaselineConfigDeliveryChannel-customer-created
      ConfigSnapshotDeliveryProperties:
        DeliveryFrequency: TwentyFour_Hours
      S3BucketName: aws-controltower-logs-LOGGING_ACCOUNT-HOME_REGION
      S3KeyPrefix: ORGANIZATION_ID
      SnsTopicARN: !Sub arn:aws:sns:${AWS::Region}:AUDIT_ACCOUNT:aws-controltower-
AllConfigNotifications
  CustomerCreatedAggregationAuthorization:
    Type: "AWS::Config::AggregationAuthorization"
    Properties:
      AuthorizedAccountId: AUDIT_ACCOUNT
      AuthorizedAwsRegion: HOME_REGION
```

Mettez à jour le modèle avec les champs obligatoires :

a. *Dans le BucketName champ **S3**, remplacez LOGGING_ACCOUNT_ID et HOME_REGION*

b. Dans le KeyPrefix champ S3, remplacez le *ORGANIZATION_ID*

c. Dans le champ SnsTopicARN, remplacez le *AUDIT_ACCOUNT*

d. Dans le AuthorizedAccountIdchamp, remplacez le *AUDIT_ACCOUNT*

e. Dans le AuthorizedAwsRegionchamp, remplacez le *HOME_REGION*

4. Lors du déploiement sur la AWS CloudFormation console, ajoutez le numéro de compte du membre.
5. Ajoutez les AWS régions identifiées à l'étape 4.
6. Déployez le stack set.

Étape 7 : enregistrer l'unité d'organisation auprès d'AWS Control Tower

Dans le tableau de bord AWS Control Tower, enregistrez l'unité d'organisation.

> **Note**
>
> Le flux de travail d'inscription du compte échouera pour cette tâche. Vous devez choisir Enregistrer l'unité d'organisation ou Réenregistrer l'unité d'organisation.

Provisionner et gérer des comptes avec Account Factory

Ce chapitre inclut une présentation et des procédures de mise en service de nouveaux comptes membres dans une zone de landing zone AWS Control Tower avec Account Factory.

Autorisations pour configurer et approvisionner des comptes

L'AWS Control Tower Account Factory permet aux administrateurs et aux utilisateurs du cloud AWS IAM Identity Center de créer des comptes dans votre zone de landing zone. Par défaut, les utilisateurs d'IAM Identity Center qui fournissent des comptes doivent faire partie du `AWSAccountFactory` groupe ou du groupe de gestion.

> **Note**
>
> Faites preuve de prudence lorsque vous travaillez à partir du compte de gestion, comme vous le feriez lorsque vous utilisez un compte doté d'autorisations au sein de votre organisation.

Le compte de gestion AWS Control Tower entretient une relation de confiance avec le `AWSControlTowerExecution` rôle, ce qui permet de configurer le compte à partir du compte de gestion, y compris une configuration automatique du compte. Pour plus d'informations sur le `AWSControlTowerExecution` rôle, consultez la section Rôles et comptes.

> **Note**
>
> Pour inscrire un utilisateur existant Compte AWS dans AWS Control Tower, le `AWSControlTowerExecution` rôle doit être activé sur ce compte. Pour de plus amples informations sur l'inscription d'un compte existant, consultez Inscrire un existant Compte AWS.

Pour plus d'informations sur les autorisations, consultez Autorisations requises pour les comptes.

Provisionner des comptes avec AWS Service Catalog Account Factory

La procédure suivante décrit comment créer et configurer des comptes en tant qu'utilisateur dans IAM Identity Center via AWS Service Catalog. Cette procédure est également appelée provisionnement de compte avancé ou provisionnement manuel de compte. Vous pouvez éventuellement provisionner des comptes par programmation, avec la AWS CLI ou avec AWS Control Tower Account Factory for Terraform (AFT). Vous pouvez peut-être configurer des comptes personnalisés dans la console si vous avez déjà configuré des plans personnalisés. Pour plus d'informations sur la personnalisation, consultezPersonnalisez les comptes avec Account Factory Customization (AFC).

Pour approvisionner des comptes individuellement dans Account Factory, en tant qu'utilisateur

1. Connectez-vous à partir de l'URL de votre portail utilisateur.
2. Dans Vos applications, sélectionnez AWS Compte.
3. Dans la liste des comptes, choisissez l'identifiant de compte de votre compte de gestion. Cet identifiant peut également comporter une étiquette, par exemple (Gestion).

4. Dans AWSServiceCatalogEndUserAccess, choisissez Console de gestion. Cela ouvre le compte AWS Management Console pour cet utilisateur.
5. Assurez-vous d'avoir sélectionné la bonne option Région AWS pour le provisionnement des comptes, qui doit être votre région AWS Control Tower.
6. Recherchez et choisissez Service Catalog pour ouvrir la console Service Catalog.
7. Dans le volet de navigation, sélectionnez Products.
8. Sélectionnez AWS Control Tower Account Factory, puis cliquez sur le bouton Lancer le produit. Cette action lance l'assistant pour le provisionnement d'un nouveau compte.
9. Renseignez les informations et gardez à l'esprit les points suivants :
   - Le SSO UserEmail peut être une nouvelle adresse e-mail ou l'adresse e-mail associée à un utilisateur IAM Identity Center existant. Quel que soit votre choix, cet utilisateur aura un accès administratif au compte que vous mettez en service.
   - AccountEmailII doit s'agir d'une adresse e-mail qui n'est pas déjà associée à un Compte AWS. Si vous avez utilisé une nouvelle adresse e-mail dans le SSO UserEmail, vous pouvez utiliser cette adresse e-mail ici.
10. Ne définissez pas TagOptionset n'activez pas les notifications, sinon le compte risque de ne pas être approvisionné. Lorsque vous avez terminé, choisissez Launch product.
11. Vérifiez les paramètres de votre compte, puis choisissez Launch (Lancer). Ne créez pas de plan de ressources, sinon le compte ne pourra pas être approvisionné.
12. Votre compte est en cours de mise en service. Cette opération peut prendre quelques minutes. Vous pouvez actualiser la page pour mettre à jour les informations de statut affichées.

> **Note**
>
> Jusqu'à cinq comptes peuvent être provisionnés à la fois.

Considérations relatives à la gestion des comptes dans Account Factory

Vous pouvez mettre à jour, dégérer et fermer les comptes que vous créez et approvisionnez via Account Factory. Vous pouvez recycler les comptes en mettant à jour les paramètres utilisateur des comptes que vous souhaitez réutiliser. Vous pouvez également modifier l'unité organisationnelle (UO) d'un compte.

> **Note**
>
> Lors de la mise à jour d'un produit provisionné associé à un compte vendu par Account Factory, si vous spécifiez une nouvelle adresse e-mail utilisateur pour AWS IAM Identity Center, AWS Control Tower crée un nouvel utilisateur dans IAM Identity Center. Le compte créé précédemment n'est pas supprimé. Pour plus d'informations sur la suppression de l'ancienne adresse e-mail de l'utilisateur IAM Identity Center d'IAM Identity Center, consultez la section Désactivation d'un utilisateur.

Mettez à jour et déplacez les comptes Account Factory avec AWS Control Tower ou avec AWS Service Catalog

Le moyen le plus simple de mettre à jour un compte inscrit consiste à utiliser la console AWS Control Tower. Les mises à jour de compte individuelles sont utiles pour résoudre les problèmes de dérive, tels queDéplacement du compte membre. Les mises à jour du compte sont également requises dans le cadre d'une mise à jour complète de la zone d'atterrissage.

Si vous déplacez un compte d'une unité organisationnelle (UO) à une autre, n'oubliez pas que les contrôles appliqués par la nouvelle UO peuvent être différents de ceux de l'ancienne UO. Assurez-vous que les contrôles de la nouvelle unité d'organisation répondent aux exigences de votre politique pour le compte.

Comportement de contrôle lorsque des comptes sont déplacés entre UOS

Lorsque vous déplacez un compte entre des unités d'organisation, les commandes de l'unité d'organisation de destination sont appliquées à compte. Toutefois, les contrôles appliqués au compte depuis l'ancienne unité d'organisation ne le sont pas supprimé. Le comportement exact des commandes est spécifique à la mise en œuvre du contrôles actifs sur l'unité d'organisation précédente et sur l'unité d'organisation de destination.

- Pour les contrôles implémentés avec AWS Config des règles : les contrôles de l'unité d'organisation précédente ne sont pas supprimés. Ces commandes doivent être supprimées manuellement.
- Pour les contrôles mis en œuvre avec les SCP : les contrôles basés sur les SCP de l'UO précédente sont supprimé. Les contrôles basés sur le SCP pour l'UO de destination entrent en vigueur sur ce compte.

- Pour les contrôles implémentés avec AWS CloudFormation des hooks : Ce comportement dépend de l'état des commandes dans la nouvelle unité d'organisation.
  - Si aucune commande basée sur un crochet n'est active dans l'unité d'organisation de destination : L'ancien les contrôles restent actifs pour le compte déplacé, sauf si vous les supprimez manuellement.
  - Si l'unité d'organisation de destination possède des commandes de crochet actives : les anciennes commandes sont supprimé et les commandes de l'unité d'organisation de destination sont appliquées au compte.

Mettre à jour le compte dans la console

Pour mettre à jour un compte dans la console AWS Control Tower

1. Une fois connecté à AWS Control Tower, accédez à la page Organisation.
2. Dans la liste des UO et des comptes, sélectionnez le nom du compte que vous souhaitez mettre à jour. Les comptes disponibles pour la mise à jour affichent le statut Mise à jour disponible.
3. Vous verrez ensuite la page des détails du compte que vous avez sélectionné.
4. Dans le coin supérieur droit, choisissez Mettre à jour le compte.

Mettre à jour le produit approvisionné

La procédure suivante vous explique comment mettre à jour votre compte dans Account Factory ou le déplacer vers une nouvelle unité d'organisation, en mettant à jour le produit provisionné du compte dans Service Catalog.

Pour mettre à jour un compte Account Factory ou modifier son unité d'organisation via Service Catalog

1. Connectez-vous à la console AWS de gestion et ouvrez-la à l' AWS Service Catalog adresse https://console.aws.amazon.com/servicecatalog/.

> **Note**
>
> Vous devez vous connecter en tant qu'utilisateur autorisé à fournir de nouveaux produits dans Service Catalog (par exemple, un utilisateur du IAM Identity Center dans un `AWSAccountFactory` ou plusieurs `AWSServiceCatalogAdmins` groupes).

2. Dans le volet de navigation, choisissez Provisioning, puis Provisioned products.
3. Pour chacun des comptes membres répertoriés, effectuez les étapes suivantes pour mettre à jour tous les comptes membres :

   a. Sélectionnez un compte membre. Vous êtes dirigé vers la page des détails du produit provisionné pour ce compte.

   b. Sur la page des détails du produit provisionné, choisissez l'onglet Événements.

   c. Notez les paramètres suivants :

      - SSO UserEmail (disponible dans les détails du produit provisionné)
      - AccountEmail(Disponible dans les détails du produit approvisionné)
      - SSO UserFirstName (disponible dans le centre d'identité IAM)
      - SSOU SerLastName (disponible dans le centre d'identité IAM)
      - AccountName(Disponible dans le centre d'identité IAM)

   d. À partir de Actions, choisissez Update (Mettre à jour).

   e. Cliquez sur le bouton en regard de la version du produit que vous souhaitez mettre à jour, puis choisissez Suivant.

   f. Fournissez les valeurs de paramètres qui ont été mentionnées précédemment.

      - Si vous souhaitez conserver l'unité d'organisation existante ManagedOrganizationalUnit, choisissez l'unité d'organisation dans laquelle se trouvait déjà le compte.
      - Si vous souhaitez migrer le compte vers une nouvelle unité d'organisation ManagedOrganizationalUnit, choisissez la nouvelle unité d'organisation pour le compte.

      Un administrateur central du cloud peut trouver ces informations dans la console AWS Control Tower, sur la page Organisation.

   g. Choisissez Suivant.

   h. Examinez vos modifications, puis choisissez Update (Mettre à jour). Ce processus peut prendre quelques minutes par compte.

Modifier l'adresse e-mail d'un compte inscrit

Pour modifier l'adresse e-mail d'un compte de membre inscrit dans AWS Control Tower, suivez la procédure décrite dans cette section.

> **Note**
>
> La procédure suivante ne vous permet pas de modifier l'adresse e-mail d'un compte de gestion, d'un compte d'archivage des journaux ou d'un compte d'audit. Pour plus d'informations à ce sujet, consultez Comment modifier l'adresse e-mail associée à mon AWS compte ? ou contactez le AWS Support.

Pour modifier l'adresse e-mail d'un compte créé par AWS Control Tower

1. Récupérez le mot de passe de l'utilisateur root pour le compte. Vous pouvez suivre les étapes décrites dans l'article Comment récupérer un mot de AWS passe perdu ou oublié ?
2. Connectez-vous au compte avec le mot de passe de l'utilisateur root.
3. Modifiez l'adresse e-mail comme vous le feriez pour n'importe quelle autre Compte AWS adresse et attendez que le changement soit reflété AWS Organizations. Il se peut que la mise à jour du changement d'adresse e-mail soit retardée.
4. Mettez à jour le produit fourni dans Service Catalog à l'aide de l'adresse e-mail qui appartenait précédemment au compte. Le processus de mise à jour du produit approvisionné comprend l'association de la nouvelle adresse e-mail au produit approvisionné. Ainsi, le changement d'adresse e-mail prend effet dans AWS Control Tower. Utilisez la nouvelle adresse e-mail pour les mises à jour des produits approvisionnés ultérieurement.

Pour modifier le mot de passe ou l'adresse e-mail d'un compte de membre que vous avez créé AWS Organizations, consultez la section Accès à un compte de membre en tant qu'utilisateur root dans le guide de AWS Organizations l'utilisateur.

Modifier le nom d'un compte inscrit

Suivez la procédure décrite dans cette section pour modifier le nom d'un compte AWS Control Tower inscrit.

> **Note**
>
> Pour modifier le nom d'un compte AWS administrateur, vous devez disposer des autorisations d'administrateur et être connecté en tant qu'utilisateur root du compte.

Pour modifier le nom d'un compte créé par AWS Control Tower

1. Récupérez le mot de passe root du compte. Vous pouvez suivre les étapes décrites dans cet article, Comment récupérer un mot de AWS passe perdu ou oublié ?
2. Connectez-vous au compte à l'aide du mot de passe root.
3. Dans la AWS Billing console, accédez à la page des paramètres du compte.
4. Modifiez le nom dans les paramètres du compte, comme vous le feriez pour tout autre nom Compte AWS.
5. AWS Control Tower se met automatiquement à jour pour refléter le changement de nom. Cette mise à jour ne sera pas reflétée dans le produit fourni dans AWS Service Catalog.

Configurer Account Factory avec les paramètres d'Amazon Virtual Private Cloud

Account Factory vous permet de créer des bases de référence et des options de configuration préapprouvées pour les comptes de votre organisation. Vous pouvez configurer et mettre en service de nouveaux comptes via AWS Service Catalog.

Sur la page Account Factory, vous pouvez consulter la liste des unités organisationnelles (UO) ainsi que le statut de leur liste d'autorisation. Par défaut, toutes les unités d'organisation figurent sur la liste d'autorisation, ce qui signifie que les comptes peuvent être mis en service sous elles. Vous pouvez désactiver certaines unités d'organisation pour le provisionnement des comptes via AWS Service Catalog.

Vous pouvez consulter les options de configuration Amazon VPC disponibles pour vos utilisateurs finaux lorsqu'ils fournissent de nouveaux comptes.

Pour configurer les paramètres Amazon VPC dans Account Factory

1. En tant qu'administrateur central du cloud, connectez-vous à la console AWS Control Tower avec les autorisations d'administrateur du compte de gestion.
2. Sur le côté gauche du tableau de bord, sélectionnez Account Factory pour accéder à la page de configuration du réseau Account Factory. Vous pouvez y voir les paramètres réseau par défaut affichés. Pour modifier, sélectionnez Modifier et consultez la version modifiable des paramètres de configuration réseau de votre Account Factory.
3. Vous pouvez modifier chaque champ des paramètres par défaut selon vos besoins. Choisissez les options de configuration VPC que vous souhaitez définir pour tous les nouveaux comptes

Account Factory que vos utilisateurs finaux sont susceptibles de créer, puis entrez vos paramètres dans les champs.

- Choisissez désactivé ou activé pour créer un sous-réseau public dans Amazon VPC. Par défaut, le sous-réseau est accessible sur Internet.

> **Note**
>
> Si vous définissez la configuration du VPC Account Factory de sorte que les sous-réseaux publics soient activés lors du provisionnement d'un nouveau compte, Account Factory configure Amazon VPC pour créer une passerelle NAT. Vous serez facturé pour votre utilisation par Amazon VPC. Pour de plus amples informations, veuillez consulter Tarification VPC.

- Choisissez le nombre maximum de sous-réseaux privés dans Amazon VPC dans la liste. Par défaut, 1 est sélectionné. Le nombre maximum de sous-réseaux privés autorisés est de 2 par zone de disponibilité.
- Entrez la plage d'adresses pour la création de vos VPC de compte. La valeur doit utiliser le format d'un bloc CIDR, (par exemple, `172.31.0.0/16`). Ce bloc CIDR fournit la gamme globale d'adresses IP de sous-réseau pour le VPC créé par Account Factory pour votre compte. Au sein de votre VPC, les sous-réseaux sont attribués automatiquement à partir de la plage que vous spécifiez, et ils ont une taille égale. Par défaut, les sous-réseaux au sein de votre VPC ne se chevauchent pas. Toutefois, les plages d'adresses IP de sous-réseau dans les VPC de tous vos comptes provisionnés peuvent se chevaucher.
- Choisissez une région ou toutes les régions pour la création d'un VPC lorsqu'un compte est mis en service. Par défaut, toutes les régions disponibles sont sélectionnées.
- Dans la liste, choisissez le nombre de zones de disponibilité pour configurer des sous-réseaux pour chaque VPC. Le nombre par défaut et recommandé est de trois.
- Choisissez Enregistrer.

Vous pouvez configurer ces options de configuration pour créer de nouveaux comptes qui n'incluent pas de VPC. Consultez la procédure.

Annuler la gestion d'un compte

Si vous avez créé un compte dans Account Factory ou que vous en avez inscrit un Compte AWS, et que vous ne souhaitez plus que le compte soit géré par AWS Control Tower dans une zone de landing zone, vous pouvez annuler la gestion du compte depuis la console AWS Control Tower.

Lorsque vous annulez la gestion d'un compte AWS Control Tower, toutes les ressources mises en service par AWS Control Tower sont supprimées, y compris les plans. Le compte est déplacé de n'importe quelle unité d'organisation AWS Control Tower vers la zone racine. Le compte ne fait plus partie d'une unité d'organisation enregistrée et n'est plus soumis aux SCP d'AWS Control Tower. Vous pouvez fermer le compte via AWS Organizations.

L'annulation de la gestion d'un compte peut également être effectuée dans la console Service Catalog par un utilisateur d'IAM Identity Center du `AWSAccountFactory` groupe, en mettant fin au produit provisionné. Pour plus d'informations sur les utilisateurs ou les groupes IAM Identity Center, voir Gérer les utilisateurs et l'accès via AWS IAM Identity Center. La procédure suivante décrit comment annuler la gestion d'un compte membre dans Service Catalog.

Pour annuler la gestion d'un compte inscrit

1. Ouvrez la console Service Catalog dans votre navigateur Web à l'adressehttps://console.aws.amazon.com/servicecatalog.
2. Dans le volet de navigation de gauche, choisissez Provisioned products list.
3. Dans la liste des comptes provisionnés, choisissez le nom du compte que vous souhaitez qu'AWS Control Tower ne gère plus.
4. Sur la page Provisioned product details (Détails du produit mis en service), dans le menu Actions, choisissez Terminate (Résilier).
5. Dans la boîte de dialogue qui s'affiche, choisissez Terminate (Résilier).

> **Important**
>
> Le mot terminate est spécifique à Service Catalog. Lorsque vous résiliez un compte dans Service Catalog Account Factory, le compte n'est pas fermé. Cette action supprime le compte de son unité opérationnelle et de votre zone de landing zone.

6. Lorsque le compte n'est pas géré, son statut passe à Non inscrit.

7. Si vous n'avez plus besoin du compte, fermez-le. Pour plus d'informations sur la fermeture de AWS comptes, consultez la section Fermeture d'un compte dans le guide de AWS Billing l'utilisateur

Lorsque vous annulez la gestion d'un compte personnalisé, AWS Control Tower supprime les ressources déployées par le plan, ainsi que toutes les autres ressources créées par AWS Control Tower dans le compte. Après avoir dégéré le compte, vous pouvez le fermer. AWS Organizations

> **Note**
>
> Un compte non géré n'est ni fermé ni supprimé. Lorsque le compte n'est pas géré, l'utilisateur IAM Identity Center que vous avez sélectionné lorsque vous avez créé le compte dans Account Factory dispose toujours d'un accès administratif au compte. Si vous ne souhaitez pas que cet utilisateur dispose d'un accès administratif, vous devez modifier ce paramètre dans IAM Identity Center en mettant à jour le compte dans Account Factory et en modifiant l'adresse e-mail de l'utilisateur IAM Identity Center pour le compte. Pour plus d'informations, consultez Mettez à jour et déplacez les comptes Account Factory avec AWS Control Tower ou avec AWS Service Catalog.

Vidéo de procédure

Cette vidéo (3:25) explique comment supprimer un compte d'AWS Control Tower, obtenir un accès root au compte et enfin fermer le Compte AWS. Vous pouvez également fermer un compte à l'aide d'une AWS Organizations API. Pour un visionnage de meilleure qualité, sélectionnez l'icône dans le coin inférieur droit de la vidéo pour l'afficher en plein écran. Le sous-titrage est disponible.

Présentation vidéo de la fermeture d'un compte dans AWS Control Tower.

Vous pouvez visionner une liste de AWS YouTube vidéos expliquant les tâches courantes dans AWS Control Tower.

Fermer un compte créé dans Account Factory

Les comptes créés dans Account Factory sont Comptes AWS. Pour plus d'informations sur la clôture Comptes AWS, consultez la section Fermeture d'un compte dans le Guide de référence AWS sur la gestion des comptes.

> **Note**
>
> Fermer un compte n' Compte AWS est pas la même chose que annuler la gestion d'un compte depuis AWS Control Tower : il s'agit d'actions distinctes. Vous devez annuler la gestion du compte avant de le fermer.

Fermez le compte d'un membre AWS Control Tower via AWS Organizations

Vous pouvez fermer vos comptes de membre AWS Control Tower depuis le compte de gestion de votre organisation sans avoir à vous connecter à chaque compte membre individuellement avec des informations d'identification root, au moyen de AWS Organizations. Vous ne pouvez toutefois pas fermer votre compte de gestion de cette manière.

Lorsque vous appelez l' AWS Organizations CloseAccountAPI ou Compte AWS que vous fermez un compte dans la AWS Organizations console, le compte du membre est isolé pendant 90 jours, comme tout autre compte. Le compte affiche le statut Suspendu dans AWS Control Tower et AWS Organizations. Si vous essayez de travailler avec le compte pendant ces 90 jours, AWS Control Tower affiche un message d'erreur.

Avant l'expiration des 90 jours, vous pouvez restaurer le compte du membre, comme vous pouvez le faire pour n'importe quel autre compte Compte AWS. Après ce délai de 90 jours, les enregistrements du compte sont supprimés.

Nous vous recommandons, comme bonne pratique, de dégérer le compte d'un membre avant de le fermer. Si vous fermez un compte membre sans le dégérer au préalable, AWS Control Tower indique que le statut du compte est suspendu, mais également inscrit. Par conséquent, si vous tentez de réenregistrer l'unité d'organisation du compte pendant cette période de 90 jours, AWS Control Tower génère un message d'erreur. Le compte suspendu bloque essentiellement les actions de réenregistrement en cas d'échec de la pré-vérification. Si vous supprimez le compte de l'unité d'organisation, vous pouvez réenregistrer l'unité d'organisation, mais cela AWS peut générer une erreur concernant un mode de paiement manquant pour le compte. Pour contourner cette contrainte, créez une autre unité organisationnelle et déplacez le compte vers cette unité d'organisation avant d'essayer de vous réenregistrer. Nous recommandons de nommer cette unité d'organisation « unité d'organisation suspendue ».

> **Note**
>
> Si vous n'annulez pas la gestion du compte avant de le fermer, vous devez supprimer le produit approvisionné au AWS Service Catalog bout de ces 90 jours.

Pour plus d'informations, consultez la AWS Organizations documentation sur l'CloseAccountAPI.

Considérations relatives aux ressources pour Account Factory

Lorsqu'un compte est approvisionné avec Account Factory, les AWS ressources suivantes sont créées dans le compte.

AWS service	Type de ressource	Nom de la ressource
AWS CloudFormation	Piles	StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL-* StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-* StackSet-AWSControlTowerBP-BASELINE-CONFIG-* StackSet-AWSControlTowerBP-BASELINE-ROLES-* StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES-*
AWS CloudTrail	Journal d'activité	aws-controltower-BaselineCloudTrail

AWS service	Type de ressource	Nom de la ressource
Amazon CloudWatch	CloudWatch Règles de l'événement	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch Journaux	aws-controltower/CloudTrailLogs /aws/lambda/aws-controltower-NotificationForwarder
AWS Identity and Access Management	Rôles	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole AWSControlTowerExecution
AWS Identity and Access Management	Politiques	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	Rubriques	aws-controltower-SecurityNotifications
AWS Lambda	Applications	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*
AWS Lambda	Fonctions	aws-controltower-NotificationForwarder

Personnalisez les comptes avec Account Factory Customization (AFC)

AWS Control Tower vous permet de personnaliser les ressources nouvelles et existantes Comptes AWS lorsque vous provisionnez leurs ressources à partir de la console AWS Control Tower. Une fois que vous avez configuré la personnalisation du compte en usine, AWS Control Tower automatise ce processus pour le provisionnement futur, de sorte que vous n'avez pas à gérer de pipelines. Les comptes personnalisés peuvent être utilisés immédiatement après le provisionnement des ressources.

Vos comptes personnalisés sont approvisionnés dans Account Factory, via des AWS CloudFormation modèles ou avec Terraform. Vous allez définir un modèle qui servira de plan de compte personnalisé. Votre plan décrit les ressources et les configurations spécifiques dont vous avez besoin lorsqu'un compte est provisionné. Des plans prédéfinis, élaborés et gérés par des AWS partenaires, sont également disponibles. Pour plus d'informations sur les plans gérés par des partenaires, consultez la bibliothèque AWS Service Catalog Getting Started.

> **Note**
>
> AWS Control Tower contient des contrôles proactifs qui surveillent AWS CloudFormation les ressources dans AWS Control Tower. Vous pouvez éventuellement activer ces commandes dans votre zone de landing zone. Lorsque vous appliquez des contrôles proactifs, ils vérifient que les ressources que vous êtes sur le point de déployer sur vos comptes sont conformes aux politiques et procédures de votre organisation. Pour plus d'informations sur les contrôles proactifs, voir Contrôles proactifs.

Les plans de votre compte sont stockés dans un compte qui Compte AWS, à nos fins, est appelé compte hub. Les plans sont stockés sous la forme d'un produit Service Catalog. Nous appelons ce produit un modèle, afin de le distinguer de tous les autres produits Service Catalog. Pour en savoir plus sur la création de produits Service Catalog, consultez la section Création de produits dans le Guide de l'AWS Service Catalog administrateur.

Appliquer des plans aux comptes existants

Vous pouvez également appliquer des plans personnalisés à des comptes existants en suivant les étapes de mise à jour du compte dans la console AWS Control Tower. Pour plus de détails, consultez Mettre à jour le compte dans la console.

Avant de commencer

Avant de commencer à créer des comptes personnalisés avec AWS Control Tower Account Factory, vous devez avoir déployé un environnement de zone d'atterrissage AWS Control Tower, et vous devez disposer d'une unité organisationnelle (UO) enregistrée auprès d'AWS Control Tower, dans laquelle seront placés vos nouveaux comptes.

Pour plus d'informations sur l'utilisation d'AFC, consultez Automatiser la personnalisation des comptes à l'aide de Account Factory Customization dans AWS Control Tower.

Préparation à la personnalisation

- Vous pouvez créer un nouveau compte pour servir de compte hub, ou vous pouvez utiliser un compte existant Compte AWS. Nous vous recommandons vivement de ne pas utiliser le compte de gestion AWS Control Tower comme compte Blueprint Hub.
- Si vous envisagez de vous inscrire Comptes AWS à AWS Control Tower et de les personnaliser, vous devez d'abord ajouter le `AWSControlTowerExecution` rôle à ces comptes, comme vous le feriez pour tout autre compte que vous inscrivez dans AWS Control Tower.
- Si vous envisagez d'utiliser des plans de partenaires soumis à des exigences d'abonnement au marché, vous devez les configurer depuis votre compte de gestion AWS Control Tower avant de déployer les plans partenaires en tant que plans de personnalisation de l'usine du compte.

Rubriques

- Autorisations supplémentaires requises pour créer un produit Service Catalog basé sur Terraform

Configuration pour la personnalisation

Les sections suivantes décrivent les étapes à suivre pour configurer Account Factory pour le processus de personnalisation. Nous vous recommandons de configurer l'administration déléguée pour le compte hub avant de commencer ces étapes.

Récapitulatif

- Étape 1. Créez le rôle requis. Créez un rôle IAM qui autorise AWS Control Tower à accéder au compte (hub) où sont stockés les produits Service Catalog, également appelés blueprints.
- Étape 2. Créez le AWS Service Catalog produit. Créez le AWS Service Catalog produit (également appelé « produit phare ») dont vous aurez besoin pour définir le compte personnalisé comme base de référence.
- Étape 3. Passez en revue votre plan personnalisé. Inspectez le AWS Service Catalog produit (plan) que vous avez créé.
- Étape 4. Appelez votre plan pour créer un compte personnalisé. Entrez les informations relatives au produit et les informations relatives au rôle dans les champs appropriés dans Account Factory, dans la console AWS Control Tower, lors de la création du compte.

Étape 1. Créez le rôle requis

Avant de commencer à personnaliser les comptes, vous devez configurer un rôle contenant une relation de confiance entre AWS Control Tower et votre compte hub. Lorsqu'il est assumé, le rôle accorde à AWS Control Tower l'accès pour administrer le compte du hub. Le rôle doit être nommé AWSControlTowerBlueprintAccess.

AWS Control Tower assume ce rôle pour créer une ressource de portefeuille en votre nom AWS Service Catalog, puis pour ajouter votre plan en tant que produit Service Catalog à ce portefeuille, puis pour partager ce portefeuille, ainsi que votre plan, avec votre compte membre lors de la mise en service du compte.

Vous allez créer le `AWSControlTowerBlueprintAccess` rôle, comme expliqué dans les sections suivantes.

Accédez à la console IAM pour configurer le rôle requis.

Pour configurer le rôle dans un compte AWS Control Tower inscrit

1. Fédérez ou connectez-vous en tant que principal dans le compte de gestion AWS Control Tower.
2. Depuis le principal fédéré du compte de gestion, assumez ou changez de rôle pour accéder au `AWSControlTowerExecution` rôle du compte AWS Control Tower inscrit que vous avez sélectionné pour servir de compte Blueprint Hub.
3. À partir du `AWSControlTowerExecution` rôle figurant dans le compte AWS Control Tower inscrit, créez le `AWSControlTowerBlueprintAccess` rôle avec les autorisations et les relations de confiance appropriées.

Note

Pour respecter les directives relatives aux AWS meilleures pratiques, il est important que vous vous déconnectiez du `AWSControlTowerExecution` rôle immédiatement après l'`AWSControlTowerBlueprintAccess`avoir créé.
Pour éviter toute modification involontaire des ressources, le `AWSControlTowerExecution` rôle est destiné à être utilisé uniquement par AWS Control Tower.

Si votre compte Blueprint Hub n'est pas inscrit à AWS Control Tower, le `AWSControlTowerExecution` rôle n'existera pas dans le compte et il n'est pas nécessaire de l'assumer avant de continuer à le `AWSControlTowerBlueprintAccess` configurer.

Pour configurer le rôle dans un compte de membre non inscrit

1. Fédérez ou connectez-vous en tant que principal au compte que vous souhaitez désigner comme compte hub, selon la méthode de votre choix.
2. Lorsque vous êtes connecté en tant que principal du compte, créez le `AWSControlTowerBlueprintAccess` rôle avec les autorisations et les relations de confiance appropriées.

Le AWSControlTowerBlueprintAccessrôle doit être configuré de manière à accorder la confiance à deux principaux :

- Le principal (utilisateur) qui exécute AWS Control Tower dans le compte de gestion AWS Control Tower.
- Le rôle indiqué `AWSControlTowerAdmin` dans le compte de gestion AWS Control Tower.

Voici un exemple de politique de confiance, similaire à celle que vous devrez inclure pour votre rôle. Cette politique illustre la meilleure pratique consistant à accorder un accès avec le moindre privilège. Lorsque vous établissez votre propre politique, remplacez le terme *YourManagementAccountId*par l'identifiant de compte réel de votre compte de gestion AWS Control Tower, et remplacez le terme *YourControlTowerUserRole*par l'identifiant du rôle IAM pour votre compte de gestion.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                "arn:aws:iam::YourManagementAccountId:role/service-role/
AWSControlTowerAdmin",
                "arn:aws:iam::YourManagementAccountId:role/YourControlTowerUserRole"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Politique d'autorisations requises

AWS Control Tower exige que la politique gérée nommée `AWSServiceCatalogAdminFullAccess` soit attachée au `AWSControlTowerBlueprintAccess` rôle. Cette politique fournit des autorisations qui AWS Service Catalog déterminent quand elle autorise AWS Control Tower à administrer votre portefeuille et les ressources de vos AWS Service Catalog produits. Vous pouvez associer cette politique lorsque vous créez le rôle dans la console IAM.

Des autorisations supplémentaires peuvent être requises

- Si vous stockez vos plans dans Amazon S3, AWS Control Tower a également besoin de la politique `AmazonS3ReadOnlyAccess` d'autorisation associée au `AWSControlTowerBlueprintAccess` rôle.
- Le type de produit AWS Service Catalog Terraform vous oblige à ajouter des autorisations supplémentaires à la politique IAM personnalisée de l'AFC, si vous n'utilisez pas la politique d'administration par défaut. Il les nécessite en plus des autorisations requises pour créer les ressources que vous définissez dans votre modèle Terraform.

Étape 2. Créez le AWS Service Catalog produit

Pour créer un AWS Service Catalog produit, suivez les étapes décrites dans la section Création de produits dans le guide de l'AWS Service Catalog administrateur. Vous ajouterez le plan de votre compte en tant que modèle lorsque vous créerez le AWS Service Catalog produit.

Important

À la suite HashiCorp de la mise à jour des licences Terraform, du AWS Service Catalog changement de support pour les produits Terraform Open Source et de l'approvisionnement des produits vers un nouveau type de produit, appelé External. Pour en savoir plus sur l'impact de cette modification sur l'AFC, notamment sur la manière de mettre à jour les plans de votre compte existants pour le type de produit externe, consultez la section Transition vers le type de produit externe.

Résumé des étapes de création d'un plan

- Créez ou téléchargez un AWS CloudFormation modèle ou un fichier de configuration Terraform tar.gz qui deviendra le plan de votre compte. Quelques exemples de modèles sont donnés plus loin dans cette section.
- Connectez-vous à l' Compte AWS endroit où vous stockez vos plans Account Factory (parfois appelé compte hub).
- Accédez à la AWS Service Catalog console. Choisissez Liste de produits, puis choisissez Télécharger un nouveau produit.

- Dans le volet Détails du produit, entrez les détails de votre produit Blueprint, tels qu'un nom et une description.
- Sélectionnez Utiliser un fichier modèle, puis sélectionnez Choisir un fichier. Sélectionnez ou collez le modèle ou le fichier de configuration que vous avez développé ou téléchargé pour l'utiliser comme plan directeur.
- Choisissez Créer un produit en bas de la page de la console.

Vous pouvez télécharger un AWS CloudFormation modèle depuis le référentiel d'architecture de AWS Service Catalog référence. Un exemple tiré de ce référentiel permet de configurer un plan de sauvegarde pour vos ressources.

Voici un exemple de modèle, pour une entreprise fictive appelée Best Pets. Cela aide à établir une connexion à leur base de données pour animaux de compagnie.

```
Resources:
  ConnectionStringGeneratorLambdaRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - lambda.amazonaws.com
            Action:
              - "sts:AssumeRole"
  ConnectionStringGeneratorLambda:
    Type: AWS::Lambda::Function
    Properties:
      FunctionName: !Join ['-', ['ConnectionStringGenerator', !Select [4, !Split
 ['-', !Select [2, !Split ['/', !Ref AWS::StackId]]]]]]
      Description: Retrieves the connection string for this account to access the Pet
 Database
      Role: !GetAtt ConnectionStringGeneratorLambdaRole.Arn
      Runtime: nodejs16.x
      Handler: index.handler
      Timeout: 5
      Code:
        ZipFile: >
          const response = require("cfn-response");
```

```
          exports.handler = function (event, context) {
            const awsAccountId = context.invokedFunctionArn.split(":")[4]
            const connectionString= "fake connection string that's specific to account
" + awsAccountId;
            const responseData = {
              Value: connectionString,
            }
            response.send(event, context, response.SUCCESS, responseData);
            return connectionString;
          };

  ConnectionString:
    Type: Custom::ConnectionStringGenerator
    Properties:
      ServiceToken: !GetAtt ConnectionStringGeneratorLambda.Arn

  PetDatabaseConnectionString:
    DependsOn: ConnectionString
    # For example purposes we're using SSM parameter store.
    # In your template, use secure alternatives to store
    # sensitive values such as connection strings.
    Type: AWS::SSM::Parameter
    Properties:
      Name: pet-database-connection-string
      Description: Connection information for the BestPets pet database
      Type: String
      Value: !GetAtt ConnectionString.Value
```

Étape 3. Passez en revue votre plan personnalisé

Vous pouvez consulter votre plan dans la AWS Service Catalog console. Pour plus d'informations, consultez la section Gestion des produits dans le Guide de l'administrateur du Service Catalog.

Étape 4 : Appelez votre plan pour créer un compte personnalisé

Lorsque vous suivez le flux de travail de création de compte dans la console AWS Control Tower, vous verrez une section facultative dans laquelle vous pouvez saisir des informations sur le plan que vous souhaitez utiliser pour personnaliser les comptes.

> **Note**
>
> Vous devez configurer votre compte de hub de personnalisation et ajouter au moins un plan (produit Service Catalog) avant de pouvoir saisir ces informations dans la console AWS Control Tower et commencer à configurer des comptes personnalisés.

Créez ou mettez à jour un compte personnalisé dans la console AWS Control Tower.

1. Entrez l'identifiant du compte qui contient vos plans.
2. À partir de ce compte, sélectionnez un produit Service Catalog existant (plan existant).
3. Sélectionnez la version appropriée du plan (produit Service Catalog), si vous en avez plusieurs versions.
4. (Facultatif) Vous pouvez ajouter ou modifier une politique de provisionnement du plan à ce stade du processus. La politique de provisionnement du plan est écrite au format JSON et attachée à un rôle IAM, afin de pouvoir provisionner les ressources spécifiées dans le modèle de plan. AWS Control Tower crée ce rôle dans le compte membre afin que Service Catalog puisse déployer des ressources à l'aide de AWS CloudFormation stack sets. Le rôle est nommé `AWSControlTower-BlueprintExecution-bp-`*`xxxx`*. La `AdministratorAccess` politique est appliquée ici par défaut.
5. Choisissez la Région AWS ou les régions dans lesquelles vous souhaitez déployer des comptes en fonction de ce plan.
6. Si votre plan contient des paramètres, vous pouvez saisir les valeurs des paramètres dans des champs supplémentaires du flux de travail AWS Control Tower. Les valeurs supplémentaires peuvent inclure : un nom de GitHub référentiel, une GitHub branche, un nom de cluster Amazon ECS et l' GitHub identité du propriétaire du référentiel.
7. Vous pouvez personnaliser les comptes ultérieurement en suivant le processus de mise à jour du compte, si votre compte hub ou vos plans ne sont pas encore prêts.

Pour en savoir plus, consultez Créez un compte personnalisé à partir d'un plan.

Créez un compte personnalisé à partir d'un plan

Après avoir créé des plans personnalisés, vous pouvez commencer à créer des comptes personnalisés dans AWS Control Tower Account Factory.

Suivez ces étapes pour déployer un plan personnalisé lorsque vous créez un nouveau AWS compte :

1. Accédez à AWS Control Tower dans le AWS Management Console.
2. Sélectionnez Account Factory et Créez un compte.
3. Entrez les détails du compte tels que le nom du compte et l'adresse e-mail.
4. Configurez les détails du centre d'identité IAM avec l'adresse e-mail et le nom d'utilisateur.
5. Sélectionnez une unité d'organisation enregistrée à laquelle votre compte sera ajouté.
6. Développez la section de personnalisation du compte en usine.
7. Entrez l'ID de compte du compte Blueprint Hub qui contient vos produits Service Catalog et choisissez Valider. Pour plus d'informations sur un compte Blueprint Hub, consultezPersonnalisez les comptes avec Account Factory Customization (AFC).
8. Sélectionnez le menu déroulant qui contient tous les plans de votre liste de produits Service Catalog (tous les plans personnalisés et ceux des partenaires). Choisissez un plan et la version correspondante à déployer.
9. Si votre plan contient des paramètres, ces champs sont affichés pour que vous puissiez les renseigner. Les valeurs par défaut sont préremplies.
10. Enfin, sélectionnez l'endroit où vous allez déployer votre plan, soit dans la région d'origine, soit dans toutes les régions gouvernées. Les ressources mondiales, telles que Route 53 ou IAM, peuvent avoir besoin d'être déployées dans une seule région. Les ressources régionales, telles que les instances Amazon EC2 ou les compartiments Amazon S3, peuvent être déployées dans toutes les régions gouvernées
11. Une fois tous les champs remplis, sélectionnez Créer un compte.

> **Note**
>
> Les plans créés avec Terraform ne peuvent être déployés que dans une seule région, et non dans plusieurs régions.

Vous pouvez suivre la progression de l'approvisionnement de votre compte sur la page Organisation. Lorsque le provisionnement de votre compte est terminé, les ressources spécifiées dans votre plan sont déjà déployées dans celui-ci. Pour consulter les détails du compte et du plan, rendez-vous sur la page des détails du compte.

Inscrivez et personnalisez des comptes

Pour inscrire et personnaliser des comptes dans la console AWS Control Tower.

1. Accédez à la console AWS Control Tower et sélectionnez Organization dans le menu de navigation de gauche.
2. Vous verrez la liste de vos comptes disponibles. Identifiez le compte que vous souhaitez enregistrer à l'aide d'un plan personnalisé. La colonne État de ce compte doit indiquer que le statut du compte est Non inscrit.
3. Sélectionnez le bouton radio situé à gauche du compte et choisissez le menu déroulant Actions, en haut à droite de l'écran. Vous allez sélectionner ici l'option S'inscrire.
4. Complétez la section Configuration de l'accès avec les informations du centre d'identité IAM du compte.
5. Sélectionnez l'unité d'organisation enregistrée dont votre compte deviendra membre.
6. Complétez la section Personnalisation du compte en usine en suivant les mêmes étapes que les étapes 7 à 12 de la procédure de création de compte. Pour plus d'informations, consultez la section Comptes Provision Account Factory avec AWS Service Catalog.

Vous pouvez consulter l'état d'avancement de votre compte sur la page Organisation. Lorsque l'inscription de votre compte est terminée, les ressources spécifiées dans le plan sont déjà déployées dans celui-ci.

Ajouter un plan à un compte AWS Control Tower

Pour ajouter un plan à un compte membre AWS Control Tower existant, suivez le flux de travail de mise à jour du compte dans la console AWS Control Tower et choisissez un nouveau plan à ajouter au compte. Pour plus d'informations, consultez Mettre à jour et déplacer des comptes Account Factory avec AWS Control Tower ou avec AWS Service Catalog.

> **Note**
>
> Si vous ajoutez un nouveau plan à un compte, le plan existant est remplacé.

> **Note**
>
> Un plan peut être déployé par compte AWS Control Tower.

Mettre à jour un plan

Les procédures suivantes décrivent comment mettre à jour des plans personnalisés et comment les déployer.

Pour mettre à jour vos plans personnalisés

1. Mettez à jour votre AWS CloudFormation modèle ou votre fichier Terraform tar.gz (plan) avec vos nouvelles configurations.
2. Enregistrez le plan mis à jour en tant que nouvelle version dans AWS Service Catalog.

Pour déployer votre plan mis à jour

1. Accédez à la page Organisation dans la console AWS Control Tower.
2. Filtrez la page Organisation par nom et version du plan.
3. Suivez le processus de mise à jour du compte et déployez la dernière version du plan sur votre compte.

Si la mise à jour du plan échoue

AWS Control Tower autorise les mises à jour du plan lorsque le produit fourni est dans son état. `AVAILABLE` Si le produit que vous avez approvisionné est en bon `TAINTED` état, la mise à jour échouera. Nous recommandons la solution suivante :

1. Dans la AWS Service Catalog console, mettez à jour manuellement le produit `TAINTED` provisionné pour changer l'état en`AVAILABLE`. Pour plus d'informations, consultez la section Mise à jour des produits provisionnés.
2. Suivez ensuite le processus de mise à jour du compte proposé par AWS Control Tower pour corriger l'erreur de déploiement du plan.

Nous recommandons cette étape manuelle car : lorsque vous supprimez un plan, des ressources du compte membre peuvent être supprimées. La suppression de ressources peut affecter vos charges

de travail existantes. C'est pourquoi nous recommandons cette méthode plutôt que l'autre méthode de mise à jour d'un plan, qui consiste à supprimer et à remplacer le plan d'origine, en particulier si vous exécutez des charges de travail de production.

Supprimer un plan d'un compte

Pour supprimer un plan d'un compte, suivez le processus de mise à jour du compte pour supprimer le plan et rétablir les configurations par défaut du compte dans l'AWS Control Tower.

Lorsque vous entrez dans le flux de travail de mise à jour du compte dans la console, vous verrez que tous les détails du compte sont renseignés et que les détails de personnalisation ne le sont pas. Si vous laissez ces informations AFC vides, AWS Control Tower supprime le plan du compte. Un message d'avertissement s'affichera avant le début de l'action.

> **Note**
>
> AWS Control Tower ajoute un plan à un compte uniquement si vous sélectionnez un plan lors du processus de création ou de mise à jour du compte.

Les plans des partenaires

AWS Control Tower Account Factory Customization (AFC) donne accès à des plans de personnalisation prédéfinis conçus et gérés par des partenaires. AWS Ces plans de partenariat vous aident à personnaliser vos comptes pour des cas d'utilisation spécifiques. Les plans de chaque partenaire vous aident à créer des comptes personnalisés, qui sont préconfigurés pour fonctionner avec les offres de produits de ce partenaire en particulier.

Pour consulter la liste complète des plans des partenaires d'AWS Control Tower, accédez à la bibliothèque Service Catalog Getting Started dans votre console. Recherchez le type de source AWS Control Tower Blueprints.

Considérations relatives aux personnalisations d'Account Factory (AFC)

- L'AFC prend en charge la personnalisation à l'aide d'un seul produit de AWS Service Catalog plan.
- Les produits AWS Service Catalog Blueprint doivent être créés dans le compte hub et dans la même région que la région d'origine de la zone d'atterrissage d'AWS Control Tower.
- Le rôle `AWSControlTowerBlueprintAccess` IAM doit être créé avec le nom, les autorisations et la politique de confiance appropriés.

- AWS Control Tower propose deux options de déploiement pour les plans : le déploiement dans la région d'origine uniquement ou le déploiement dans toutes les régions régies par AWS Control Tower. La sélection des régions n'est pas disponible.
- Lorsque vous mettez à jour un plan dans un compte membre, l'identifiant du compte Blueprint Hub et le produit AWS Service Catalog Blueprint ne peuvent pas être modifiés.
- AWS Control Tower ne prend pas en charge la suppression d'un plan existant et l'ajout d'un nouveau plan en une seule opération de mise à jour du plan. Vous pouvez supprimer un plan puis en ajouter un nouveau dans le cadre d'opérations distinctes.
- AWS Control Tower modifie le comportement selon que vous créez ou inscrivez des comptes personnalisés ou des comptes non personnalisés. Si vous ne créez ou n'inscrivez pas de comptes personnalisés à l'aide de plans, AWS Control Tower crée un produit approvisionné par Account Factory (via Service Catalog) dans le compte de gestion AWS Control Tower. Si vous spécifiez la personnalisation lors de la création ou de l'inscription de comptes à l'aide de plans, AWS Control Tower ne crée pas de produit approvisionné par Account Factory dans le compte de gestion AWS Control Tower.

En cas d'erreur de plan

Erreur lors de l'application d'un plan

Si une erreur se produit lors du processus d'application d'un plan à un compte, qu'il s'agisse d'un nouveau compte ou d'un compte existant que vous inscrivez dans AWS Control Tower, la procédure de restauration est la même. Le compte existera, mais il n'est pas personnalisé et il n'est pas inscrit dans AWS Control Tower. Pour continuer, suivez les étapes pour inscrire le compte dans AWS Control Tower et ajoutez le plan au moment de l'inscription.

Erreur lors de la création du **`AWSControlTowerBlueprintAccess`** rôle et solutions

Lorsque vous créez le `AWSControlTowerBlueprintAccess` rôle à partir d'un compte AWS Control Tower, vous devez être connecté en tant que principal en utilisant le `AWSControlTowerExecution` rôle. Si vous êtes connecté comme un autre utilisateur, l'`CreateRole`opération est empêchée par un SCP, comme le montre l'artefact suivant :

```
{
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalArn": [
```

```
                    "arn:aws:iam::*:role/AWSControlTowerExecution",
                    "arn:aws:iam::*:role/stacksets-exec-*"
                ]
            }
        },
        "Action": [
            "iam:AttachRolePolicy",
            "iam:CreateRole",
            "iam:DeleteRole",
            "iam:DeleteRolePermissionsBoundary",
            "iam:DeleteRolePolicy",
            "iam:DetachRolePolicy",
            "iam:PutRolePermissionsBoundary",
            "iam:PutRolePolicy",
            "iam:UpdateAssumeRolePolicy",
            "iam:UpdateRole",
            "iam:UpdateRoleDescription"
        ],
        "Resource": [
            "arn:aws:iam::*:role/aws-controltower-*",
            "arn:aws:iam::*:role/*AWSControlTower*",
            "arn:aws:iam::*:role/stacksets-exec-*"
        ],
        "Effect": "Deny",
        "Sid": "GRIAMROLEPOLICY"
    }
```

Les solutions de contournement suivantes sont disponibles :

- (Très recommandé) Assumez le `AWSControlTowerExecution` rôle et `AWSControlTowerBlueprintAccess` créez-le. Si vous choisissez cette solution, veillez à vous déconnecter du `AWSControlTowerExecution` rôle immédiatement après, afin d'éviter toute modification involontaire des ressources.
- Connectez-vous à un compte qui n'est pas inscrit dans AWS Control Tower et qui n'est donc pas soumis à ce SCP.
- Modifiez temporairement ce SCP pour autoriser l'opération.
- (Fortement déconseillé) Utilisez votre compte de gestion AWS Control Tower comme compte hub, afin qu'il ne soit pas soumis au SCP.

Personnalisation de votre document de politique pour les plans de l'AFC sur la base de CloudFormation

Lorsque vous activez un plan par le biais de Account Factory, AWS Control Tower vous demande AWS CloudFormation d'en créer un StackSet en votre nom. AWS CloudFormation nécessite l'accès à votre compte géré pour créer des AWS CloudFormation piles dans le StackSet. Bien qu'il dispose AWS CloudFormation déjà de privilèges d'administrateur sur le compte géré via le `AWSControlTowerExecution` rôle, ce rôle n'est pas assumable par AWS CloudFormation.

Dans le cadre de l'activation d'un plan, AWS Control Tower crée un rôle dans le compte du membre, qui AWS CloudFormation peut être chargé d'effectuer les tâches StackSet de gestion. Le moyen le plus simple d'activer votre plan personnalisé via Account Factory consiste à utiliser une politique d'autorisation complète, car ces politiques sont compatibles avec n'importe quel modèle de plan.

Cependant, les meilleures pratiques suggèrent que vous devez restreindre les autorisations pour AWS CloudFormation le compte cible. Vous pouvez fournir une politique personnalisée, qu'AWS Control Tower applique au rôle qu'elle crée AWS CloudFormation pour être utilisé. Par exemple, si votre plan crée un paramètre SSM appelé something-important, vous pouvez fournir la politique suivante :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCloudFormationActionsOnStacks",
            "Effect": "Allow",
            "Action": "cloudformation:*",
            "Resource": "arn:aws:cloudformation:*:*:stack/*"
        },
        {
            "Sid": "AllowSsmParameterActions",
            "Effect": "Allow",
            "Action": [
                "ssm:PutParameter",
                 "ssm:DeleteParameter",
                 "ssm:GetParameter",
                 "ssm:GetParameters"
            ],
            "Resource": "arn:*:ssm:*:*:parameter/something-important"
        }
    ]
```

```
}
```

L'`AllowCloudFormationActionsOnStacks`instruction est obligatoire pour toutes les politiques personnalisées de l'AFC ; AWS CloudFormation utilise ce rôle pour créer des instances de pile, elle nécessite donc une autorisation pour effectuer des AWS CloudFormation actions sur les piles. La `AllowSsmParameterActions` section est spécifique au modèle en cours d'activation.

Résoudre les problèmes d'autorisation

Lorsque vous activez un plan avec une politique restreinte, il se peut que les autorisations soient insuffisantes pour activer le plan. Pour résoudre ces problèmes, révisez votre document de politique et mettez à jour les préférences relatives au plan du compte membre afin d'utiliser la politique corrigée. Pour vérifier que la politique est suffisante pour activer le plan, assurez-vous que les AWS CloudFormation autorisations sont accordées et que vous pouvez créer une pile directement à l'aide de ce rôle.

Autorisations supplémentaires requises pour créer un produit Service Catalog basé sur Terraform

Lorsque vous créez un produit AWS Service Catalog externe avec un fichier de configuration Terraform pour AFC, AWS Service Catalog certaines autorisations doivent être ajoutées à votre politique IAM personnalisée AFC, en plus des autorisations requises pour créer les ressources définies dans votre modèle. Si vous choisissez la politique d'administration complète par défaut, vous n'avez pas besoin d'ajouter ces autorisations supplémentaires.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "resource-groups:CreateGroup",
                "resource-groups:ListGroupResources",
                "resource-groups:DeleteGroup",
                "resource-groups:Tag"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "tag:GetResources",
```

```
                "tag:GetTagKeys",
                "tag:GetTagValues",
                "tag:TagResources",
                "tag:UntagResources"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": "s3:GetObject",
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
                }
            }
        }
    ]
}
```

Pour plus d'informations sur la création de produits Terraform à l'aide du type de produit externe dans AWS Service Catalog, voir Étape 5 : Création de rôles de lancement dans le Guide de l'administrateur du Service Catalog.

Provisionner des comptes avec AWS Control Tower Account Factory for Terraform (AFT)

AWS Control Tower Account Factory for Terraform (AFT) adopte un GitOps modèle qui automatise le processus de mise en service et de mise à jour des comptes dans AWS Control Tower.

> **Note**
>
> L'AFT n'a aucun impact sur les performances du flux de travail dans AWS Control Tower. Si vous créez un compte via AFT ou Account Factory, le même flux de travail principal se produit.

Avec AFT, vous créez un fichier Terraform de demande de compte, qui contient l'entrée qui appelle le flux de travail AFT. Une fois le provisionnement et la mise à jour des comptes terminés, le flux de

travail AFT continue en exécutant le cadre de provisionnement des comptes AFT et les étapes de personnalisation des comptes.

Prérequis

Avant de commencer à utiliser AFT, vous devez créer les éléments suivants :

- Un environnement AFT entièrement déployé. Pour plus d'informations, consultez Présentation d'AWS Control Tower Account Factory pour Terraform (AFT) et Déploiement d'AWS Control Tower Account Factory pour Terraform (AFT)
- Un ou plusieurs `git` référentiels AFT dans votre environnement AFT entièrement déployé. Pour plus d'informations, consultez la section Étapes post-déploiement pour AFT.

> **Tip**
>
> Vous pouvez éventuellement créer un dossier de modèles de comptes dans le aft-account-customizationsréférentiel.

Pour plus d'informations sur les Régions AWS domaines dans lesquels AFT impose des limites de déploiement, reportez-vous Limitations et quotas dans AWS Control Tower aux sections etLimites de contrôle.

Création d'un nouveau compte auprès de l'AFT

Pour créer un nouveau compte auprès d'AFT, créez un fichier Terraform de demande de compte. Ce fichier contient les entrées pour les paramètres du aft-account-requestréférentiel. Après avoir créé un fichier Terraform de demande de compte, commencez à traiter votre demande de compte en exécutant. `git push` Cette commande appelle l'`ct-aft-account-request`opération dans le AWS CodePipeline, qui est créée dans le compte de gestion AFT une fois le provisionnement du compte terminé. Pour plus d'informations, consultez la section Pipeline de provisionnement des comptes AFT.

Paramètres du fichier Terraform de demande de compte

Vous devez inclure les paramètres suivants dans le fichier Terraform de votre demande de compte. Vous pouvez consulter un exemple de fichier Terraform de demande de compte sur. GitHub

- La valeur de `module name` doit être unique par Compte AWS demande.
- La valeur de `module source` est le chemin d'accès au module Terraform de demande de compte fourni par AFT.
- La valeur de `control_tower_parameters` capture les données requises pour créer un compte AWS Control Tower. La valeur inclut les champs de saisie suivants :
  - `AccountEmail`
  - `AccountName`
  - `ManagedOrganizationalUnit`
  - `SSOUserEmail`
  - `SSOUserFirstName`
  - `SSOUserLastName`

> **Note**
>
> La saisie que vous fournissez ne `control_tower_parameters` peut pas être modifiée lors de la mise en service du compte.
> Les formats pris en charge pour la spécification `ManagedOrganizationalUnit` dans le aft-account-requestréférentiel incluent `OUName` et`OUName (OU-ID)`.

- `account_tags`capture les clés et les valeurs définies par l'utilisateur, qui peuvent être étiquetées Comptes AWS en fonction de critères commerciaux. Pour plus d'informations, consultez la section AWS Organizations Ressources relatives au balisage dans le Guide de AWS Organizations l'utilisateur.
- La valeur de `change_management_parameters` capture des informations supplémentaires, telles que la raison pour laquelle une demande de compte a été créée et l'auteur de la demande de compte. La valeur inclut les champs de saisie suivants :
  - `change_reason`
  - `change_requested_by`
- `custom_fields`capture des métadonnées supplémentaires avec des clés et des valeurs qui sont déployées sous forme de paramètres SSM dans le compte vendu sous /aft/account-request/custom-fields/. Vous pouvez faire référence à ces métadonnées lors de la personnalisation du compte afin de déployer les contrôles appropriés. Par exemple, un compte soumis à la conformité réglementaire peut en déployer d'autres AWS Config Rules. Les métadonnées que vous collectez

`custom_fields` peuvent nécessiter un traitement supplémentaire lors de la mise en service et de la mise à jour du compte. Si un champ personnalisé est supprimé de la demande de compte, il est supprimé du magasin de paramètres SSM pour le compte vendu.

- (Facultatif) `account_customizations_name` capture le dossier des modèles de comptes dans le aft-account-customizationsréférentiel. Pour plus d'informations, consultez la section Personnalisations du compte.

Soumettre plusieurs demandes de compte

AFT traite les demandes de compte une par une, mais vous pouvez soumettre plusieurs demandes de compte au pipeline AFT. Lorsque vous soumettez plusieurs demandes de compte au pipeline AFT, AFT met en file d'attente et traite les demandes de compte selon le principe du premier entré, premier sorti.

> **Note**
>
> Vous pouvez créer un fichier Terraform de demande de compte pour chaque compte que vous souhaitez qu'AFT provisionne ou mettre en cascade plusieurs demandes de compte dans un seul fichier Terraform de demande de compte.

Mettre à jour un compte existant

Vous pouvez mettre à jour les comptes approvisionnés par l'AFT en modifiant les demandes de compte soumises précédemment et en les exécutant`git push`. Cette commande appelle le flux de travail de provisionnement du compte et peut traiter les demandes de mise à jour du compte. Vous pouvez mettre à jour l'entrée pour`ManagedOrganizationalUnit`, qui fait partie de la valeur requise pour`control_tower_parameters`, et d'autres paramètres dans le fichier Terraform de demande de compte. Pour plus d'informations, voir Création d'un nouveau compte auprès d'AFT.

> **Note**
>
> La saisie que vous fournissez ne `control_tower_parameters` peut pas être modifiée lors de la mise en service du compte.
> Les formats pris en charge pour la spécification `ManagedOrganizationalUnit` dans le aft-account-requestréférentiel incluent `OUName` et`OUName (OU-ID)`.

Mettre à jour un compte que l'AFT ne fournit pas

Vous pouvez mettre à jour les comptes AWS Control Tower créés en dehors d'AFT en spécifiant le compte dans le aft-account-requestréférentiel.

> **Note**
>
> Assurez-vous que tous les détails du compte sont corrects et cohérents avec l'organisation AWS Control Tower et le produit AWS Service Catalog provisionné correspondant.

Conditions préalables à la mise à jour d'un existant Compte AWS avec AFT

- Ils Compte AWS doivent être inscrits à AWS Control Tower.
- Ils Compte AWS doivent faire partie de l'organisation AWS Control Tower.

Déployez AWS Control Tower Account Factory pour Terraform (AFT)

Cette section s'adresse aux administrateurs des environnements AWS Control Tower qui souhaitent configurer Account Factory for Terraform (AFT) dans leur environnement existant. Il décrit comment configurer un environnement Account Factory for Terraform (AFT) avec un nouveau compte de gestion AFT dédié.

> **Note**
>
> Un module Terraform déploie AFT. Ce module est disponible dans le référentiel AFT le GitHub, et l'ensemble du référentiel AFT est considéré comme le module.
> Nous vous recommandons de vous référer aux modules AFT GitHub plutôt que de cloner le référentiel AFT. De cette façon, vous pouvez contrôler et utiliser les mises à jour des modules dès qu'elles sont disponibles.

Pour en savoir plus sur les dernières versions de la fonctionnalité AWS Control Tower Account Factory for Terraform (AFT), consultez le fichier Releases de ce GitHub référentiel.

Conditions préalables au déploiement

Avant de configurer et de lancer votre environnement AFT, vous devez disposer des éléments suivants :

- Une zone d'atterrissage pour AWS Control Tower. Pour plus d'informations, consultez Planifier la zone d'atterrissage de votre AWS Control Tower.
- Une région d'origine pour votre zone de landing AWS Control Tower. Pour plus d'informations, consultez Comment Régions AWS travailler avec AWS Control Tower.
- Une version et une distribution de Terraform. Pour plus d'informations, consultez les versions Terraform et AFT.
- Un fournisseur VCS pour le suivi et la gestion des modifications apportées au code et à d'autres fichiers. Par défaut, AFT utilise AWS CodeCommit. Pour plus d'informations, voir Qu'est-ce que c'est AWS CodeCommit ? dans le guide de AWS CodeCommit l'utilisateur. Si vous souhaitez choisir un autre fournisseur VCS, consultez la section Alternatives pour le contrôle de version du code source dans AFT.
- Un environnement d'exécution dans lequel vous pouvez exécuter le module Terraform qui installe AFT.
- Options de fonctionnalités AFT. Pour plus d'informations, voir Activer les options des fonctionnalités.

Configurez et lancez votre AWS Control Tower Account Factory pour Terraform

Les étapes suivantes supposent que vous connaissez le flux de travail Terraform. Vous pouvez également en savoir plus sur le déploiement de l'AFT en suivant le laboratoire d'introduction à l'AFT sur le site Web de AWS Workshop Studio.

Étape 1 : Lancez votre zone de landing zone AWS Control Tower

Suivez les étapes décrites dans Getting Started with AWS Control Tower. C'est ici que vous créez le compte de gestion AWS Control Tower et que vous configurez votre zone de landing zone AWS Control Tower.

> **Note**
>
> Assurez-vous de créer un rôle pour le compte de gestion AWS Control Tower doté d'AdministratorAccessinformations d'identification. Pour plus d'informations, consultez les ressources suivantes :
>
> - Identités IAM (utilisateurs, groupes d'utilisateurs et rôles) dans le guide de l'AWS Identity and Access Management utilisateur

- AdministratorAccessdans le Guide de référence des politiques AWS gérées

Étape 2 : Création d'une nouvelle unité organisationnelle pour l'AFT (recommandé)

Nous vous recommandons de créer une unité d'organisation distincte dans votre AWS organisation. C'est ici que vous déployez le compte de gestion AFT. Créez la nouvelle unité d'organisation avec votre compte de gestion AWS Control Tower. Pour plus d'informations, voir Créer une nouvelle unité d'organisation.

Étape 3 : provisionner le compte de gestion AFT

L'AFT exige que vous créiez un AWS compte dédié aux opérations de gestion de l'AFT. Le compte de gestion AWS Control Tower, associé à votre zone d'atterrissage AWS Control Tower, vend le compte de gestion AFT. Pour plus d'informations, consultez Provisionner des comptes avec AWS Service Catalog Account Factory.

> **Note**
>
> Si vous avez créé une unité d'organisation distincte pour AFT, assurez-vous de sélectionner cette unité d'organisation lorsque vous créez le compte de gestion AFT.

Le provisionnement complet du compte de gestion AFT peut prendre jusqu'à 30 minutes.

Étape 4 : Vérifiez que l'environnement Terraform est disponible pour le déploiement

Cette étape suppose que vous avez de l'expérience avec Terraform et que vous avez mis en place des procédures pour exécuter Terraform. Pour plus d'informations, consultez Command : init sur le site Web du HashiCorp développeur.

> **Note**
>
> AFT prend en charge la version Terraform `1.2.0` ou ultérieure.

Étape 5 : Appelez le module Account Factory for Terraform pour déployer AFT

Appelez le module AFT avec le rôle que vous avez créé pour le compte de gestion AWS Control Tower doté d'AdministratorAccessinformations d'identification. AWS Control Tower fournit un module

Terraform via le compte de gestion AWS Control Tower, qui établit toute l'infrastructure requise pour orchestrer les demandes AWS Control Tower Account Factory.

Vous pouvez consulter le module AFT dans le référentiel AFT sur GitHub. L'ensemble du GitHub référentiel est considéré comme le module AFT. Reportez-vous au fichier README pour obtenir des informations sur les entrées requises pour exécuter le module AFT et déployer AFT. Vous pouvez également consulter le module AFT dans le registre Terraform.

Le module AFT inclut un `aft_enable_vpc` paramètre qui indique si AWS Control Tower fournit les ressources du compte au sein d'un cloud privé virtuel (VPC) dans le compte de gestion AFT central. Par défaut, le paramètre est défini sur`true`. Si vous définissez ce paramètre sur`false`, AWS Control Tower déploie AFT sans utiliser de VPC ni de ressources réseau privées, telles que des passerelles NAT ou des points de terminaison VPC. La désactivation `aft_enable_vpc` peut contribuer à réduire les coûts d'exploitation de l'AFT pour certains modèles d'utilisation.

> **Note**
>
> La réactivation du `aft_enable_vpc` paramètre (passage de la valeur de `false` à`true`) peut nécessiter que vous exécutiez la `terraform apply` commande deux fois de suite.

Si votre environnement possède des pipelines établis pour gérer Terraform, vous pouvez intégrer le module AFT dans votre flux de travail existant. Sinon, exécutez le module AFT depuis n'importe quel environnement authentifié avec les informations d'identification requises.

Le délai d'expiration entraîne l'échec du déploiement. Nous vous recommandons d'utiliser les informations d'identification AWS Security Token Service (STS) pour vous assurer que vous disposez d'un délai d'attente suffisant pour un déploiement complet. Le délai minimum pour les AWS STS informations d'identification est de 60 minutes. Pour plus d'informations, consultez la section Informations d'identification de sécurité temporaires dans IAM dans le Guide de l'AWS Identity and Access Management utilisateur.

> **Note**
>
> Vous pouvez attendre jusqu'à 30 minutes pour qu'AFT termine son déploiement via le module Terraform.

Étape 6 : Gérer le fichier d'état Terraform

Un fichier d'état Terraform est généré lorsque vous déployez AFT. Cet artefact décrit l'état des ressources créées par Terraform. Si vous prévoyez de mettre à jour la version AFT, assurez-vous de conserver le fichier d'état Terraform ou de configurer un backend Terraform à l'aide d'Amazon S3 et DynamoDB. Le module AFT ne gère pas l'état Terraform d'un backend.

> **Note**
>
> Vous êtes responsable de la protection du fichier d'état Terraform. Certaines variables d'entrée peuvent contenir des valeurs sensibles, telles qu'une `ssh` clé privée ou un jeton Terraform. Selon votre méthode de déploiement, ces valeurs peuvent être visualisées sous forme de texte brut dans le fichier d'état Terraform. Pour plus d'informations, consultez la section Données sensibles en état sur le HashiCorp site Web.

Étapes postérieures au déploiement

Une fois le déploiement de l'infrastructure AFT terminé, suivez ces étapes supplémentaires pour terminer le processus de configuration et vous préparer à provisionner des comptes.

Étape 1 : (Facultatif) Complétez CodeConnections avec le fournisseur VCS de votre choix

Si vous choisissez un fournisseur de VCS tiers, l'AFT les établit CodeConnections et vous les confirmez. Reportez-vous Alternatives pour le contrôle de version du code source dans AFT à pour savoir comment configurer AFT avec votre VCS préféré.

L'étape initiale d'établissement de la AWS CodeStar connexion est réalisée par AFT. Vous devez confirmer la connexion.

Étape 2 : (Obligatoire) Remplissez chaque référentiel

AFT nécessite que vous gériez quatre référentiels :

1. Demandes de compte — Ce référentiel gère le placement ou la mise à jour des demandes de compte. Exemples disponibles. Pour plus d'informations sur les demandes de compte AFT, consultezCréation d'un nouveau compte auprès de l'AFT.
2. Personnalisations du provisionnement des comptes AFT — Ce référentiel gère les personnalisations appliquées à tous les comptes créés et gérés par AFT, avant de commencer la phase de personnalisation globale. Exemples disponibles. Pour créer des personnalisations de provisionnement de comptes AFT, voir. Créez votre compte AFT, provisionnement, personnalisation, machine à états

3. Personnalisations globales — Ce référentiel gère les personnalisations appliquées à tous les comptes créés et gérés avec AFT. Exemples disponibles. Pour créer des personnalisations globales AFT, voirAppliquer des personnalisations globales.
4. Personnalisations de compte — Ce référentiel gère les personnalisations appliquées uniquement à des comptes spécifiques créés et gérés avec AFT. Exemples disponibles. Pour créer des personnalisations de compte AFT, voirAppliquer les personnalisations de compte.

AFT s'attend à ce que chacun de ces référentiels suive une structure de répertoire spécifique. Les modèles utilisés pour remplir vos référentiels et les instructions décrivant comment remplir les modèles sont disponibles dans le module Account Factory for Terraform du référentiel AFT github.

Présentation d'AWS Control Tower Account Factory pour Terraform (AFT)

Account Factory for Terraform (AFT) met en place un pipeline Terraform pour vous aider à provisionner et à personnaliser des comptes dans AWS Control Tower. AFT vous offre l'avantage du provisionnement de comptes basé sur Terraform tout en vous permettant de gérer vos comptes avec AWS Control Tower.

Avec AFT, vous créez un fichier Terraform de demande de compte pour obtenir les informations qui déclenchent le flux de travail AFT pour le provisionnement du compte. Une fois la phase de provisionnement du compte terminée, AFT exécute automatiquement une série d'étapes avant le début de la phase de personnalisation du compte. Pour plus d'informations, consultez la section Pipeline de provisionnement des comptes AFT.

AFT prend en charge Terraform Cloud, Terraform Enterprise et Terraform Community Edition. Avec AFT, vous pouvez lancer la création de comptes à l'aide d'un fichier d'entrée et d'une simple `git push` commande et personnaliser des comptes nouveaux ou existants. La création de compte inclut tous les avantages de gouvernance d'AWS Control Tower et les personnalisations de compte qui vous aident à respecter les procédures de sécurité standard et les directives de conformité de votre organisation.

AFT prend en charge le suivi des demandes de personnalisation des comptes. Chaque fois que vous soumettez une demande de personnalisation de compte, AFT génère un jeton de suivi unique qui passe par une machine d' AWS Step Functions état de personnalisation AFT, qui enregistre le jeton dans le cadre de son exécution. Vous pouvez ensuite utiliser les requêtes Amazon CloudWatch Logs Insights pour rechercher des plages d'horodatage et récupérer le jeton de demande. Par conséquent, vous pouvez voir les charges utiles qui accompagnent le jeton, ce qui vous permet de

suivre la demande de personnalisation de votre compte tout au long du flux de travail AFT. Pour plus d'informations sur CloudWatch les journaux et les Step Functions, consultez les rubriques suivantes :

- Qu'est-ce qu'Amazon CloudWatch Logs ? dans le guide de l'utilisateur d'Amazon CloudWatch Logs
- Qu'est-ce que c'est AWS Step Functions ? dans le guide AWS Step Functions du développeur

AFT combine les capacités d'autres AWS servicesServices relatifs aux composants, notamment pour créer un framework, avec des pipelines qui déploient Terraform Infrastructure as Code (IaC). L'AFT vous permet de :

- Soumettre des demandes de provisionnement et de mise à jour de comptes dans un modèle GitOps
- Stocker les métadonnées du compte et l'historique des audits
- Appliquer des balises au niveau du compte
- Ajoutez des personnalisations à tous les comptes, à un ensemble de comptes ou à des comptes individuels
- Activer les options de fonctionnalités

AFT crée un compte distinct, appelé compte de gestion AFT, pour déployer les capacités AFT. Avant de configurer l'AFT, vous devez disposer d'une zone d'atterrissage AWS Control Tower existante. Le compte de gestion AFT n'est pas le même que le compte de gestion AWS Control Tower.

L'AFT offre de la flexibilité

- Flexibilité pour votre plateforme : AFT prend en charge toutes les distributions Terraform pour le déploiement initial et le fonctionnement continu : Community Edition, Cloud et Enterprise.
- Flexibilité pour votre système de contrôle de version : AFT s'appuie nativement sur des sources alternatives AWS CodeCommit, mais il prend en charge des sources alternatives pour CodeConnections.

AFT propose des options de fonctionnalités

Vous pouvez activer plusieurs options de fonctionnalités, conformément aux meilleures pratiques :

- Création d'un système au niveau de l'organisation CloudTrail pour la journalisation des événements liés aux données

- Supprimer le VPC AWS par défaut pour les comptes
- Inscription de comptes provisionnés dans le plan de AWS Support aux entreprises

> **Note**
>
> Le pipeline AFT n'est pas destiné à être utilisé pour déployer des ressources, telles que des instances Amazon EC2, dont vos comptes ont besoin pour exécuter vos applications. Il est uniquement destiné au provisionnement et à la personnalisation automatisés des comptes AWS Control Tower.

Vidéo de procédure

Cette vidéo (7:33) explique comment déployer des comptes avec AWS Control Tower Account Factory for Terraform. Pour un visionnage de meilleure qualité, sélectionnez l'icône dans le coin inférieur droit de la vidéo pour l'afficher en plein écran. Le sous-titrage est disponible.

Présentation vidéo du provisionnement automatique des comptes dans AWS Control Tower.

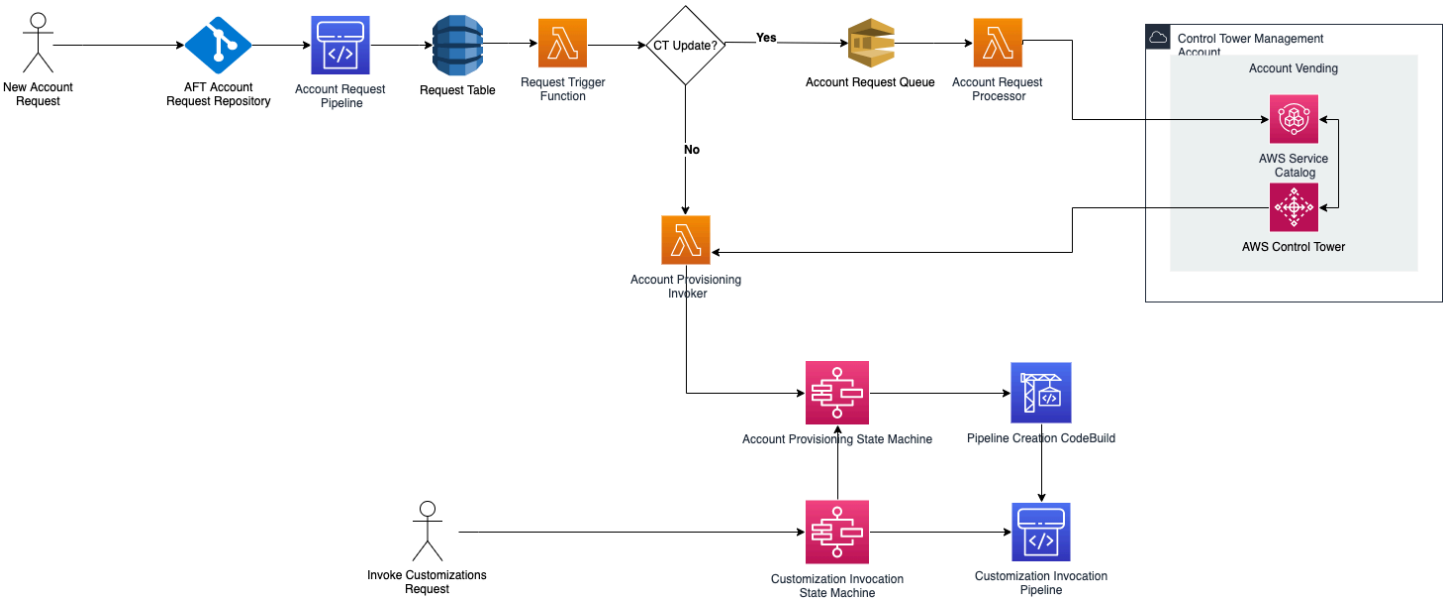
Architecture AFT

Ordre des opérations

Vous gérez les opérations AFT dans le compte de gestion AFT. Pour un flux de travail complet de provisionnement de comptes, l'ordre des étapes de gauche à droite dans le diagramme est le suivant :

1. Les demandes de compte sont créées et soumises au pipeline. Vous pouvez créer et soumettre plusieurs demandes de compte à la fois. Account Factory traite les demandes dans le cadre d'une first-in-first-out commande. Pour plus d'informations, voir Soumettre des demandes de comptes multiples.
2. Chaque compte est approvisionné. Cette étape s'exécute dans le compte de gestion AWS Control Tower.
3. Les personnalisations globales s'exécutent dans les pipelines créés pour chaque compte vendeur.
4. Si des personnalisations sont spécifiées dans les demandes de provisionnement de compte initiales, elles s'exécutent uniquement sur les comptes ciblés. Si vous possédez un compte déjà provisionné, vous devez effectuer d'autres personnalisations manuellement dans le pipeline du compte.

AWS Control Tower Account Factory pour Terraform : flux de travail de provisionnement de comptes



Coût

Il n'y a pas de frais supplémentaires pour l'AFT. Vous ne payez que pour les ressources déployées par AFT, les AWS services fournis par AFT et les ressources que vous déployez dans votre environnement AFT.

La configuration AFT par défaut inclut l'allocation de AWS PrivateLink points de terminaison, pour une protection et une sécurité accrues des données, ainsi qu'une passerelle NAT dont la prise en charge AWS CodeBuild est requise. Pour plus de détails sur la tarification de cette infrastructure, consultez la AWS PrivateLink tarification et la tarification Amazon VPC pour la passerelle NAT. Contactez le représentant de votre AWS compte pour obtenir des informations plus spécifiques sur la gestion de ces coûts. Vous pouvez modifier ces paramètres par défaut pour AFT.

Versions Terraform et AFT

Account Factory for Terraform (AFT) prend en charge la version Terraform ou ultérieure. `1.2.0` Vous devez fournir une version Terraform comme paramètre d'entrée pour le processus de déploiement AFT, comme indiqué dans l'exemple suivant.

```
terraform_version = "1.2.0"
```

Distributions Terraform

AFT prend en charge trois distributions Terraform :

- Édition communautaire Terraform
- Cloud Terraform
- Terraform Entreprise

Ces distributions sont expliquées dans les sections qui suivent. Fournissez la distribution Terraform de votre choix comme paramètre d'entrée lors du processus de démarrage AFT. Pour plus d'informations sur le déploiement d'AFT et les paramètres d'entrée, consultezDéployez AWS Control Tower Account Factory pour Terraform (AFT).

Si vous choisissez les distributions Terraform Cloud ou Terraform Enterprise, le jeton d'API que vous spécifiez `terraform_token` doit être un jeton d'API utilisateur ou d'équipe. Un jeton d'organisation n'est pas pris en charge pour toutes les API requises. Pour des raisons de sécurité, vous devez éviter d'enregistrer la valeur de ce jeton dans votre système de contrôle de version (VCS) en affectant une variable terraform, comme indiqué dans l'exemple suivant.

```
# Sensitive variable managed in Terraform Cloud:
terraform_token = var.terraform_cloud_token
```

Édition communautaire Terraform

Lorsque vous sélectionnez Terraform Community Edition comme distribution, AFT gère le backend Terraform pour vous dans le compte de gestion AFT. AFT télécharge la version `terraform-cli` de Terraform que vous avez spécifiée pour l'exécuter pendant les phases de déploiement d'AFT et de pipeline AFT. La configuration d'état Terraform qui en résulte est stockée dans un compartiment Amazon S3, nommé sous la forme suivante :

```
aft-backend-[account_id]-primary-region
```

AFT crée également un compartiment Amazon S3 qui reproduit votre configuration d'état Terraform dans un autre Région AWS, à des fins de reprise après sinistre, nommé sous la forme suivante :

```
aft-backend-[account_id]-secondary-region
```

Nous vous recommandons d'activer l'authentification multifactorielle (MFA) pour les fonctions de suppression sur ces compartiments Amazon S3 d'état Terraform. Pour en savoir plus sur Terraform Community Edition, consultez la documentation Terraform.

Pour sélectionner Terraform OSS comme distribution, fournissez le paramètre d'entrée suivant :

```
terraform_distribution = "oss"
```

Cloud Terraform

Lorsque vous sélectionnez Terraform Cloud comme distribution, AFT crée des espaces de travail pour les composants suivants dans votre organisation Terraform Cloud, ce qui lance un flux de travail piloté par API.

- Demande de compte
- Personnalisations AFT pour les comptes approvisionnés par AFT
- Personnalisations de compte pour les comptes approvisionnés par l'AFT
- Personnalisations globales pour les comptes approvisionnés par AFT

Terraform Cloud gère la configuration d'état Terraform qui en résulte.

Lorsque vous sélectionnez Terraform Cloud comme distribution, fournissez les paramètres d'entrée suivants :

- `terraform_distribution = "tfc"`
- `terraform_token`— Ce paramètre contient la valeur du jeton Terraform Cloud. AFT marque la valeur comme sensible et stocke la valeur sous forme de chaîne sécurisée dans le magasin de paramètres SSM du compte de gestion AFT. Nous vous recommandons de modifier régulièrement la valeur du jeton Terraform conformément aux politiques de sécurité et aux directives de conformité de votre entreprise. Le jeton Terraform doit être un jeton d'API au niveau de l'utilisateur ou de l'équipe. Les jetons d'organisation ne sont pas pris en charge.
- `terraform_org_name`— Ce paramètre contient le nom de votre organisation Terraform Cloud.

> **Note**
>
> Les déploiements AFT multiples dans une même organisation Terraform Cloud ne sont pas pris en charge.

Pour plus d'informations sur la configuration de Terraform Cloud, consultez la documentation Terraform.

Terraform Entreprise

Lorsque vous sélectionnez Terraform Enterprise comme distribution, AFT crée des espaces de travail pour les composants suivants dans votre organisation Terraform Enterprise, et déclenche un flux de travail piloté par API pour les exécutions Terraform qui en résultent.

- Demande de compte
- Personnalisations du provisionnement des comptes AFT pour les comptes provisionnés par AFT
- Personnalisations de compte pour les comptes provisionnés par AFT
- Personnalisations globales pour les comptes provisionnés par AFT

La configuration d'état Terraform qui en résulte est gérée par votre configuration Terraform Enterprise.

Pour sélectionner Terraform Enterprise comme distribution, fournissez les paramètres d'entrée suivants :

- `terraform_distribution = "tfe"`
- `terraform_token`— Ce paramètre contient la valeur de votre jeton Terraform Enterprise. AFT marque sa valeur comme sensible et la stocke sous forme de chaîne sécurisée dans le magasin de paramètres SSM, dans le compte de gestion AFT. Nous vous recommandons de modifier régulièrement la valeur du jeton Terraform, conformément aux politiques de sécurité et aux directives de conformité de votre entreprise.
- `terraform_org_name`— Ce paramètre contient le nom de votre organisation Terraform Enterprise.
- `terraform_api_endpoint`— Ce paramètre contient l'URL de votre environnement Terraform Enterprise. La valeur de ce paramètre doit être au format suivant :

```
https://{fqdn}/api/v2/
```

Consultez la documentation Terraform pour en savoir plus sur la configuration de Terraform Enterprise.

Vérifiez la version AFT

Vous pouvez vérifier votre version AFT déployée en interrogeant la clé AWS SSM Parameter Store :

```
/aft/config/aft/version
```

Si vous utilisez la méthode du registre, vous pouvez épingler la version.

```
module "control_tower_account_factory" {
  source  = "aws-ia/control_tower_account_factory/aws"
  version = "1.3.2"
  # insert the 6 required variables here
}
```

Vous pouvez consulter plus d'informations sur les versions AFT dans le référentiel AFT.

Mettre à jour la version AFT

Vous pouvez mettre à jour votre version AFT déployée en l'extrayant depuis la branche du `main` référentiel :

```
terraform get -update
```

Une fois l'extraction terminée, vous pouvez réexécuter le plan Terraform ou exécuter Apply pour mettre à jour l'infrastructure AFT avec les dernières modifications.

Activer les options de fonctionnalités

AFT propose des options de fonctionnalités basées sur les meilleures pratiques. Vous pouvez opter pour ces fonctionnalités, au moyen d'indicateurs de fonctionnalités, lors du déploiement de l'AFT. Création d'un nouveau compte auprès de l'AFTPour plus d'informations sur les paramètres de configuration d'entrée AFT, reportez-vous à.

Ces fonctionnalités ne sont pas activées par défaut. Vous devez activer chacune d'entre elles de manière explicite dans votre environnement.

Rubriques

- AWS CloudTrail événements liés aux données
- AWS Plan de support aux entreprises
- Supprimer le AWS VPC par défaut

AWS CloudTrail événements liés aux données

Lorsqu'elle est activée, l'option AWS CloudTrail Data Events configure ces fonctionnalités.

- Crée un historique d'organisation dans le compte de gestion AWS Control Tower, pour CloudTrail
- Active la journalisation des événements de données Amazon S3 et Lambda
- Chiffre et exporte tous les événements de CloudTrail données vers un compartiment `aws-aft-logs-*` S3 du compte AWS Control Tower Log Archive, avec AWS KMS chiffrement
- Active le paramètre de validation du fichier journal

Pour activer cette option, définissez l'indicateur de fonctionnalité suivant sur True dans la configuration d'entrée de votre déploiement AFT.

```
aft_feature_cloudtrail_data_events
```

Prérequis

Avant d'activer cette option de fonctionnalité, assurez-vous que l'accès sécurisé AWS CloudTrail est activé dans votre organisation.

Pour vérifier l'état de l'accès sécurisé pour CloudTrail :

1. Accédez à la AWS Organizations console.
2. Choisissez Services > CloudTrail.
3. Sélectionnez ensuite Activer l'accès sécurisé en haut à droite, si nécessaire.

Vous pouvez recevoir un message d'avertissement vous conseillant d'utiliser la AWS CloudTrail console, mais dans ce cas, ignorez cet avertissement. AFT crée le parcours dans le cadre de l'activation de cette option de fonctionnalité, une fois que vous avez autorisé un accès sécurisé. Si l'accès sécurisé n'est pas activé, vous recevrez un message d'erreur lorsque l'AFT tentera de créer votre trace pour les événements liés aux données.

> **Note**
>
> Ce paramètre fonctionne au niveau de l'organisation. L'activation de ce paramètre affecte tous les comptes AWS Organizations, qu'ils soient gérés par AFT ou non. Tous les compartiments du compte AWS Control Tower Log Archive au moment de l'activation sont

exclus des événements de données Amazon S3. Reportez-vous au guide de AWS CloudTrail l'utilisateur pour en savoir plus sur CloudTrail.

AWS Plan de support aux entreprises

Lorsque cette option est activée, le pipeline AFT active le plan AWS Enterprise Support pour les comptes provisionnés par AFT.

AWS les comptes sont fournis par défaut avec le plan Support AWS de base activé. AFT fournit une inscription automatique au niveau de support d'entreprise, pour les comptes approvisionnés par AFT. Le processus de provisionnement ouvre un ticket d'assistance pour le compte, demandant son ajout au plan de support aux AWS entreprises.

Pour activer l'option Enterprise Support, définissez l'indicateur de fonctionnalité suivant sur True dans la configuration d'entrée de votre déploiement AFT.

```
aft_feature_enterprise_support=false
```

Reportez-vous à la section Comparer les plans de AWS support pour en savoir plus sur les plans de AWS support.

> **Note**
>
> Pour permettre à cette fonctionnalité de fonctionner, vous devez inscrire le compte payeur au plan Enterprise Support.

Supprimer le AWS VPC par défaut

Lorsque vous activez cette option, AFT supprime tous les VPC AWS par défaut du compte de gestion Régions AWS, même si aucune ressource AWS Control Tower n'y est déployée. Régions AWS

AFT ne supprime pas automatiquement les VPC AWS par défaut pour les comptes AWS Control Tower approvisionnés par AFT ou pour les AWS comptes existants que vous inscrivez dans AWS Control Tower via AFT.

Les nouveaux AWS comptes sont créés avec un VPC configuré par défaut dans chacun Région AWSd'eux. Votre entreprise applique peut-être des pratiques standard pour créer des VPC, qui vous

obligent à supprimer le VPC AWS par défaut et à éviter de l'activer, en particulier pour le compte de gestion AFT.

Pour activer cette option, définissez l'indicateur de fonctionnalité suivant sur True dans la configuration d'entrée de votre déploiement AFT.

```
aft_feature_delete_default_vpcs_enabled
```

Reportez-vous à la section VPC par défaut et sous-réseaux par défaut pour en savoir plus sur les VPC par défaut.

Considérations relatives aux ressources pour AWS Control Tower Account Factory for Terraform

Lorsque vous configurez votre zone de landing zone à l'aide d'AWS Control Tower Account Factory for Terraform, plusieurs types de AWS ressources sont créés dans vos AWS comptes.

Rechercher des ressources

- Vous pouvez utiliser des balises pour rechercher la liste la plus récente des ressources AFT. La paire clé-valeur pour votre recherche est la suivante :

  ```
  Key: managed_by | Value: AFT
  ```

- Pour les services de composants qui ne prennent pas en charge les balises, vous pouvez localiser les ressources en effectuant une recherche `aft` dans les noms des ressources.

Tableaux des ressources initialement créés, par compte

Compte de gestion AWS Control Tower Account Factory pour Terraform

AWS web	Type de ressource	Nom de la ressource
AWS Identity and Access Management	Rôles	AWSAFTAdministrator AWSAFTExecution AWSAFTService aws-ct-aft-*

AWS web	Type de ressource	Nom de la ressource
AWS Identity and Access Management	Politiques	aws-ct-aft-*
CodeCommit	Référentiels	aws-ct-aft-*
CodeBuild	Projets de génération	aws-ct-aft-*
Pipeline de codes	Pipelines	*-baseline-*
Amazon S3	Compartiments	*-aws-ct-aft-* aws-ct-aft-*
Lambda	Fonctions	aws-ct-aft-*
Lambda	Couches	aws-ct-aft-common-layer
DynamoDB	Tables	aws-ct-aft-request aws-ct-aft-request-audit aws-ct-aft-request-metadata aws-ct-aft-controltower-events
Step Functions	Machines d'État	aws-ct-aft-prebaseline aws-ct-aft-prebaseline-customizations aws-ct-aft-trigger-baseline aws-ct-aft-features
VPC	VPC	aws-ct-aft-vpc
Amazon SNS	Rubriques	aws-ct-aft-notifications aws-ct-aft-failure-notifications

AWS web	Type de ressource	Nom de la ressource
Amazon EventBridge	Bus d'événements	aws-ct-aft-events-from-ct-management
Amazon EventBridge	Règles de l'événement	aws-ct-aft-capture-ct-events aws-ct-aft-lambda-account-request-processor
Service de gestion des clés (KMS)	Clés gérées par le client	*-aws-ct-aft-* aws-ct-aft-*
AWS Systems Manager	Magasin de paramètres	/aws-ct-aft/account/* /aws/ct-aft/config/*
Amazon SQS	Files d'attente	aws-ct-aft-account-request.fifo aws-ct-aft-account-request-dlg.fifo
CloudWatch	Groupes de journaux	/aws/*/aws-ct-aft-* aws-ct-aft-*
AWS Centre de support (facultatif)	Plans de support	Enterprise

AWS comptes provisionnés via AWS Control Tower Account Factory pour Terraform

AWS web	Type de ressource	Nom de la ressource
AWS Identity and Access Management	Rôles	AWSAFTExecution
AWS Centre de support (facultatif)	Plans de support	Enterprise

Compte de gestion AWS Control Tower

AWS web	Type de ressource	Nom de la ressource
AWS Identity and Access Management	Rôles	AWSAFTExecutionRole AWSAFTExecution aws-ct-aft-controltower-events-rule
AWS Systems Manager	Magasin de paramètres	/aws-ct-aft/account/aws-ct-aft-management/account-id
AWS Organizations (Facultatif)	Politiques de contrôle de service	aws-ct-aft-protect-resources
CloudTrail (Facultatif)	Journaux de suivi	aws-ct-aft-BaselineCloudTrail
Centre de support AWS (facultatif)	Plans de support	Enterprise

Compte d'archivage des journaux AWS Control Tower

AWS web	Type de ressource	Nom de la ressource
AWS Identity and Access Management	Rôles	AWSAFTExecutionRole AWSAFTExecution aws-ct-aft-cloudtrail-data-events-role
Service de gestion des clés (KMS)	Clés gérées par le client	*-aws-ct-aft-kms-gd-findings
Amazon S3	Compartiments	*-aws-ct-aft-logs* aws-ct-aft-s3-access-logs*

AWS web	Type de ressource	Nom de la ressource
AWS Centre de support (facultatif)	Plans de support	Enterprise

Compte d'audit AWS Control Tower

AWS web	Type de ressource	Nom de la ressource
AWS Identity and Access Management	Rôles	AWSAFTExecutionRole AWSAFTExecution
AWS Centre de support (facultatif)	Plans de support	Enterprise

Rôles obligatoires

En général, les rôles et les politiques font partie de la gestion des identités et des accès (IAM) dans AWS. Reportez-vous au guide de l'utilisateurAWS IAM pour plus d'informations.

AFT crée plusieurs rôles et politiques IAM dans les comptes de gestion AFT et de gestion AWS Control Tower afin de soutenir les opérations du pipeline AFT. Ces rôles sont créés sur la base du modèle d'accès avec le moindre privilège, qui limite les autorisations aux ensembles d'actions et de ressources minimalement requis pour chaque rôle et chaque politique. Ces rôles et politiques se voient attribuer une `key:value` paire de AWS balises, comme `managed_by:AFT` pour l'identification.

Outre ces rôles IAM, l'AFT crée trois rôles essentiels :

- le `AWSAFTAdmin` rôle
- le `AWSAFTExecution` rôle
- le `AWSAFTService` rôle

Ces rôles sont expliqués dans les sections suivantes.

Le AWSAFTAdmin rôle, expliqué

Lorsque vous déployez AFT, le `AWSAFTAdmin` rôle est créé dans le compte de gestion AFT. Ce rôle permet au pipeline AFT d'assumer le `AWSAFTExecution` rôle dans les comptes provisionnés par AWS Control Tower et AFT, afin d'effectuer des actions liées au provisionnement et à la personnalisation des comptes.

Voici la politique intégrée (artefact JSON) attachée au `AWSAFTAdmin` rôle :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": [
                "arn:aws:iam::*:role/AWSAFTExecution",
                "arn:aws:iam::*:role/AWSAFTService"
            ]
        }
    ]
}
```

L'artefact JSON suivant montre la relation de confiance associée au `AWSAFTAdmin` rôle. Le numéro d'espace réservé `012345678901` est remplacé par le numéro d'identification du compte de gestion AFT.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Le AWSAFTExecution rôle, expliqué

Lorsque vous déployez AFT, le `AWSAFTExecution` rôle est créé dans les comptes de gestion AFT et de gestion AWS Control Tower. Plus tard, le pipeline AFT crée le `AWSAFTExecution` rôle dans chaque compte provisionné AFT pendant la phase de provisionnement du compte AFT.

AFT utilise le `AWSControlTowerExecution` rôle dans un premier temps, pour le `AWSAFTExecution` créer dans des comptes spécifiés. Le `AWSAFTExecution` rôle permet au pipeline AFT d'exécuter les étapes effectuées lors des étapes de provisionnement et de personnalisation du provisionnement du framework AFT, pour les comptes provisionnés AFT et pour les comptes partagés.

> **Des rôles distincts vous aident à limiter la portée**
>
> Il est recommandé de séparer les autorisations de personnalisation de celles autorisées lors du déploiement initial des ressources. N'oubliez pas que le `AWSAFTService` rôle est destiné au provisionnement du compte et qu'il est destiné à la `AWSAFTExecution` personnalisation du compte. Cette séparation limite l'étendue des autorisations autorisées au cours de chaque phase du pipeline. Cette distinction est particulièrement importante si vous personnalisez les comptes partagés AWS Control Tower, car ceux-ci peuvent contenir des informations sensibles, telles que des informations de facturation ou des informations utilisateur.

Autorisations pour `AWSAFTExecution` le rôle : AdministratorAccess— une politique gérée par AWS

L'artefact JSON suivant montre la politique IAM (relation de confiance) attachée au `AWSAFTExecution` rôle. Le numéro d'espace réservé `012345678901` est remplacé par le numéro d'identification du compte de gestion AFT.

Politique de confiance pour `AWSAFTExecution`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
    }
  ]
```

```
}
```

Le AWSAFTService rôle, expliqué

Le `AWSAFTService` rôle déploie les ressources AFT dans tous les comptes inscrits et gérés, y compris les comptes partagés et le compte de gestion. Auparavant, les ressources étaient déployées uniquement par le `AWSAFTExecution` rôle.

Le `AWSAFTService` rôle est destiné à être utilisé par l'infrastructure de service pour déployer des ressources pendant la phase de provisionnement, et le `AWSAFTExecution` rôle est destiné à être utilisé uniquement pour déployer des personnalisations. En assumant les rôles de cette manière, vous pouvez maintenir un contrôle d'accès plus précis à chaque étape.

Autorisations pour `AWSAFTService` le rôle : AdministratorAccess— une politique gérée par AWS

L'artefact JSON suivant montre la politique IAM (relation de confiance) attachée au `AWSAFTService` rôle. Le numéro d'espace réservé `012345678901` est remplacé par le numéro d'identification du compte de gestion AFT.

Politique de confiance pour `AWSAFTService`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Services relatifs aux composants

Lorsque vous déployez AFT, des composants sont ajoutés à votre AWS environnement à partir de chacun de ces AWS services.

- AWS Control Tower — AFT utilise AWS Control Tower Account Factory dans le compte de gestion AWS Control Tower pour provisionner des comptes.

- Amazon DynamoDB — AFT crée des tables Amazon DynamoDB dans le compte de gestion AFT, qui stockent les demandes de compte, l'historique des audits des mises à jour du compte, les métadonnées du compte et les événements du cycle de vie de l'AWS Control Tower. AFT crée également des déclencheurs DynamoDB Lambda pour lancer des processus en aval, tels que le démarrage du flux de travail de provisionnement des comptes AFT.
- Amazon Simple Storage Service — AFT crée des compartiments Amazon Simple Storage Service (S3) dans le compte de gestion AFT et le compte d'archivage des journaux AWS Control Tower, qui stockent les journaux générés par les services AWS requis par le pipeline AFT. AFT crée également un compartiment S3 principal Terraform, dans les régions AWS principales et secondaires, pour stocker les états Terraform générés lors des flux de travail du pipeline AFT.
- Amazon Simple Notification Service — AFT crée des rubriques Amazon Simple Notification Service (SNS) dans le compte de gestion AFT, qui stocke les notifications de réussite et d'échec après le traitement de chaque demande de compte AFT. Vous pouvez recevoir ces messages en utilisant le protocole de votre choix.
- Amazon Simple Queuing Service — AFT crée une file d'attente FIFO Amazon Simple Queuing Service (Amazon SQS) dans le compte de gestion AFT. La file d'attente vous permet de soumettre plusieurs demandes de compte en parallèle, mais elle envoie une demande à la fois à AWS Control Tower Account Factory, pour un traitement séquentiel.
- AWS CodeBuild — AFT crée des projets de CodeBuild construction AWS dans le compte de gestion AFT afin d'initialiser, de compiler, de tester et d'appliquer les plans Terraform pour le code source AFT au cours des différentes étapes de construction.
- AWS CodePipeline — AFT crée des CodePipeline pipelines AWS dans le compte de gestion AFT afin de les intégrer au fournisseur de CodeStar connexions AWS que vous avez sélectionné et pris en charge pour le code source AFT, et de déclencher des tâches de création dans AWS CodeBuild.
- AWS Lambda — AFT crée des fonctions et des couches AWS Lambda dans le compte de gestion AFT pour effectuer des étapes lors de la demande de compte, du provisionnement du compte AFT et des processus de personnalisation du compte.
- AWS Systems Manager Parameter Store — AFT configure le magasin de paramètres AWS Systems Manager dans le compte de gestion AFT, afin de stocker les paramètres de configuration requis pour les processus du pipeline AFT.
- Amazon CloudWatch — AFT crée des groupes de CloudWatch journaux Amazon dans le compte de gestion AFT pour stocker les journaux générés par les services AWS utilisés par le pipeline AFT. La période de conservation des CloudWatch journaux est définie sur`Never Expire`.

- Amazon VPC — AFT crée un Amazon Virtual Private Cloud (VPC) pour isoler les services et les ressources du compte de gestion AFT dans un environnement réseau distinct, afin d'améliorer la sécurité.
- AWS KMS — AFT utilise le service AWS Key Management Service (KMS) dans le compte de gestion AFT et dans le compte d'archivage des journaux AWS Control Tower. AFT crée des clés pour chiffrer les états Terraform, les données stockées dans les tables DynamoDB et les rubriques SNS. Ces journaux et artefacts sont générés lorsque les ressources et les services AWS sont déployés par AFT. La rotation annuelle des clés KMS créées par AFT est activée par défaut.
- AWS Identity and Access Management (IAM) — AFT suit le modèle de moindre privilège recommandé. Il crée des rôles et des politiques AWS Identity and Access Management (IAM) dans le compte de gestion AFT, dans les comptes AWS Control Tower et dans les comptes provisionnés par AFT, selon les besoins, afin d'effectuer les actions requises pendant le flux de travail du pipeline AFT.
- AWS Step Functions — AFT crée des machines d'état AWS Step Functions dans le compte de gestion AFT. Ces machines d'état orchestrent et automatisent le processus et les étapes du cadre de provisionnement et de personnalisation des comptes AFT.
- Amazon EventBridge — AFT crée un bus d' EventBridgeévénements Amazon dans le compte de gestion AFT et AWS Control Tower afin de capturer et de stocker les événements du cycle de vie d'AWS Control Tower à long terme dans la table DynamoDB du compte de gestion AFT. AFT crée des règles relatives aux CloudWatch événements AWS dans les comptes de gestion AFT et de gestion AWS Control Tower, qui déclenchent les multiples étapes requises lors de l'exécution du flux de travail du pipeline AFT
- AWS CloudTrail (facultatif) — Lorsque cette fonctionnalité est activée, AFT crée un journal de CloudTrail l'organisation AWS dans le compte de gestion AWS Control Tower, afin de consigner les événements de données pour les buckets Amazon S3 et les fonctions AWS Lambda. AFT envoie ces journaux vers un compartiment S3 central dans le compte d'archivage des journaux d'AWS Control Tower.
- AWS Support (facultatif) — Lorsque cette fonctionnalité est activée, AFT active le plan AWS Enterprise Support pour les comptes fournis par AFT. Par défaut, les comptes AWS sont créés avec le plan AWS Basic Support activé.

Pipeline de provisionnement de comptes AFT

Une fois la phase de provisionnement des comptes du pipeline terminée, le cadre AFT se poursuit. Il exécute automatiquement une série d'étapes pour s'assurer que les informations relatives aux comptes nouvellement provisionnés sont en place, avant le début de l'Personnaliser le compteétape.

Voici les prochaines étapes du pipeline AFT.

1. Valide la saisie de la demande de compte.
2. Récupère des informations sur le compte provisionné, par exemple l'identifiant du compte.
3. Stocke les métadonnées du compte dans une table DynamoDB du compte de gestion AFT.
4. Crée le rôle AWSAFTExecutionIAM dans le compte nouvellement provisionné. AFT assume ce rôle pour effectuer l'étape de personnalisation des comptes, car ce rôle donne accès au portefeuille Account Factory.
5. Applique les balises de compte que vous avez fournies dans le cadre des paramètres de saisie de la demande de compte.
6. Applique les options de fonctionnalité AFT que vous avez choisies au moment du déploiement de l'AFT.
7. Applique les personnalisations de provisionnement du compte AFT que vous avez fournies. La section suivante explique comment configurer ces personnalisations avec une machine d'état AWS Step Functions, dans un `git` référentiel. Cette étape est parfois appelée étape du cadre de provisionnement des comptes. Cela fait partie du processus de provisionnement de base, mais vous avez déjà mis en place un framework qui fournit des intégrations personnalisées dans le cadre de votre flux de travail de provisionnement de comptes, avant que des personnalisations supplémentaires ne soient ajoutées aux comptes à l'étape suivante.
8. Pour chaque compte provisionné, il crée un compte de gestion intégré AWS CodePipeline à l'AFT, qui sera exécuté pour effectuer l'Personnaliser le compteétape (globale suivante).
9. Invoque le pipeline de personnalisation des comptes pour chaque compte provisionné (et ciblé).
10. Envoie une notification de réussite ou d'échec à la rubrique SNS, à partir de laquelle vous pouvez récupérer les messages.

Configurez les personnalisations de la structure de provisionnement des comptes avec une machine à états

Si vous configurez des intégrations personnalisées autres que Terraform avant de provisionner vos comptes, ces personnalisations sont incluses dans le flux de travail de provisionnement de votre compte AFT. Par exemple, vous pouvez avoir besoin de certaines personnalisations pour garantir que tous les comptes créés par AFT sont conformes aux normes et politiques de votre organisation, telles que les normes de sécurité, et ces normes peuvent être ajoutées aux comptes avant une personnalisation supplémentaire. Ces personnalisations du cadre de provisionnement des comptes sont mises en œuvre sur chaque compte provisionné, avant que la phase de personnalisation globale du compte ne commence ensuite.

> **Note**
>
> La fonctionnalité AFT décrite dans cette section est destinée aux utilisateurs avancés qui comprennent le fonctionnement d'AWS Step Functions. Nous vous recommandons également de travailler avec les assistants globaux lors de la phase de personnalisation du compte.

Le framework de provisionnement des comptes AFT fait appel à une machine d'état AWS Step Functions, que vous définissez, pour implémenter vos personnalisations. Reportez-vous à la documentation AWS Step Functions pour en savoir plus sur les intégrations possibles de machines à états.

Voici quelques intégrations courantes.

- AWS Lambda fonctionne dans la langue de votre choix
- Tâches AWS ECS ou AWS Fargate, à l'aide de conteneurs Docker
- Activités AWS Step Functions utilisant des travailleurs personnalisés, hébergées sur AWS ou sur site
- Intégrations Amazon SNS ou SQS

Si aucune machine d'état AWS Step Functions n'est définie, l'étape passe sans opération. Pour créer un compte AFT provisionnant une machine à états de personnalisation, suivez les instructions figurant dans. Créez votre compte AFT, provisionnement, personnalisation, machine à états Avant d'ajouter des personnalisations, assurez-vous que les prérequis sont en place.

Ces types d'intégrations ne font pas partie d'AWS Control Tower et ne peuvent pas être ajoutés pendant la phase globale de pré-API de personnalisation du compte AFT. Le pipeline AFT vous permet plutôt de configurer ces personnalisations dans le cadre du processus de provisionnement, et elles sont exécutées dans le flux de travail de provisionnement. Vous devez implémenter ces personnalisations en créant votre machine à états à l'avance, avant de lancer la phase de provisionnement du compte AFT, comme décrit dans les sections suivantes.

Conditions préalables à la création d'une machine à états

- Un AFT entièrement déployé. Voir Déployez AWS Control Tower Account Factory pour Terraform (AFT) pour plus d'informations sur le déploiement de l'AFT.
- Configurez un `git` référentiel dans votre environnement pour les personnalisations du provisionnement des comptes AFT. Pour plus d'informations, consultez Étapes postérieures au déploiement.

Créez votre compte AFT, provisionnement, personnalisation, machine à états

Étape 1 : modifier la définition de la machine à états

Modifiez l'exemple de définition de la machine à `customizations.asl.json` états. L'exemple est disponible dans le `git` référentiel que vous avez configuré pour stocker les personnalisations de provisionnement des comptes AFT, lors des étapes post-déploiement. Reportez-vous au guide du développeur AWS Step Functions pour en savoir plus sur les définitions des machines à états.

Étape 2 : inclure la configuration Terraform correspondante

Incluez les fichiers Terraform avec l'`.tf`extension dans le même `git` référentiel avec la définition de la machine à états pour votre intégration personnalisée. Par exemple, si vous choisissez d'appeler une fonction Lambda dans votre définition de tâche State Machine, vous devez inclure le `lambda.tf` fichier dans le même répertoire. Assurez-vous d'inclure les rôles et autorisations IAM requis pour vos configurations personnalisées.

Lorsque vous fournissez les informations appropriées, le pipeline AFT invoque automatiquement votre machine d'état et déploie vos personnalisations dans le cadre de l'étape du cadre de provisionnement des comptes AFT.

Pour redémarrer le cadre de provisionnement des comptes AFT et les personnalisations

AFT gère le cadre de provisionnement des comptes et les étapes de personnalisation pour chaque compte vendu via le pipeline AFT. Pour relancer les personnalisations de provisionnement des comptes, vous pouvez utiliser l'une des deux méthodes suivantes :

1. Apportez toute modification à un compte existant dans le dépôt des demandes de compte.
2. Ouvrez un nouveau compte auprès de l'AFT.

Personnaliser le compte

AFT peut déployer des configurations standard ou personnalisées dans des comptes provisionnés. Dans le compte de gestion de l'AFT, l'AFT fournit un pipeline pour chaque compte. Avec ce pipeline, vous pouvez implémenter vos personnalisations dans tous les comptes, dans un ensemble de comptes ou dans des comptes individuels. Vous pouvez exécuter des scripts Python, des scripts bash et des configurations Terraform, ou vous pouvez interagir avec l'AWS CLI dans le cadre de l'étape de personnalisation de votre compte.

Présentation

Une fois que vos personnalisations ont été spécifiées dans les `git` référentiels que vous avez choisis, soit celui dans lequel vous stockez vos personnalisations globales, soit celui dans lequel vous stockez les personnalisations de votre compte, l'étape de personnalisation du compte est terminée automatiquement par le pipeline AFT. Pour personnaliser les comptes rétroactivement, voirRéinvoquer les personnalisations.

Personnalisations globales (facultatif)

Vous pouvez choisir d'appliquer certaines personnalisations à tous les comptes fournis par AFT. Par exemple, si vous devez créer un rôle IAM particulier ou déployer un contrôle personnalisé dans chaque compte, l'étape de personnalisation globale du pipeline AFT vous permet de le faire automatiquement.

Personnalisations du compte (facultatif)

Pour personnaliser un compte individuel ou un ensemble de comptes différemment des autres comptes provisionnés par AFT, vous pouvez tirer parti de la partie du pipeline AFT consacrée aux

personnalisations de comptes pour implémenter des configurations spécifiques au compte. Par exemple, seul un certain compte peut nécessiter l'accès à une passerelle Internet.

Conditions préalables à la personnalisation

Avant de commencer à personnaliser les comptes, assurez-vous que ces conditions préalables sont réunies.

- Un AFT entièrement déployé. Pour plus d'informations sur le déploiement, consultezConfigurez et lancez votre AWS Control Tower Account Factory pour Terraform.
- `git`Référentiels préremplis pour les personnalisations globales et les personnalisations de compte dans votre environnement. Reportez-vous à l'étape 3 : renseigner chaque référentiel Étapes postérieures au déploiement pour plus d'informations.

Appliquer des personnalisations globales

Pour appliquer des personnalisations globales, vous devez transférer une structure de dossiers spécifique vers le référentiel de votre choix.

- Si vos configurations personnalisées prennent la forme de programmes ou de scripts Python, placez-les dans le dossier api_helpers/python de votre dépôt.
- Si vos configurations personnalisées prennent la forme de scripts Bash, placez-les dans le dossier api_helpers de votre dépôt.
- Si vos configurations personnalisées sont sous la forme de Terraform, placez-les dans le dossier terraform de votre référentiel.
- Reportez-vous au fichier README des personnalisations globales pour plus de détails sur la création de configurations personnalisées.

> **Note**
>
> Les personnalisations globales sont appliquées automatiquement, après l'étape du framework de provisionnement des comptes AFT dans le pipeline AFT.

Appliquer les personnalisations de compte

Vous pouvez appliquer des personnalisations de compte en transférant une structure de dossiers spécifique vers le référentiel de votre choix. Les personnalisations de compte sont appliquées automatiquement dans le pipeline AFT et après l'étape de personnalisation globale. Vous pouvez également créer plusieurs dossiers contenant différentes personnalisations de compte dans votre référentiel de personnalisations de compte. Pour chaque personnalisation de compte dont vous avez besoin, procédez comme suit.

Pour appliquer les personnalisations de compte

1. Étape 1 : Création d'un dossier pour la personnalisation d'un compte

   Dans le dépôt de votre choix, copiez le `ACCOUNT_TEMPLATE` dossier fourni par AFT dans un nouveau dossier. Le nom de votre nouveau dossier doit correspondre à celui `account_customizations_name` que vous avez indiqué dans votre demande de compte.

2. Ajoutez les configurations à votre dossier de personnalisation de compte spécifique

   Vous pouvez ajouter des configurations au dossier de personnalisation de votre compte en fonction du format de vos configurations.

   - Si vos configurations personnalisées prennent la forme de programmes ou de scripts Python, placez-les dans le dossier ***[account_customizations_name] /api_helpers/python*** qui se trouve dans votre dépôt.
   - Si vos configurations personnalisées prennent la forme de scripts Bash, placez-les dans le dossier ***[account_customizations_name] /api_helpers qui*** se trouve dans votre dépôt.
   - Si vos configurations personnalisées sont sous la forme de Terraform, placez-les dans le dossier ***[account_customizations_name]*** /terraform qui se trouve dans votre référentiel.

   Pour plus d'informations sur la création de configurations personnalisées, reportez-vous au fichier README de personnalisation du compte.

3. Reportez-vous au **`account_customizations_name`** paramètre spécifique dans le fichier de demande de compte

   Le fichier de demande de compte AFT inclut le paramètre d'entrée`account_customizations_name`. Entrez le nom de la personnalisation de votre compte comme valeur de ce paramètre.

> **Note**
>
> Vous pouvez soumettre plusieurs demandes de compte pour les comptes de votre environnement. Lorsque vous souhaitez appliquer des personnalisations de compte différentes ou similaires, spécifiez-les à l'aide du paramètre `account_customizations_name` d'entrée dans les demandes de compte. Pour plus d'informations, voir Soumettre des demandes de comptes multiples.

Réinvoquer les personnalisations

L'AFT fournit un moyen de réinvoquer les personnalisations dans le pipeline AFT. Cette méthode est utile lorsque vous avez ajouté une nouvelle étape de personnalisation ou lorsque vous apportez des modifications à une personnalisation existante. Lorsque vous le réappelez, AFT lance le pipeline de personnalisations pour apporter des modifications au compte provisionné par AFT. Une event-source-based réinvocation vous permet d'appliquer des personnalisations à des comptes individuels, à tous les comptes, à des comptes en fonction de leur unité d'organisation ou à des comptes sélectionnés en fonction de balises.

Suivez ces trois étapes pour réinvoquer les personnalisations pour les comptes provisionnés par AFT.

Étape 1 : transférer les modifications vers les référentiels globaux ou de personnalisation des **`git`** comptes

Vous pouvez mettre à jour vos personnalisations globales et de compte selon vos besoins et renvoyer les modifications à vos `git` référentiels. À ce stade, rien ne se passe. Le pipeline de personnalisations doit être invoqué par une source d'événements, comme expliqué dans les deux étapes suivantes.

Étape 2 : démarrer l'exécution d'une fonction AWS Step pour réinvoquer des personnalisations

AFT fournit une fonction AWS Step appelée `aft-invoke-customizations` dans le compte de gestion AFT. Le but de cette fonction est de réinvoquer le pipeline de personnalisation pour les comptes provisionnés par AFT.

Voici un exemple de schéma d'événement (format JSON) que vous pouvez créer pour transmettre des données à la fonction `aft-invoke-customizations` AWS Step.

```
{
  "include": [
    {
      "type": "all"
    },
    {
      "type": "ous",
      "target_value": [ "ou1","ou2"]
    },
    {
      "type": "tags",
      "target_value": [ {"key1": "value1"}, {"key2": "value2"}]
    },
    {
      "type": "accounts",
      "target_value": [ "acc1_ID","acc2_ID"]
    }
  ],

  "exclude": [
    {
      "type": "ous",
      "target_value": [ "ou1","ou2"]
    },
    {
      "type": "tags",
      "target_value": [ {"key1": "value1"}, {"key2": "value2"}]
    },
    {
      "type": "accounts",
      "target_value": [ "acc1_ID","acc2_ID"]
    }
  ]
}
```

L'exemple de schéma d'événement montre que vous pouvez choisir les comptes à inclure ou à exclure du processus de réappel. Vous pouvez filtrer par unité organisationnelle (UO), tags de compte et ID de compte. Si vous n'appliquez aucun filtre et que vous incluez la déclaration`"type":"all"`, la personnalisation pour tous les comptes provisionnés par AFT est à nouveau invoquée.

> **Note**
>
> Si votre version d'AWS Control Tower est 1.6.5 ou ultérieure, vous pouvez cibler des unités d'organisation imbriquées (avec la syntaxe`OU Name (ou-id-1234)`). Pour plus d'informations, consultez la rubrique suivante sur GitHub.

Une fois que vous avez renseigné les paramètres de l'événement, Step Functions s'exécute et invoque les personnalisations correspondantes. AFT peut invoquer un maximum de 5 personnalisations à la fois. Step Functions attend et tourne en boucle jusqu'à ce que tous les comptes correspondant aux critères de l'événement soient complets.

Étape 3 : surveillez la sortie de la fonction AWS Step et observez l' CodePipeline exécution d'AWS

- La sortie Step Function qui en résulte contient des identifiants de compte qui correspondent à la source d'événement d'entrée Step Function.
- Accédez à AWS CodePipeline sous Outils de développement et consultez les pipelines de personnalisation correspondants pour l'ID de compte.

Résolution des problèmes liés au suivi des demandes de personnalisation du compte AFT

Des flux de travail de personnalisation des comptes basés sur des AWS Lambda journaux d'émission contenant les identifiants du compte cible et des demandes de personnalisation. AFT vous permet de suivre et de résoudre les demandes de personnalisation avec Amazon CloudWatch Logs en vous fournissant des requêtes CloudWatch Logs Insights que vous pouvez utiliser pour filtrer les CloudWatch journaux liés à votre demande de personnalisation en fonction de votre compte cible ou de votre ID de demande de personnalisation. Pour plus d'informations, consultez la section Analyse des données de journal avec Amazon CloudWatch Logs dans le guide de l'utilisateur Amazon CloudWatch Logs.

Pour utiliser CloudWatch Logs Insights pour AFT

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le volet de navigation, choisissez Logs, puis Logs insights.
3. Choisissez Requêtes.

4. Sous Exemples de requêtes, choisissez Account Factory for Terraform, puis sélectionnez l'une des requêtes suivantes :

   - Journaux de personnalisation par identifiant de compte

   > **Note**
   >
   > Assurez-vous de remplacer *« YOUR-ACCOUNT-ID » par votre identifiant* de compte cible.

   ```
   fields @timestamp, log_message.account_id as target_account_id,
    log_message.customization_request_id as customization_request_id,
    log_message.detail as detail, @logStream
   | sort @timestamp desc
   | filter log_message.account_id == "YOUR-ACCOUNT-ID" and @message like /
   customization_request_id/
   ```

   - Journaux de personnalisation par ID de demande de personnalisation

   > **Note**
   >
   > Assurez-vous de remplacer *« YOUR-CUSTOMIZATION-REQUEST-ID » par votre ID de demande* de personnalisation. Vous pouvez trouver l'ID de votre demande de personnalisation dans la sortie de la machine d' AWS Step Functions état du framework de provisionnement de comptes AFT. Pour plus d'informations sur le cadre de provisionnement des comptes AFT, voir Pipeline de provisionnement des comptes AFT

   ```
   fields @timestamp, log_message.account_id as target_account_id,
    log_message.customization_request_id as customization_request_id,
    log_message.detail as detail, @logStream
   | sort @timestamp desc
   | filter log_message.customization_request_id == "YOUR-CUSTOMIZATION-REQUEST-ID"
   ```

5. Après avoir sélectionné une requête, assurez-vous de sélectionner un intervalle de temps, puis choisissez Exécuter la requête.

Alternatives pour le contrôle de version du code source dans AFT

AFT utilise nativement un système AWS CodeCommit de contrôle de version du code source (VCS), mais il en autorise d'autres CodeConnectionsqui répondent aux exigences de votre entreprise ou à votre architecture existante. Vous pouvez spécifier un VCS tiers dans le cadre des conditions préalables au déploiement de l'AFT.

AFT prend en charge les alternatives de contrôle du code source suivantes :

- GitHub
- GitHub Serveur d'entreprise
- BitBucket

Si vous le sélectionnez AWS CodeCommit comme VCS, aucune étape supplémentaire n'est requise. Par défaut, AFT crée les `git` référentiels nécessaires dans votre environnement, avec des noms par défaut. Toutefois, vous pouvez remplacer les noms de référentiel par défaut afin de respecter les CodeCommit normes de votre organisation, le cas échéant.

Mettre en place un autre système de contrôle de version du code source (VCS personnalisé) avec AFT

Pour configurer un autre système de contrôle de version du code source pour votre déploiement AFT, procédez comme suit.

Étape 1 : créer des **`git`** référentiels dans un système de contrôle de version (VCS) tiers pris en charge.

Si vous n'en utilisez pas AWS CodeCommit, vous devez créer des `git` référentiels dans votre environnement de fournisseur VCS tiers pris en charge par AFT pour les éléments suivants.

- Demandes de compte AFT. Exemple de code disponible. Pour plus d'informations sur les demandes de compte AFT, consultezCréation d'un nouveau compte auprès de l'AFT.
- Personnalisations du provisionnement des comptes AFT. Exemple de code disponible. Pour plus d'informations sur les personnalisations de provisionnement des comptes AFT, consultez. Créez votre compte AFT, provisionnement, personnalisation, machine à états
- Personnalisations globales d'AFT. Exemple de code disponible. Pour plus d'informations sur les personnalisations globales d'AFT, consultezPersonnaliser le compte.

- Personnalisations du compte AFT. Exemple de code disponible. Pour plus d'informations sur les personnalisations des comptes AFT, consultezPersonnaliser le compte.

Étape 2 : Spécifier les paramètres de configuration VCS requis pour le déploiement d'AFT

Les paramètres d'entrée suivants sont nécessaires pour configurer votre fournisseur VCS dans le cadre du déploiement AFT.

- vcs_provider : Si vous ne l'utilisez pas AWS CodeCommit, spécifiez le fournisseur VCS en tant que`"bitbucket"`, ou `"github"``"githubenterprise"`, en fonction de votre cas d'utilisation.
- github_enterprise_url : pour les clients GitHub Enterprise uniquement, spécifiez l'URL. GitHub
- account_request_repo_name : par défaut, cette valeur est définie sur pour les utilisateurs. `aft-account-request` AWS CodeCommit Si vous avez créé votre dépôt sous un nouveau nom dans CodeCommit ou dans un environnement de fournisseur VCS tiers pris en charge par AFT, mettez à jour cette valeur d'entrée avec le nom réel de votre dépôt. Pour BitBucket Github et GitHub Enterprise, le nom du référentiel doit être au format`[Org]/[Repo]`.
- account_customizations_repo_name : par défaut, cette valeur est définie sur « pour les utilisateurs ». `aft-account-customizations` AWS CodeCommit Si vous avez créé un référentiel sous un nouveau nom dans CodeCommit ou dans un environnement de fournisseur VCS tiers compatible avec AFT, mettez à jour cette valeur d'entrée avec le nom de votre référentiel. Pour BitBucket Github et GitHub Enterprise, le nom du référentiel doit être au format`[Org]/[Repo]`.
- account_provisioning_customizations_repo_name : par défaut, cette valeur est définie sur « pour les utilisateurs ». `aft-account-provisioning-customizations` AWS CodeCommit Si vous avez créé un référentiel sous un nouveau nom dans AWS CodeCommit ou dans un environnement de fournisseur VCS tiers compatible avec l'AFT, mettez à jour cette valeur d'entrée avec le nom de votre référentiel. Pour BitBucket Github et GitHub Enterprise, le nom du référentiel doit être au format`[Org]/[Repo]`.
- global_customizations_repo_name : par défaut, cette valeur est définie sur pour les utilisateurs. `aft-global-customizations` AWS CodeCommit Si vous avez créé un référentiel sous un nouveau nom dans CodeCommit ou dans un environnement de fournisseur VCS tiers compatible avec AFT, mettez à jour cette valeur d'entrée avec le nom de votre référentiel. Pour BitBucket Github et GitHub Enterprise, le nom du référentiel doit être au format`[Org]/[Repo]`.
- account_request_repo_branch : La branche est définie `main` par défaut, mais la valeur peut être remplacée.

Par défaut, les sources AFT proviennent de la `main` branche de chaque `git` dépôt. Vous pouvez remplacer la valeur du nom de branche par un paramètre d'entrée supplémentaire. Pour plus d'informations sur les paramètres d'entrée, reportez-vous au fichier README du module AFT Terraform.

Étape 3 : terminer la AWS CodeStar connexion pour les fournisseurs VCS tiers

Lorsque votre déploiement s'exécute, AFT crée les AWS CodeCommit référentiels requis ou crée une AWS CodeStar connexion pour le fournisseur VCS tiers que vous avez choisi. Dans ce dernier cas, vous devez vous connecter manuellement à la console du compte de gestion AFT pour terminer la AWS CodeStar connexion en attente. Consultez la AWS CodeStar documentation pour obtenir des instructions supplémentaires sur l'établissement de la AWS CodeStar connexion.

Protection des données

Le modèle de responsabilitéAWS partagée s'applique à la protection des données dans l'AFT. À des fins de protection des données, nous recommandons les meilleures pratiques suivantes en matière de sécurité.

- Suivez les directives de protection des données fournies par AWS Control Tower. Pour plus de détails, consultez Protection des données dans AWS Control Tower.
- Préservez la configuration d'état Terraform générée au moment du déploiement d'AFT. Pour plus de détails, consultez Déployez AWS Control Tower Account Factory pour Terraform (AFT).
- Changez régulièrement les informations d'identification sensibles conformément à la politique de sécurité de votre entreprise. Les jetons Terraform, les `git` jetons, etc. sont des exemples de secrets.

Chiffrement au repos

AFT crée des compartiments Amazon S3, des rubriques Amazon SNS, des files d'attente Amazon SQS et des bases de données Amazon DynamoDB qui sont chiffrées au repos à l'aide des clés du service de gestion des clés. AWS La rotation annuelle des clés KMS créées par AFT est activée par défaut. Si vous choisissez les distributions Terraform Cloud ou Terraform Enterprise de Terraform, AFT inclut un SecureString paramètre AWS Systems Manager pour stocker les valeurs des jetons Terraform sensibles.

AFT utilise AWS les services décrits dans Services relatifs aux composants le document qui sont, par défaut, chiffrés au repos. Pour plus de détails, consultez la AWS documentation de chaque AWS

service composant d'AFT et découvrez les pratiques de protection des données suivies par chaque service.

Chiffrement en transit

L'AFT s'appuie sur AWS les services décrits dans Services relatifs aux composants le présent document qui utilisent le chiffrement en transit, par défaut. Pour plus de détails, consultez la AWS documentation de chaque AWS service composant d'AFT et découvrez les pratiques de protection des données suivies par chaque service.

Pour les distributions Terraform Cloud ou Terraform Enterprise, AFT appelle une API de point de terminaison HTTPS pour accéder à votre organisation Terraform. Si vous choisissez un fournisseur de VCS tiers supporté par des AWS CodeStar connexions, AFT appelle une API de point de terminaison HTTPS pour accéder à votre organisation de fournisseur de VCS.

Supprimer un compte d'AFT

Cette rubrique décrit comment supprimer un compte d'AFT afin que le pipeline AFT arrête le déploiement et la mise à jour du compte.

> **Important**
>
> La suppression d'un compte du pipeline AFT est irréversible et peut entraîner une perte d'état.

Vous pouvez supprimer un compte d'AFT lorsque vous souhaitez fermer le compte d'une application retirée, isoler un compte compromis ou transférer un compte d'une organisation à une autre.

> **Note**
>
> La suppression d'un compte d'AFT est différente de la suppression d'un compte AWS Control Tower ou Compte AWS. Lorsque vous supprimez un compte d'AFT, AWS Control Tower le gère toujours. Pour supprimer un compte AWS Control Tower ou Compte AWSconsultez ce qui suit :
>
> - Annulez la gestion d'un compte dans le guide de l'utilisateur d'AWS Control Tower.
> - Fermeture d'un compte dans le guide deAWS Billing l'utilisateur.

Pour supprimer un compte des pipelines AFT

La procédure suivante décrit comment supprimer un compte d'AFT.

1. Supprimer le compte du **`git`** référentiel qui stocke les demandes de compte

   Dans le `git` référentiel où vous stockez les demandes de compte, supprimez la demande de compte pour le compte que vous souhaitez supprimer d'AFT.

   Lorsque vous supprimez une demande de compte du référentiel de demandes de compte, AFT supprime le pipeline de personnalisation et les métadonnées du compte. Pour plus d'informations, consultez les notes de mise à jour de la version 1.8.0 d'AFT on GitHub.
2. Supprimer l'espace de travail Terraform (pour les clients Terraform Cloud et Terraform Enterprise uniquement)

   Supprimez les espaces de travail de personnalisation globale et de personnalisation de compte pour le compte que vous souhaitez supprimer d'AFT.
3. Supprimer l'état Terraform du backend Amazon S3

   Dans le compte de gestion AFT, supprimez tous les dossiers pertinents contenus dans les compartiments Amazon S3 pour le compte que vous souhaitez supprimer d'AFT.

   > **Tip**
   >
   > Dans les exemples suivants, remplacez par le numéro *`012345678901`* d'identification du compte de gestion AFT.

   Exemple : Terraform OSS

   Lorsque vous choisissez Terraform OSS, vous trouvez 3 dossiers pour chaque compte dans les compartiments `aft-backend-`*`012345678901`*`-primary-region` et `aft-backend-`*`012345678901`*`-secondary-region` Amazon S3. Ces dossiers sont liés à l'état des personnalisations du compte, à l'état du pipeline de personnalisations et à l'état des personnalisations globales

   Exemple : Terraform Cloud ou Terraform Enterprise

Lorsque vous choisissez Terraform Cloud ou Terraform Enterprise, vous trouvez un dossier pour chaque compte dans les compartiments et Amazon `aft-backend-`*`012345678901`*`-primary-region` S3`aft-backend-`*`012345678901`*`-secondary-region`. Ces dossiers sont liés à l'état du pipeline de personnalisations.

Métriques opérationnelles

Par défaut, Account Factory for Terraform (AFT) envoie des métriques opérationnelles anonymes à. AWSNous utilisons ces données pour comprendre comment les clients utilisent l'AFT afin d'améliorer la qualité et les fonctionnalités de la solution. Vous pouvez refuser la collecte de données en modifiant un paramètre lors du déploiement d'AFT. Lorsque la collecte est activée, les données suivantes sont envoyées à AWS :

- Solution : l'identifiant spécifique à l'AFT
- Version : La version d'AFT
- Identifiant unique universel (UUID) : identifiant unique généré aléatoirement pour chaque déploiement AFT
- Horodatage : horodatage de la collecte de données
- Données : configuration AFT et mesures prises par le client

AWS est propriétaire des données collectées. La collecte de données est soumise à la AWS Politique de confidentialité.

> **Note**
>
> Les versions d'AFT antérieures à la version 1.6.0 ne communiquent pas les métriques d'utilisation à AWS.

Pour désactiver les statistiques de reporting, procédez comme suit :

- Définissez la valeur d'entrée de `aft_metrics_reporting` to `false` dans votre fichier de configuration d'entrée Terraform, comme indiqué dans l'exemple suivant, et redéployez AFT. Cette valeur est définie `true` par défaut, si vous ne la définissez pas explicitement.

Si vous copiez l'exemple, n'oubliez pas de remplacer les valeurs réelles de votre ID et de votre région par les éléments indiqués dans les chaînes parx.

```
module "control_tower_account_factory" {
source = "aws-ia/control_tower_account_factory/aws"

# Required Vars
ct_management_account_id    = "xxxxxxxxxxx"
log_archive_account_id      = "xxxxxxxxxxx"
audit_account_id            = "xxxxxxxxxxx"
aft_management_account_id   = "xxxxxxxxxxx"
ct_home_region              = "xx-xxxx-x"
tf_backend_secondary_region = "xx-xxxx-x"

# Optional Vars
aft_metrics_reporting = false    # to opt out, set this value to false
}
```

Guide de dépannage d'Account Factory pour Terraform (AFT)

Cette section peut vous aider à résoudre les problèmes courants que vous pouvez rencontrer lors de l'utilisation de Account Factory for Terraform (AFT).

Rubriques

- Problèmes généraux
- Problèmes liés à l'ouverture et à l'enregistrement du compte
- Problèmes liés à l'invocation des personnalisations
- Problèmes liés au flux de travail de personnalisation des comptes

Problèmes généraux

- Quotas AWS de ressources dépassés

  Si vos groupes de journaux indiquent que vous avez dépassé les quotas de AWS ressources, contactez le AWS Support. Account Factory utilise Services AWS des quotas de ressources qui incluent AWS CodeBuild AWS Organizations, et AWS Systems Manager. Pour plus d'informations, consultez les ressources suivantes :

  - Qu'est-ce que c'est AWS CodeBuild ? dans le guide de CodeBuild l'utilisateur.

  - Qu'est-ce que c'est AWS Organizations ? dans le Guide de l'utilisateur des Organizations.
  - Qu'est-ce que c'est AWS Systems Manager ? dans le Guide de l'utilisateur de Systems Manager.
- Version obsolète d'Account Factory

  Si vous rencontrez un problème et pensez qu'il s'agit d'un bogue, assurez-vous de disposer de la dernière version d'Account Factory. Pour plus d'informations, consultez Mettre à jour la version d'Account Factory.
- Des modifications locales ont été apportées au code source d'Account Factory

  Account Factory est un projet open source. AWS Control Tower prend en charge le code de base d'Account Factory. Si vous apportez une modification locale au code de base d'Account Factory, AWS Control Tower ne prend en charge votre déploiement d'Account Factory que dans la mesure du possible.
- Autorisations de rôle Account Factory insuffisantes

  Account Factory crée des rôles et des politiques IAM pour gérer les déploiements et les personnalisations de comptes vendus. Si vous modifiez ces rôles ou politiques, le pipeline Account Factory risque de ne pas être en mesure d'effectuer certaines actions. Pour plus d'informations, consultez la section Rôles obligatoires.
- Les référentiels de comptes ne sont pas correctement renseignés

  Assurez-vous de suivre les étapes postérieures au déploiement avant de provisionner des comptes.
- Ne pas détecter la dérive après avoir changé l'unité d'organisation manuellement

  > **Note**
  >
  > AWS Control Tower détecte automatiquement la dérive. Pour plus d'informations sur la résolution de la dérive, consultez la section Détecter et résoudre la dérive dans AWS Control Tower.

  La dérive n'est pas détectée lorsque l'unité organisationnelle (UO) est modifiée manuellement. Cela est dû à la nature événementielle d'Account Factory. Lorsqu'une demande de compte est soumise, la ressource gérée par Terraform est un élément Amazon DynamoDB, et non un compte direct. Une fois qu'un élément est modifié, la demande est placée dans une file d'attente, où AWS Control

Tower la traite via Service Catalog (le service qui gère les détails du compte). Si vous modifiez l'unité d'organisation manuellement, la dérive n'est pas détectée car la demande de compte n'a pas changé.

Problèmes liés à l'ouverture et à l'enregistrement du compte

- La demande de compte (adresse e-mail/nom) existe déjà

  Le problème entraîne généralement une défaillance du produit Service Catalog lors du provisionnement ou en tant que`ConditionalCheckFailedException`.

  Vous pouvez obtenir plus d'informations sur le problème en procédant de l'une des manières suivantes :

  - Passez en revue vos groupes de journaux Terraform ou CloudWatch Logs.
  - Passez en revue les échecs signalés dans la rubrique Amazon SNS. `aft-failure-notifications`
- Demande de compte mal formée

  Assurez-vous que votre demande de compte suit le schéma attendu. Pour des exemples, consultez terraform-aws-control_tower_account_factory on. GitHub
- Quotas de ressources dépassés pour les AWS Organisations

  Assurez-vous que votre demande de compte ne dépasse pas les quotas de AWS Organizations ressources. Pour plus d'informations, consultez la section Quotas pour AWS les organisations.

Problèmes liés à l'invocation des personnalisations

- Le compte cible n'est pas intégré à Account Factory

  Assurez-vous que tous les comptes inclus dans une demande de personnalisation ont été intégrés à Account Factory. Pour plus d'informations, voir Mettre à jour un compte existant.
- Le compte ciblé par la demande de personnalisation existe dans la **`aft-request-metadata`** table DynamoDB, mais pas dans le référentiel des demandes de compte

  Formatez votre demande d'invocation de personnalisation pour exclure le compte incriminé en effectuant l'une des opérations suivantes :

  - Dans le `aft-request-metadata` tableau DynamoDB, supprimez l'entrée faisant référence au compte qui ne figure plus dans le référentiel de demandes de compte.
  - Ne pas utiliser « tous » comme cible.
  - Ne pas cibler l'unité d'organisation à laquelle appartient le compte.
  - Ne pas cibler directement le compte.
- Jeton incorrect utilisé pour Terraform Cloud

  Assurez-vous d'avoir configuré le bon jeton. Terraform Cloud ne prend en charge que les jetons basés sur l'équipe, et non les jetons basés sur l'organisation.
- Impossible de créer le compte avant la création du pipeline de personnalisation du compte ; impossible de personnaliser le compte

  Apportez une modification à la spécification du compte dans le référentiel des demandes de compte. Lorsque vous apportez une modification, telle que la modification de la valeur d'une balise pour un compte, Account Factory suit le chemin qui tente de créer le pipeline, même si celui-ci n'existe pas.

Problèmes liés au flux de travail de personnalisation des comptes

Si vous rencontrez des problèmes liés au flux de personnalisation des comptes, assurez-vous que votre version d'AFT est 1.8.0 ou supérieure et que vous supprimez toutes les instances de métadonnées relatives au compte de votre table de requêtes DynamoDB.

Pour plus d'informations sur la version 1.8.0 d'AFT, voir la version 1.8.0 sur. GitHub

Pour plus d'informations sur la façon de vérifier et de mettre à jour votre version d'AFT, consultez ce qui suit :

- Vérifiez la version AFT
- Mettre à jour la version AFT

Vous pouvez également suivre et résoudre les demandes de personnalisation en utilisant les requêtes Amazon CloudWatch Logs Insights pour filtrer les journaux contenant votre compte cible et les identifiants de demande de personnalisation. Pour plus d'informations, consultez la section Résolution des problèmes liés au suivi des demandes de personnalisation du compte AFT.

Détectez et corrigez les dérives dans AWS Control Tower

L'identification et la résolution des problèmes de dérive sont des tâches opérationnelles régulières pour les administrateurs de comptes de gestion d'AWS Control Tower. La résolution de la dérive contribue à garantir votre conformité aux exigences de gouvernance.

Lorsque vous créez votre zone d'atterrissage, celle-ci ainsi que toutes les unités organisationnelles (UO), les comptes et les ressources sont conformes aux règles de gouvernance appliquées par les contrôles que vous avez choisis. Lorsque vous et les membres de votre organisation utilisez la zone d'atterrissage, des modifications de ce statut de conformité peuvent se produire. Certaines modifications peuvent être accidentelles, et d'autres peuvent être apportées intentionnellement pour répondre aux événements opérationnels prioritaires.

La détection de la dérive vous aide à identifier les ressources qui ont besoin de modifications ou de mises à jour de la configuration pour résoudre la dérive.

Détection de la dérive

AWS Control Tower détecte automatiquement la dérive. Pour détecter les dérives, le `AWSControlTowerAdmin` rôle nécessite un accès permanent à votre compte de gestion afin qu'AWS Control Tower puisse effectuer des appels d'API en lecture seule. AWS Organizations Ces appels d'API apparaissent sous forme d' AWS CloudTrail événements.

La dérive apparaît dans les notifications Amazon Simple Notification Service (Amazon SNS) qui sont agrégées dans le compte d'audit. Les notifications de chaque compte membre envoient des alertes à une rubrique Amazon SNS locale et à une fonction Lambda.

Pour les contrôles faisant partie de la norme de AWS Security Hub gestion des services : AWS Control Tower, la dérive est affichée sur les pages du compte et des détails du compte dans la console AWS Control Tower, ainsi que par le biais d'une notification Amazon SNS.

Les administrateurs de comptes membres peuvent (et dans le cadre des bonnes pratiques, ce devrait même être une obligation) s'abonner aux notifications de dérive SNS pour des comptes spécifiques. Par exemple, la rubrique `aws-controltower-AggregateSecurityNotifications` SNS fournit des notifications de dérive. La console AWS Control Tower indique aux administrateurs des comptes de gestion en cas de dérive. Pour plus d'informations sur les sujets SNS relatifs à la détection et à la notification de la dérive, consultez la section Prévention et notification de la dérive.

Déduplication des notifications de dérive

Si le même type de dérive se produit plusieurs fois sur le même ensemble de ressources, AWS Control Tower envoie une notification SNS uniquement pour l'instance initiale de dérive. Si AWS Control Tower détecte que cette instance de dérive a été corrigée, elle envoie une autre notification uniquement si la dérive se reproduit pour ces ressources identiques.

Exemples : la dérive du compte et la dérive du SCP sont gérées de la manière suivante

- Si vous modifiez le même SCP géré plusieurs fois, vous recevez une notification lorsque vous le modifiez pour la première fois.
- Si vous modifiez un SCP géré, puis que vous corrigez une dérive, puis que vous le modifiez à nouveau, vous recevrez deux notifications.
- Si un compte est déplacé plusieurs fois entre les mêmes unités d'organisation source et de destination, sans que la dérive soit réparée au préalable, une seule notification est envoyée, même si le compte a été transféré entre ces unités d'organisation à plusieurs reprises.

Types de dérive des comptes

- Compte transféré entre les unités d'organisation
- Compte supprimé de l'organisation

> **Note**
>
> Lorsque vous déplacez un compte d'une unité organisationnelle à une autre, les commandes de l'unité d'organisation précédente ne sont pas supprimées. Si vous activez un nouveau contrôle basé sur le crochet sur l'unité d'organisation de destination, l'ancien le contrôle basé sur un crochet est supprimé du compte et le nouveau contrôle le remplace. Les contrôles mis en œuvre avec les SCP et AWS Config les règles doivent toujours être supprimés manuellement lorsqu'un compte change d'UO.

Types de dérive politique

- SCP mis à jour
- SCP attaché à l'OU
- SCP détaché de l'OU
- SCP attaché au compte

Pour plus d'informations, consultez la section Types de dérive de la gouvernance.

Résolution de la dérive

Bien que la détection soit automatique, les étapes pour résoudre l'écart sont manuelles et doivent être effectuées via la console.

- De nombreux types de dérive peuvent être résolus via la page des paramètres de la zone d'atterrissage. Vous pouvez cliquer sur le bouton Réinitialiser dans la section Versions pour résoudre ces types de dérive.
- Si votre unité d'organisation compte moins de 300 comptes, vous pouvez remédier à la dérive des comptes provisionnés par Account Factory, ou à la dérive SCP, en sélectionnant Réenregistrer l'unité d'organisation sur la page de l'organisation ou sur la page des détails de l'unité d'organisation.
- Vous pouvez peut-être résoudre le problème de la dérive du compte, par exemple en Déplacement du compte membre mettant à jour un compte individuel. Pour plus d'informations, consultez Mettre à jour le compte dans la console.

⚠ Lorsque vous prenez des mesures pour résoudre le problème de dérive sur une version en zone d'atterrissage, deux comportements sont possibles.

- Si vous utilisez la dernière version de la zone d'atterrissage, lorsque vous sélectionnez Réinitialiser puis Confirmer, les ressources de votre zone d'atterrissage dérivée sont réinitialisées selon la configuration enregistrée d'AWS Control Tower. La version de la zone d'atterrissage reste la même.
- Si vous n'utilisez pas la dernière version, vous devez sélectionner Mettre à jour. La zone d'atterrissage est mise à niveau vers la dernière version de la zone d'atterrissage. La dérive est résolue dans le cadre de ce processus.

Considérations relatives à la dérive et aux scans SCP

AWS Control Tower analyse quotidiennement vos SCP gérés pour vérifier que les contrôles correspondants sont correctement appliqués et qu'ils n'ont pas été modifiés. Pour récupérer les SCP et les vérifier, AWS Control Tower appelle en votre AWS Organizations nom, en utilisant un rôle dans votre compte de gestion.

Si un scan effectué par AWS Control Tower détecte une dérive, vous recevrez une notification. AWS Control Tower envoie une seule notification par problème de dérive. Ainsi, si votre zone d'atterrissage est déjà en état de dérive, vous ne recevrez pas de notifications supplémentaires à moins qu'un nouvel élément de dérive ne soit trouvé.

AWS Organizations limite la fréquence à laquelle chacune de ses API peut être appelée. Cette limite est exprimée en transactions par seconde (TPS) et est connue sous le nom de limite TPS, de taux de régulation ou de taux de demandes d'API. Lorsqu'AWS Control Tower audite vos SCP en les appelant AWS Organizations, les appels d'API effectués par AWS Control Tower sont pris en compte dans votre limite de TPS, car AWS Control Tower utilise le compte de gestion pour effectuer les appels.

Dans de rares cas, cette limite peut être atteinte lorsque vous appelez les mêmes API à plusieurs reprises, que ce soit par le biais d'une solution tierce ou d'un script personnalisé que vous avez écrit. Par exemple, si vous et AWS Control Tower appelez les mêmes AWS Organizations API au même moment (dans un délai d'une seconde) et que les limites du TPS sont atteintes, les appels suivants sont limités. C'est-à-dire que ces appels renvoient une erreur telle que`Rate exceeded`.

Si le taux de demandes d'API est dépassé

- Si AWS Control Tower atteint la limite et est limitée, nous suspendons l'exécution de l'audit et le reprenons ultérieurement.
- Si votre charge de travail atteint la limite et est limitée, le résultat peut aller d'une légère latence à une erreur fatale dans la charge de travail, selon la façon dont la charge de travail est configurée. Il faut être conscient de cette coque Edge.

Un scan SCP quotidien consiste en

1. Récupération de vos unités d'organisation récemment actives.
2. Pour chaque unité d'organisation enregistrée, récupération de tous les SCP gérés par AWS Control Tower qui sont attachés à l'unité d'organisation. Les SCP gérés ont des identifiants qui commencent par. `aws-guardrails`
3. Pour chaque contrôle préventif activé sur l'UO, vérifier que la déclaration de politique du contrôle est présente dans les SCP gérés par l'UO.

Une UO peut avoir un ou plusieurs SCP gérés.

Types de dérive à résoudre immédiatement

La plupart des types de dérive peuvent être résolus par les administrateurs. Certains types de dérive doivent être résolus immédiatement, notamment la suppression d'une unité organisationnelle requise par la zone de landing zone d'AWS Control Tower. Voici quelques exemples de dérives majeures que vous souhaiterez peut-être éviter :

- Ne supprimez pas l'unité organisationnelle de sécurité : l'unité organisationnelle initialement nommée Security lors de la configuration de la zone d'atterrissage par AWS Control Tower ne doit pas être supprimée. Si vous le supprimez, vous verrez un message d'erreur vous demandant de réinitialiser immédiatement la zone d'atterrissage. Vous ne pourrez effectuer aucune autre action dans AWS Control Tower tant que la réinitialisation ne sera pas terminée.
- Ne supprimez pas les rôles obligatoires : AWS Control Tower vérifie certains rôles AWS Identity and Access Management (IAM) lorsque vous vous connectez à la console pour détecter toute dérive des rôles IAM. Si ces rôles sont absents ou inaccessibles, vous verrez une page d'erreur vous demandant de réinitialiser votre zone de landing zone. Ces rôles sont `AWSControlTowerAdmin` `AWSControlTowerCloudTrailRoleAWSControlTowerStackSetRole`.

  Pour plus d'informations sur ces rôles, consultezAutorisations requises pour utiliser la console AWS Control Tower.
- Ne supprimez pas toutes les unités d'organisation supplémentaires : si vous supprimez l'unité organisationnelle initialement nommée Sandbox lors de la configuration de la zone d'atterrissage par AWS Control Tower, votre zone de destination sera en état de dérive, mais vous pourrez toujours utiliser AWS Control Tower. Au moins une unité d'organisation supplémentaire est requise pour qu'AWS Control Tower fonctionne, mais il n'est pas nécessaire qu'il s'agisse de l'unité d'organisation Sandbox.
- Ne supprimez pas les comptes partagés : si vous supprimez des comptes partagés des UO de base, par exemple si vous supprimez le compte de journalisation de l'unité d'organisation de sécurité, votre zone de landing sera en état de dérive. La zone de landing zone doit être réinitialisée pour que vous puissiez continuer à utiliser la console AWS Control Tower.

Modifications réparables apportées aux ressources

Voici une liste des modifications autorisées apportées aux ressources d'AWS Control Tower, bien qu'elles créent une dérive susceptible d'être résolue. Les résultats de ces opérations autorisées sont visibles dans la console AWS Control Tower, mais une actualisation peut être nécessaire.

Pour plus d'informations sur la manière de résoudre la dérive qui en résulte, consultez Managing Resources Outside of AWS Control Tower.

Modifications autorisées en dehors de la console AWS Control Tower

- Modifiez le nom d'une unité d'organisation enregistrée.
- Modifiez le nom de l'unité d'organisation de sécurité.
- Modifiez le nom des comptes des membres dans les unités d'organisation non fondamentales.
- Modifiez le nom des comptes partagés AWS Control Tower dans l'unité d'organisation de sécurité.
- Supprimez une unité d'organisation non fondamentale.
- Supprimez un compte inscrit d'une unité d'organisation non fondamentale.
- Modifiez l'adresse e-mail d'un compte partagé dans l'unité d'organisation de sécurité.
- Modifiez l'adresse e-mail d'un compte membre dans une unité d'organisation enregistrée.

> **Note**
>
> Le transfert de comptes entre des unités d'organisation est considéré comme une dérive, et il faut y remédier.

Dérive et provisionnement de compte

Si votre zone d'atterrissage est en état de dérive, la fonctionnalité d'inscription d'un compte dans AWS Control Tower ne fonctionnera pas. Dans ce cas, vous devez provisionner les nouveaux comptes via AWS Service Catalog. Pour obtenir des instructions, veuillez consulter Provisionner des comptes avec AWS Service Catalog Account Factory .

En particulier, si vous avez apporté certaines modifications à vos comptes par le biais du Service Catalog, par exemple en modifiant le nom de votre portefeuille, la fonctionnalité d'inscription au compte ne fonctionnera pas.

Types de dérive de gouvernance

La dérive de la gouvernance, également appelée dérive organisationnelle, se produit lorsque les UO, les SCP et les comptes des membres sont modifiés ou mis à jour. Les types de dérive en matière de gouvernance qui peuvent être détectés dans AWS Control Tower sont les suivants :

- Déplacement du compte membre
- Suppression de compte membre
- Mise à jour non planifiée de la stratégie de contrôle de service gérée
- Stratégie de contrôle de service attachée au compte membre
- Stratégie de contrôle de service attachée à l'unité d'organisation gérée
- Stratégie de contrôle de service détachée de l'unité d'organisation gérée
- UO de base supprimée
- Security Hub contrôle la dérive
- Accès sécurisé désactivé

Un autre type de dérive est la dérive de la zone d'atterrissage, qui peut être détectée via le compte de gestion. La dérive de la zone d'atterrissage correspond à la dérive des rôles IAM, ou à tout type de dérive organisationnelle qui affecte spécifiquement les unités d'organisation fondamentales et les comptes partagés.

Un cas particulier de dérive de la zone d'atterrissage est la dérive des rôles, qui est détectée lorsqu'un rôle requis n'est pas disponible. Si ce type de dérive se produit, la console affiche une page d'avertissement et des instructions sur la façon de restaurer le rôle. Votre zone d'atterrissage n'est pas disponible tant que la dérive des rôles n'est pas résolue. Pour plus d'informations sur le drift, voir Ne pas supprimer les rôles obligatoires dans la section intitulée Types de dérive à résoudre immédiatement.

AWS Control Tower ne recherche aucune dérive en ce qui concerne les autres services qui fonctionnent avec le compte de gestion CloudTrail CloudWatch, notamment IAM Identity Center AWS CloudFormation AWS Config,,, etc. Aucune détection de dérive n'est disponible dans les comptes enfants, car ces comptes sont protégés par des contrôles obligatoires préventifs.

Cependant, il signale une dérive concernant les contrôles qui font partie de la norme de AWS Security Hub gestion des services : AWS Control Tower.

Déplacement du compte membre

Ce type de dérive se produit sur le compte plutôt que sur l'unité d'organisation. Ce type de dérive peut se produire lorsqu'un compte membre d'AWS Control Tower, le compte d'audit ou le compte d'archivage des journaux est déplacé d'une unité d'organisation AWS Control Tower enregistrée vers une autre unité d'organisation. Voici un exemple de notification Amazon SNS lorsque ce type de dérive est détecté.

```
{
  "Message" : "AWS Control Tower has detected that your member account 'account-
email@amazon.com (012345678909)' has been moved from organizational unit 'Sandbox
 (ou-0123-eEXAMPLE)' to 'Security (ou-3210-1EXAMPLE)'. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
move-account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ACCOUNT_MOVED_BETWEEN_OUS",
  "RemediationStep" : "Re-register this organizational unit (OU), or if the OU has more
 than 300 accounts, you must update the provisioned product in Account Factory.",
  "AccountId" : "012345678909",
  "SourceId" : "012345678909",
  "DestinationId" : "ou-3210-1EXAMPLE"
}
```

Résolutions

Lorsque ce type de dérive se produit pour un compte provisionné par Account Factory dans une unité d'organisation comptant jusqu'à 300 comptes, vous pouvez y remédier en :

- Accédez à la page Organisation dans la console AWS Control Tower, sélectionnez le compte, puis choisissez Mettre à jour le compte en haut à droite (option la plus rapide pour les comptes individuels).
- Accédez à la page Organisation dans la console AWS Control Tower, puis sélectionnez Ré-enregistrer pour l'unité d'organisation contenant le compte (option la plus rapide pour plusieurs comptes). Pour plus d'informations, consultez Enregistrer une unité organisationnelle existante auprès d'AWS Control Tower.

- Mettre à jour le produit approvisionné dans Account Factory. Pour plus d'informations, consultez Mettez à jour et déplacez les comptes Account Factory avec AWS Control Tower ou avec AWS Service Catalog.

  > **Note**
  >
  > Si vous avez plusieurs comptes individuels à mettre à jour, consultez également cette méthode pour effectuer des mises à jour avec un script :Fournir et mettre à jour des comptes à l'aide de l'automatisation.

- Lorsque ce type de dérive se produit dans une unité d'organisation comportant plus de 300 comptes, la résolution de la dérive peut dépendre du type de compte qui a été déplacé, comme expliqué dans les paragraphes suivants. Pour plus d'informations, consultez Mettre à jour votre zone de destination.
  - Si un compte approvisionné par Account Factory est déplacé : dans une unité d'organisation comptant moins de 300 comptes, vous pouvez résoudre le problème de dérive du compte en mettant à jour le produit approvisionné dans Account Factory, en réenregistrant l'unité d'organisation ou en mettant à jour votre zone de destination.

    Dans une unité d'organisation comptant plus de 300 comptes, vous devez résoudre le problème en mettant à jour chaque compte déplacé, soit via la console AWS Control Tower, soit via le produit provisionné, car le fait de réenregistrer l'unité d'organisation n'effectuera pas la mise à jour. Pour plus d'informations, consultez Mettez à jour et déplacez les comptes Account Factory avec AWS Control Tower ou avec AWS Service Catalog.
  - Si un compte partagé est déplacé : vous pouvez résoudre le problème lié au déplacement du compte d'audit ou d'archivage des journaux en mettant à jour votre zone de landing zone. Pour plus d'informations, consultez Mettre à jour votre zone de destination.

> **Nom de champ obsolète**
>
> Le nom du champ `MasterAccountID` a été modifié conformément aux AWS directives. `ManagementAccountID` L'ancien nom est obsolète. À partir de 2022, les scripts contenant le nom de champ obsolète ne fonctionneront plus.

Suppression de compte membre

Ce type de dérive peut se produire lorsqu'un compte membre est supprimé d'une unité organisationnelle enregistrée dans AWS Control Tower. L'exemple suivant montre la notification Amazon SNS lorsque ce type de dérive est détecté.

```
{
  "Message" : "AWS Control Tower has detected that the member account 012345678909 has
 been removed from organization o-123EXAMPLE. For more information, including steps
 to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/remove-
account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ACCOUNT_REMOVED_FROM_ORGANIZATION",
  "RemediationStep" : "Add account to Organization and update Account Factory
 provisioned product",
  "AccountId" : "012345678909"
}
```

Résolution

- Lorsque ce type de dérive se produit dans un compte membre, vous pouvez y remédier en mettant à jour le compte dans la console AWS Control Tower ou dans Account Factory. Par exemple, vous pouvez ajouter le compte à une autre unité d'organisation enregistrée à l'aide de l'assistant de mise à jour d'Account Factory. Pour plus d'informations, consultez Mettez à jour et déplacez les comptes Account Factory avec AWS Control Tower ou avec AWS Service Catalog.
- Si un compte partagé est supprimé d'une UO de base, vous devez résoudre le problème en réinitialisant votre zone de landing zone. Tant que cette dérive n'est pas résolue, vous ne pourrez pas utiliser la console AWS Control Tower.
- Pour de plus amples informations sur la résolution de la dérive pour les comptes et les UO, veuillez consulter Si vous gérez des ressources en dehors d'AWS Control Tower.

> **Note**
>
> Dans Service Catalog, le produit approvisionné par Account Factory qui représente le compte n'est pas mis à jour pour supprimer le compte. Au lieu de cela, le produit provisionné est

affiché en tant que TAINTED et il est dans un état d'erreur. Pour effectuer le nettoyage, accédez au Service Catalog, choisissez le produit approvisionné, puis choisissez Terminate.

Mise à jour non planifiée de la stratégie de contrôle de service gérée

Ce type de dérive peut se produire lorsqu'un SCP pour un contrôle est mis à jour dans la AWS Organizations console ou par programmation à l'aide du AWS CLI ou de l'un des kits SDK AWS. Voici un exemple de notification Amazon SNS lorsque ce type de dérive est détecté.

```
{
  "Message" : "AWS Control Tower has detected that the managed service control policy
 'aws-guardrails-012345 (p-tEXAMPLE)', attached to the registered organizational unit
 'Security (ou-0123-1EXAMPLE)', has been modified. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
update-scp'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_UPDATED",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
  "PolicyId" : "p-tEXAMPLE"
}
```

Résolution

Lorsque ce type de dérive se produit dans une unité d'organisation comptant jusqu'à 300 comptes, vous pouvez y remédier en :

- Accédez à la page Organisation de la console AWS Control Tower pour réenregistrer l'unité d'organisation (option la plus rapide). Pour plus d'informations, consultez Enregistrer une unité organisationnelle existante auprès d'AWS Control Tower.
- Mise à jour de votre zone d'atterrissage (option plus lente). Pour plus d'informations, consultez Mettre à jour votre zone de destination.

Lorsque ce type de dérive se produit dans une unité d'organisation comptant plus de 300 comptes, corrigez-le en mettant à jour votre zone de landing zone. Pour plus d'informations, consultez Mettre à jour votre zone de destination.

Stratégie de contrôle de service attachée à l'unité d'organisation gérée

Ce type de dérive peut se produire lorsqu'un SCP pour un contrôle est connecté à une autre unité d'organisation. Cela se produit particulièrement souvent lorsque vous travaillez sur vos unités d'organisation en dehors de la console AWS Control Tower. Voici un exemple de notification Amazon SNS lorsque ce type de dérive est détecté.

```
{
  "Message" : "AWS Control Tower has detected that the managed service control
 policy 'aws-guardrails-012345 (p-tEXAMPLE)' has been attached to the registered
 organizational unit 'Sandbox (ou-0123-1EXAMPLE)'. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
scp-detached-ou'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_ATTACHED_TO_OU",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
  "PolicyId" : "p-tEXAMPLE"
}
```

Résolution

Lorsque ce type de dérive se produit dans une unité d'organisation comptant jusqu'à 300 comptes, vous pouvez y remédier en :

- Accédez à la page Organisation de la console AWS Control Tower pour réenregistrer l'unité d'organisation (option la plus rapide). Pour plus d'informations, consultez Enregistrer une unité organisationnelle existante auprès d'AWS Control Tower.
- Mise à jour de votre zone d'atterrissage (option plus lente). Pour plus d'informations, consultez Mettre à jour votre zone de destination.

Lorsque ce type de dérive se produit dans une unité d'organisation comptant plus de 300 comptes, corrigez-le en mettant à jour votre zone de landing zone. Pour plus d'informations, consultez Mettre à jour votre zone de destination.

Stratégie de contrôle de service détachée de l'unité d'organisation gérée

Ce type de dérive peut se produire lorsqu'un SCP d'un contrôle a été détaché d'une UO gérée par AWS Control Tower. Ce phénomène est particulièrement fréquent lorsque vous travaillez en dehors de la console AWS Control Tower. Voici un exemple de notification Amazon SNS lorsque ce type de dérive est détecté.

```
{
  "Message" : "AWS Control Tower has detected that the managed service control
 policy 'aws-guardrails-012345 (p-tEXAMPLE)' has been detached from the registered
 organizational unit 'Sandbox (ou-0123-1EXAMPLE)'. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
scp-detached'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_DETACHED_FROM_OU",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
  "PolicyId" : "p-tEXAMPLE"
}
```

Résolution

Lorsque ce type de dérive se produit dans une unité d'organisation comptant jusqu'à 300 comptes, vous pouvez y remédier en :

- Accédez à l'unité d'organisation dans la console AWS Control Tower pour réenregistrer l'unité d'organisation (option la plus rapide). Pour plus d'informations, consultez Enregistrer une unité organisationnelle existante auprès d'AWS Control Tower.
- Mise à jour de votre zone d'atterrissage (option plus lente). Si la dérive affecte un contrôle obligatoire, le processus de mise à jour crée une nouvelle politique de contrôle des services (SCP) et l'attache à l'unité d'organisation pour résoudre la dérive. Pour plus d'informations sur la mise à jour de votre zone d'atterrissage, consultezMettre à jour votre zone de destination.

Lorsque ce type de dérive se produit dans une unité d'organisation comptant plus de 300 comptes, corrigez-le en mettant à jour votre zone de landing zone. Si la dérive affecte un contrôle obligatoire, le processus de mise à jour crée une nouvelle politique de contrôle des services (SCP) et l'attache

à l'unité d'organisation pour résoudre la dérive. Pour plus d'informations sur la mise à jour de votre zone d'atterrissage, consultezMettre à jour votre zone de destination.

Stratégie de contrôle de service attachée au compte membre

Ce type de dérive peut se produire lorsqu'un SCP pour un contrôle est associé à un compte dans la console Organizations. Les barrières de sécurité et leurs SCP peuvent être activés sur les unités d'organisation (et donc appliqués à tous les comptes inscrits d'une unité d'organisation) via la console AWS Control Tower. Voici un exemple de notification Amazon SNS lorsque ce type de dérive est détecté.

```
{
  "Message" : "AWS Control Tower has detected that the managed service control policy
 'aws-guardrails-012345 (p-tEXAMPLE)' has been attached to the member account 'account-
email@amazon.com (012345678909)'. For more information, including steps to resolve this
 issue, see 'https://docs.aws.amazon.com/console/controltower/scp-detached-account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_ATTACHED_TO_ACCOUNT",
  "RemediationStep" : "Re-register this organizational unit (OU)",
  "AccountId" : "012345678909",
  "PolicyId" : "p-tEXAMPLE"
}
```

Résolution

Ce type de dérive se produit sur le compte plutôt que sur l'unité d'organisation.

Lorsque ce type de dérive se produit pour les comptes d'une unité d'organisation de base, telle que l'unité d'organisation de sécurité, la solution consiste à mettre à jour votre zone d'atterrissage. Pour plus d'informations, consultez Mettre à jour votre zone de destination.

Lorsque ce type de dérive se produit dans une unité d'organisation non fondamentale comptant jusqu'à 300 comptes, vous pouvez y remédier en :

- Détacher le SCP AWS Control Tower du compte Account Factory.
- Accédez à l'unité d'organisation dans la console AWS Control Tower pour réenregistrer l'unité d'organisation (option la plus rapide). Pour plus d'informations, consultez Enregistrer une unité organisationnelle existante auprès d'AWS Control Tower.

Lorsque ce type de dérive se produit dans une unité d'organisation comportant plus de 300 comptes, vous pouvez tenter de le résoudre en mettant à jour la configuration d'usine du compte. Il se peut qu'il ne soit pas possible de le résoudre correctement. Pour plus d'informations, consultez Mettre à jour votre zone de destination.

UO de base supprimée

Ce type de dérive s'applique uniquement aux unités d'organisation AWS Control Tower Foundational, telles que l'unité d'organisation de sécurité. Cela peut se produire si une UO de base est supprimée en dehors de la console AWS Control Tower. Les UO de base ne peuvent pas être déplacées sans créer ce type de dérive, car déplacer une UO revient à la supprimer puis à l'ajouter à un autre endroit. Lorsque vous corrigez le problème en mettant à jour votre zone de landing zone, AWS Control Tower remplace l'unité d'organisation de base à son emplacement d'origine. L'exemple suivant montre une notification Amazon SNS que vous pouvez recevoir lorsque ce type de dérive est détecté.

```
{
  "Message" : "AWS Control Tower has detected that the registered organizational unit
 'Security (ou-0123-1EXAMPLE)' has been deleted. For more information, including steps
 to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/delete-
ou'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ORGANIZATIONAL_UNIT_DELETED",
  "RemediationStep" : "Delete organizational unit in Control Tower",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE"
}
```

Résolution

Comme cette dérive ne se produit que pour les UO de base, la solution consiste à mettre à jour la zone d'atterrissage. Lorsque d'autres types d'UO sont supprimés, AWS Control Tower est automatiquement mis à jour.

Pour de plus amples informations sur la résolution de la dérive pour les comptes et les UO, veuillez consulter Si vous gérez des ressources en dehors d'AWS Control Tower.

Security Hub contrôle la dérive

Ce type de dérive se produit lorsqu'un contrôle faisant partie de la norme de AWS Security Hub gestion des services : AWS Control Tower signale un état de dérive. Le AWS Security Hub service

lui-même ne signale aucun état de dérive pour ces commandes. Le service envoie plutôt ses résultats à AWS Control Tower.

Une dérive du contrôle de Security Hub peut également être détectée si AWS Control Tower n'a pas reçu de mise à jour de statut de la part de Security Hub depuis plus de 24 heures. Si ces résultats ne sont pas reçus comme prévu, AWS Control Tower vérifie que le contrôle est en dérive. L'exemple suivant montre une notification Amazon SNS que vous pouvez recevoir lorsque ce type de dérive est détecté.

```
{
"Message" : "AWS Control Tower has detected that an AWS Security Hub control
 was removed in your account example-account@amazon.com <mailto:example-
account@amazon.com>. The artifact deployed on the target OU and accounts does not match
 the expected template and configuration for the control. This mismatch indicates that
 configuration changes were made outside of AWS Control Tower. For more information,
 view Security Hub standard",
"MasterAccountId" : "123456789XXX",
"ManagementAccountId" : "123456789XXX",
"OrganizationId" : "o-123EXAMPLE",
"DriftType" : "SECURITY_HUB_CONTROL_DISABLED",
"RemediationStep" : "To remediate the issue, Re-register the OU, or remove the control
 and enable it again. If the problem persists, contact AWS support.",
"AccountId" : "7876543219XXX",
"ControlId" : "PYBETSAGNUZB",
"ControlName" : "EBS snapshots should not be publicly restorable",
"ApiControlIdentifier" : "arn:aws:controltower:us-east-1::control/PYBETSAGNUZB",
"Region" : "us-east-1"
}
```

Résolution

Pour les unités d'organisation comptant moins de 300 comptes, la solution consiste à réenregistrer l'unité d'organisation, ce qui rétablit le contrôle à son état d'origine. Pour n'importe quelle unité d'organisation, vous pouvez supprimer et réactiver le contrôle via la console ou les API AWS Control Tower, qui réinitialisent également le contrôle.

Pour de plus amples informations sur la résolution de la dérive pour les comptes et les UO, veuillez consulter Si vous gérez des ressources en dehors d'AWS Control Tower.

Accès sécurisé désactivé

Ce type de dérive s'applique aux zones d'atterrissage d'AWS Control Tower. Cela se produit lorsque vous désactivez l'accès sécurisé à AWS Control Tower AWS Organizations après avoir configuré votre zone de landing zone AWS Control Tower.

Lorsque l'accès sécurisé est désactivé, AWS Control Tower ne reçoit plus d'événements de modification de la part de AWS Organizations. AWS Control Tower s'appuie sur ces événements de changement pour rester synchronisée AWS Organizations. Par conséquent, AWS Control Tower risque de ne pas apporter de modifications organisationnelles aux comptes et aux unités d'organisation. C'est pourquoi il est important de réenregistrer chaque UO chaque fois que vous mettez à jour votre zone de landing zone.

Exemple : notification Amazon SNS

Voici un exemple de notification Amazon SNS que vous recevez lorsque ce type de dérive se produit.

```
{
  "Message" : "AWS Control Tower has detected that trusted access has been disabled in
 AWS Organizations. For more information, including steps to resolve this issue, see
 https://docs.aws.amazon.com/controltower/latest/userguide/drift.html#drift-trusted-
access-disabled",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "TRUSTED_ACCESS_DISABLED",
  "RemediationStep" : "Reset Control Tower landing zone."
}
```

Résolution

AWS Control Tower vous avertit lorsque ce type de dérive se produit dans la console AWS Control Tower. La solution consiste à réinitialiser la zone d'atterrissage de votre AWS Control Tower. Pour plus d'informations, consultez la section Résolution de la dérive.

Si vous gérez des ressources en dehors d'AWS Control Tower

AWS Control Tower configure les comptes, les unités organisationnelles et les autres ressources en votre nom, mais vous êtes le propriétaire de ces ressources. Vous pouvez modifier ces ressources au sein ou en dehors d'AWS Control Tower. L'endroit le plus courant pour modifier les ressources

en dehors d'AWS Control Tower est la AWS Organizations console. Cette rubrique décrit comment concilier les modifications apportées aux ressources d'AWS Control Tower lorsque vous effectuez les modifications en dehors d'AWS Control Tower.

Le changement de nom, la suppression et le déplacement de ressources en dehors de la console AWS Control Tower entraînent une désynchronisation de la console. De nombreuses modifications peuvent être réconciliées automatiquement. Certaines modifications nécessitent une réinitialisation de votre zone de landing zone, afin de mettre à jour les informations affichées dans la console AWS Control Tower.

En général, les modifications que vous apportez aux ressources d'AWS Control Tower en dehors de la console AWS Control Tower créent un état de dérive résoluble dans votre zone de landing zone. Pour plus d'informations sur ces modifications, consultez Modifications réparables apportées aux ressources.

Tâches nécessitant une réinitialisation de la zone d'atterrissage

- Suppression de l'unité d'organisation de sécurité (cas particulier, à ne pas faire à la légère.)
- Supprimer un compte partagé de l'unité d'organisation de sécurité (non recommandé)
- Mettre à jour, attacher ou détacher un SCP associé à l'unité d'organisation de sécurité.

Modifications mises à jour automatiquement par AWS Control Tower

- Modification de l'adresse e-mail d'un compte inscrit
- Renommer un compte inscrit
- Création d'une nouvelle unité organisationnelle (UO) de haut niveau
- Modification du nom d'une unité d'organisation enregistrée
- Suppression d'une unité d'organisation enregistrée (à l'exception de l'unité d'organisation de sécurité, qui nécessite une mise à jour.)
- Suppression d'un compte inscrit (sauf un compte partagé dans l'unité d'organisation de sécurité.)

> **Note**
>
> AWS Service Catalog gère les modifications différemment d'AWS Control Tower. AWS Service Catalog peut entraîner un changement de posture de gouvernance lorsqu'il concilie vos changements. Pour plus d'informations sur la mise à jour d'un produit provisionné,

consultez la section Mise à jour des produits provisionnés dans la AWS Service Catalog documentation.

Référence à des ressources extérieures à AWS Control Tower

Lorsque vous créez de nouvelles unités d'organisation et de nouveaux comptes en dehors d'AWS Control Tower, ils ne sont pas régis par AWS Control Tower, même s'ils peuvent être affichés.

Création d'une unité d'organisation

Les unités organisationnelles (UO) créées en dehors d'AWS Control Tower sont considérées comme non enregistrées. Ils sont affichés sur la page Organisation, mais ils ne sont pas régis par les contrôles de l'AWS Control Tower.

Création d'un compte

Les comptes créés en dehors d'AWS Control Tower sont appelés « Non inscrits ». Les comptes inscrits et non inscrits appartenant à une unité d'organisation enregistrée auprès d'AWS Control Tower sont affichés sur la page Organisation. Les comptes qui n'appartiennent pas à une unité d'organisation enregistrée peuvent être invités à l'aide de la AWS Organizations console. Cette invitation à adhérer n'a pas pour effet d'inscrire le compte dans AWS Control Tower ni d'étendre la gouvernance d'AWS Control Tower au compte. Pour étendre la gouvernance en inscrivant le compte, rendez-vous sur la page Organisation ou sur la page détaillée du compte dans AWS Control Tower et choisissez Inscrire un compte.

Modification externe des noms des ressources AWS Control Tower

Vous pouvez modifier les noms de vos unités organisationnelles (UO) et de vos comptes en dehors de la console AWS Control Tower, et la console est automatiquement mise à jour pour refléter ces modifications.

Modification du nom d'une unité d'organisation

Dans AWS Organizations, vous pouvez modifier le nom d'une unité d'organisation à l'aide de l' AWS Organizations API ou de la console. Lorsque vous modifiez le nom d'une unité d'organisation en dehors d'AWS Control Tower, la console AWS Control Tower reflète automatiquement le changement de nom. Toutefois, si vous approvisionnez vos comptes en utilisant AWS Service Catalog, vous devez également réinitialiser votre zone de landing afin de garantir la cohérence avec AWS Control Tower AWS Organizations. Le flux de travail de réinitialisation garantit la cohérence entre les services

pour les unités d'organisation de base et supplémentaires. Vous pouvez résoudre ce type de dérive depuis la page des paramètres de la zone d'atterrissage. Consultez la section intitulée « Résoudre la dérive » dansDétectez et corrigez les dérives dans AWS Control Tower.

AWS Control Tower affiche les noms des unités d'organisation sur la page Organisation du tableau de bord AWS Control Tower. Vous pouvez voir quand votre opération de réinitialisation de la zone d'atterrissage a réussi.

Renommer un compte inscrit

Chaque AWS compte possède un nom d'affichage qui peut être modifié par l'utilisateur root du compte dans la AWS Billing and Cost Management console. Lorsque vous renommez un compte inscrit dans AWS Control Tower, le changement de nom est automatiquement reflété dans AWS Control Tower. Pour plus d'informations sur la modification du nom d'un compte, consultez la section Gestion d'un AWS compte dans le Guide AWS de l'utilisateur de facturation.

Suppression de l'unité d'organisation de sécurité

Ce type de dérive est un cas particulier. Si vous supprimez l'UO de sécurité, vous verrez une page de message d'erreur vous demandant de réinitialiser votre zone de landing zone. Vous devez réinitialiser votre zone de landing zone avant de pouvoir effectuer toute autre action dans AWS Control Tower.

- Vous ne pourrez effectuer aucune action dans la console AWS Control Tower et vous ne pourrez pas créer de nouveaux comptes AWS Service Catalog tant que la réinitialisation ne sera pas terminée.
- Vous ne pourrez pas consulter la page des paramètres de la zone d'atterrissage pour y voir le bouton de réinitialisation.

Dans ce cas, le processus de réinitialisation de la zone d'atterrissage crée une nouvelle unité d'organisation de sécurité et déplace les deux comptes partagés vers la nouvelle unité d'organisation de sécurité. AWS Control Tower indique que les comptes Log Archive et Audit sont dérivés. Le même processus permet de résoudre le problème de dérive de ces comptes.

Si vous déterminez que vous devez supprimer l'unité d'organisation de sécurité, voici ce que vous devez savoir :

Avant de supprimer l'unité d'organisation de sécurité, vous devez vous assurer qu'elle ne contient aucun compte. Plus précisément, vous devez supprimer les comptes Log Archive et Audit de l'UO. Nous vous recommandons de déplacer ces comptes vers une autre unité d'organisation.

> **Note**
>
> La suppression de votre unité d'organisation sécurisée ne doit pas être effectuée sans mûre réflexion. Cette action peut créer des problèmes de conformité si la journalisation est suspendue temporairement et parce que certains contrôles risquent de ne pas être appliqués.

Pour de plus amples informations générales sur la dérive, veuillez consulter « Résolution de la dérive » dans Détectez et corrigez les dérives dans AWS Control Tower.

Supprimer un compte de l'unité d'organisation de sécurité

Nous vous déconseillons de supprimer les comptes partagés de votre organisation ou de les déplacer hors de l'unité d'organisation de sécurité. Si vous avez supprimé accidentellement un compte partagé, vous pouvez suivre les étapes de correction décrites dans cette section pour le restaurer.

- Depuis la console AWS Control Tower : pour démarrer le processus de correction, suivez les étapes de correction semi-manuelles. Assurez-vous que l'utilisateur ou le rôle que vous utilisez pour accéder à la console AWS Control Tower est autorisé à s'exécuter`organizations:InviteAccountToOrganization`. Si vous ne disposez pas de telles autorisations, suivez les étapes de correction manuelles, qui utilisent à la fois la console AWS Control Tower et la AWS Organizations console.
- À partir de la AWS Organizations console : ce processus de correction est une procédure légèrement plus longue et entièrement manuelle. Lorsque vous suivez les étapes de correction manuelles, vous passerez de la AWS Organizations console à la console AWS Control Tower. Lorsque vous travaillez dans AWS Organizations, vous aurez besoin d'un utilisateur ou d'un rôle doté de la politique `AWSOrganizationsFullAccess` gérée ou d'un équivalent. Lorsque vous travaillez dans la console AWS Control Tower, vous devez disposer d'un utilisateur ou d'un rôle doté de la politique `AWSControlTowerServiceRolePolicy` gérée ou d'une autorisation équivalente, et être autorisé à exécuter toutes les actions de la tour de contrôle AWS (tour de contrôle : *).
- Si les étapes de correction ne permettent pas de restaurer le compte, contactez AWS Support.

Les conséquences de la suppression d'un compte partagé sont les suivantes AWS Organizations :

- Le compte n'est plus protégé par les contrôles obligatoires d'AWS Control Tower avec des politiques de contrôle des services (SCP). Résultat : les ressources créées par AWS Control Tower dans le compte peuvent être modifiées ou supprimées.
- Le compte ne figure plus dans le compte AWS Organizations de gestion. Résultat : l'administrateur du compte de AWS Organizations gestion n'a plus aucune visibilité sur les dépenses du compte.
- Il n'est plus garanti que le compte soit surveillé par AWS Config. Résultat : l'administrateur du compte de AWS Organizations gestion risque de ne pas être en mesure de détecter les modifications des ressources.
- Le compte n'appartient plus à l'organisation. Résultat : les mises à jour et la réinitialisation d'AWS Control Tower échoueront.

Pour restaurer un compte partagé à l'aide de la console AWS Control Tower (procédure semi-manuelle)

1. Connectez-vous à la console AWS Control Tower à l'adresse https://console.aws.amazon.com/controltower. Vous devez vous connecter en tant qu'utilisateur IAM, utilisateur dans IAM Identity Center ou en tant que rôle autorisé à exécuter. `organizations:InviteAccountToOrganization` Si vous ne disposez pas de telles autorisations, utilisez la procédure de correction manuelle décrite plus loin dans cette rubrique.
2. Sur la page Déviation détectée dans la zone d'atterrissage, choisissez Réinviter pour remédier à la suppression du compte partagé en réinvitant le compte partagé dans l'organisation. Un e-mail généré automatiquement est envoyé à l'adresse e-mail associée au compte.
3. Acceptez l'invitation à réintégrer le compte partagé dans l'organisation. Effectuez l'une des actions suivantes :

   - Connectez-vous au compte partagé qui a été supprimé, puis rendez-vous sur https://console.aws.amazon.com/organizations/home#/invites
   - Si vous avez accès au message électronique envoyé lorsque vous avez réinvité le compte, connectez-vous au compte supprimé, puis cliquez sur le lien contenu dans le message pour accéder directement à l'invitation du compte.
   - Si le compte partagé qui a été supprimé n'appartient pas à une autre organisation, connectez-vous au compte, ouvrez la AWS Organizations console et accédez à Invitations.

4. Connectez-vous à nouveau au compte de gestion ou rechargez la console AWS Control Tower si elle est déjà ouverte. Vous verrez la page de dérive de la zone d'atterrissage. Choisissez Réinitialiser pour réparer la zone d'atterrissage.
5. Attendez que le processus de réinitialisation soit terminé.

Si la correction est réussie, le compte partagé apparaît dans un état et une conformité normaux.

Si les étapes de correction ne permettent pas de restaurer le compte, contactez AWS Support.

Pour restaurer un compte partagé à l'aide de l'AWS Control Tower et des AWS Organizations consoles (correction manuelle)

1. Connectez-vous à la AWS Organizations console à l'adressehttps://console.aws.amazon.com/organizations/. Vous devez vous connecter en tant qu'utilisateur IAM, utilisateur dans IAM Identity Center ou en tant que rôle doté de la politique `AWSOrganizationsFullAccess` gérée ou d'un équivalent.
2. Réinvitez le compte partagé dans l'organisation. Pour plus d'informations sur les exigences, les prérequis et la procédure d'invitation d'un compte AWS Organizations, consultez la section Inviter un AWS compte dans votre organisation dans le Guide de l'AWS Organizations utilisateur.
3. Connectez-vous au compte partagé qui a été supprimé, puis rendez-vous sur https://console.aws.amazon.com/organizations/home#/invites pour accepter l'invitation.
4. Connectez-vous à nouveau au compte de gestion.
5. Connectez-vous à la console AWS Control Tower en tant qu'utilisateur ou en tant que rôle doté de la politique `AWSControlTowerServiceRolePolicy` gérée ou d'une version équivalente, et des autorisations nécessaires pour exécuter toutes les actions d'AWS Control Tower (tour de contrôle : *).
6. Vous verrez la page de dérive de la zone d'atterrissage avec une option permettant de réinitialiser la zone d'atterrissage. Choisissez Réinitialiser pour réparer la zone d'atterrissage.
7. Attendez que le processus de réinitialisation soit terminé.

Si la correction est réussie, le compte partagé apparaît dans un état et une conformité normaux.

Si les étapes de correction ne permettent pas de restaurer le compte, contactez AWS Support.

Modifications externes mises à jour automatiquement

Les modifications que vous apportez aux adresses e-mail de votre compte sont mises à jour automatiquement par AWS Control Tower, mais Account Factory ne les met pas automatiquement à jour.

Modification de l'adresse e-mail d'un compte régi

AWS Control Tower récupère et affiche les adresses e-mail conformément aux exigences de l'expérience de la console. Par conséquent, les adresses e-mail partagées et autres sont mises à jour et affichées de manière cohérente dans AWS Control Tower une fois que vous les avez modifiées.

> **Note**
>
> Dans AWS Service Catalog, Account Factory affiche les paramètres qui ont été spécifiés dans la console lorsque vous avez créé un produit provisionné. Toutefois, l'adresse e-mail du compte d'origine n'est pas mise à jour automatiquement lorsque l'adresse e-mail du compte change. En effet, le compte est contenu conceptuellement dans le produit provisionné ; il n'est pas le même que le produit provisionné. Pour mettre à jour cette valeur, vous devez mettre à jour le produit provisionné, ce qui peut entraîner une modification de la posture de gouvernance.

Appliquer des AWS Config règles externes

AWS Control Tower affiche l'état de conformité de toutes les AWS Config règles déployées dans les unités organisationnelles enregistrées auprès d'AWS Control Tower, y compris les règles activées en dehors de la console AWS Control Tower.

Suppression de ressources AWS Control Tower en dehors d'AWS Control Tower

Vous pouvez supprimer des unités d'organisation et des comptes dans AWS Control Tower et vous n'avez aucune autre action à effectuer pour voir les mises à jour. Account Factory est automatiquement mis à jour lorsque vous supprimez une unité d'organisation, mais pas lorsque vous supprimez un compte.

Supprimer une unité d'organisation enregistrée (à l'exception de l'unité d'organisation de sécurité)

Vous pouvez AWS Organizations y supprimer des unités d'organisation (UO) vides à l'aide de l'API ou de la console. Les informations d'origine contenant des comptes ne peuvent pas être supprimées.

AWS Control Tower reçoit une notification AWS Organizations lorsqu'une unité d'organisation est supprimée. Il met à jour la liste des unités d'organisation dans Account Factory, afin que la liste des unités d'organisation enregistrées reste cohérente.

> **Note**
>
> Dans AWS Service Catalog, Account Factory est mis à jour pour supprimer l'unité d'organisation supprimée de la liste des unités d'organisation disponibles dans lesquelles vous pouvez créer un compte.

Suppression d'un compte inscrit d'une unité d'organisation

Lorsque vous supprimez un compte inscrit, AWS Control Tower reçoit une notification et effectue des mises à jour afin que les informations restent cohérentes.

> **Note**
>
> Dans AWS Service Catalog, le produit approvisionné par Account Factory qui représente le compte gouverné n'est pas mis à jour pour supprimer le compte. Au lieu de cela, le produit provisionné est affiché en tant que `TAINTED` et il est dans un état d'erreur. Pour nettoyer, accédez à AWS Service Catalog, choisissez le produit provisionné, puis choisissez Terminer.

Gérez les organisations et les comptes avec AWS Control Tower

Toutes les unités organisationnelles (UO) et tous les comptes que vous créez dans AWS Control Tower sont régis automatiquement par AWS Control Tower. De plus, si vous avez des UO et des comptes existants qui ont été créés en dehors d'AWS Control Tower, vous pouvez les intégrer à la gouvernance d'AWS Control Tower.

Pour les comptes existants AWS Organizations et les AWS comptes, la plupart des clients préfèrent inscrire des groupes de comptes en enregistrant l'ensemble de l'unité organisationnelle (UO) qui contient les comptes. Vous pouvez également créer des comptes individuellement. Pour plus d'informations sur l'inscription de comptes individuels, consultezInscrire un existant Compte AWS.

Terminologie

- Lorsque vous intégrez une organisation existante dans AWS Control Tower, cela s'appelle enregistrer l'organisation ou étendre la gouvernance à l'organisation.
- Lorsque vous ajoutez un AWS compte à AWS Control Tower, cela s'appelle l'inscrire.

Consultez vos unités d'organisation et vos comptes

Sur la page AWS Control Tower Organization, vous pouvez consulter toutes les unités d'organisation de votre organisation AWS Organizations, y compris les unités d'organisation enregistrées auprès d'AWS Control Tower et celles qui ne le sont pas. Vous pouvez afficher les unités d'organisation imbriquées dans le cadre de la hiérarchie. Pour visualiser facilement vos unités organisationnelles sur la page Organisation, sélectionnez Unités organisationnelles uniquement dans le menu déroulant en haut à droite.

La page Organisation répertorie tous les comptes de votre organisation, quel que soit l'unité d'organisation ou le statut d'inscription dans AWS Control Tower. Pour consulter facilement vos comptes sur la page Organisation, sélectionnez Comptes uniquement dans le menu déroulant en haut à droite. Vous pouvez consulter, mettre à jour et inscrire des comptes individuellement au sein des unités d'organisation, si les comptes répondent aux conditions requises pour l'inscription.

Si vous ne sélectionnez aucun filtre, la page Organisation affiche vos comptes et vos unités d'organisation dans une hiérarchie. Il s'agit d'un emplacement central pour surveiller et prendre

des mesures sur toutes vos ressources AWS Control Tower. Pour plus d'informations sur la page Organisation, vous pouvez visionner la vidéo de présentation.

Vidéo de procédure

Cette vidéo (4:01) explique comment utiliser la page Organisation dans AWS Control Tower. Pour un visionnage de meilleure qualité, sélectionnez l'icône dans le coin inférieur droit de la vidéo pour l'afficher en plein écran. Le sous-titrage est disponible.

Présentation vidéo de l'utilisation de la page d'organisation dans AWS Control Tower.

Rubriques

- Enregistrer une unité organisationnelle existante auprès d'AWS Control Tower
- Inscrire un existant Compte AWS

Étendre la gouvernance à une organisation existante

Vous pouvez ajouter la gouvernance d'AWS Control Tower à une organisation existante en configurant une zone d'atterrissage (LZ), comme indiqué dans le guide de l'utilisateur d'AWS Control Tower à l'étape 2 de Getting Started.

Voici à quoi vous attendre lorsque vous configurez votre zone de landing zone AWS Control Tower dans une organisation existante.

- Vous ne pouvez avoir qu'une seule zone de landing zone par AWS Organizations organisation.
- AWS Control Tower utilise le compte de gestion de votre AWS Organizations organisation existante comme compte de gestion. Aucun nouveau compte de gestion n'est nécessaire.
- AWS Control Tower configure deux nouveaux comptes dans une unité d'organisation enregistrée : un compte d'audit et un compte de journalisation.
- Les limites de service de votre organisation doivent permettre la création de ces deux comptes supplémentaires.
- Une fois que vous avez lancé votre zone d'atterrissage ou enregistré une unité d'organisation, les contrôles d'AWS Control Tower s'appliquent automatiquement à tous les comptes inscrits dans cette unité d'organisation.
- Vous pouvez inscrire des AWS comptes existants supplémentaires dans une unité d'organisation régie par AWS Control Tower, afin que les contrôles s'appliquent à ces comptes.

- Vous pouvez ajouter d'autres unités d'organisation dans AWS Control Tower et enregistrer des unités d'organisation existantes.

Pour vérifier les autres conditions requises pour l'enregistrement et l'inscription, consultez Getting Started with AWS Control Tower.

Voici plus de détails sur la façon dont les contrôles d'AWS Control Tower ne s'appliquent pas à vos unités d'organisation dans les organisations AWS qui n'ont pas configuré de zones d'atterrissage AWS Control Tower :

- Les nouveaux comptes créés en dehors d'AWS Control Tower Account Factory ne sont pas soumis aux contrôles de l'unité d'organisation enregistrée.
- Les nouveaux comptes créés dans des unités d'organisation qui ne sont pas enregistrées auprès d'AWS Control Tower ne sont pas soumis à des contrôles, sauf si vous inscrivez spécifiquement ces comptes dans AWS Control Tower. Veuillez consulter Inscrire un existant Compte AWS pour de plus amples informations sur l'inscription de comptes.
- Les organisations existantes supplémentaires, les comptes existants et les nouvelles unités d'organisation ou les comptes que vous créez en dehors d'AWS Control Tower ne sont pas liés par les contrôles d'AWS Control Tower, sauf si vous enregistrez l'unité d'organisation ou que vous inscrivez le compte séparément.

Pour plus d'informations sur la façon d'appliquer AWS Control Tower aux UO et aux comptes existants, consultezEnregistrer une unité organisationnelle existante auprès d'AWS Control Tower.

Pour une présentation du processus de configuration d'une zone de landing zone AWS Control Tower dans votre organisation existante, regardez la vidéo dans la section suivante.

> **Note**
>
> Lors de la configuration, AWS Control Tower effectue des vérifications préliminaires afin d'éviter les problèmes courants. Toutefois, si vous utilisez actuellement la solution AWS Landing Zone pour AWS Organizations, contactez votre architecte de AWS solutions avant d'essayer d'activer AWS Control Tower dans votre organisation afin de déterminer si AWS Control Tower peut interférer avec le déploiement actuel de votre zone d'atterrissage. Consultez également Et si le compte ne répond pas aux prérequis ? les informations relatives au transfert de comptes d'une zone d'atterrissage à une autre.

Vidéo : Activer une zone d'atterrissage dans une zone existante AWS Organizations

Cette vidéo (7:48) explique comment configurer et activer une zone d'atterrissage AWS Control Tower dans les AWS Organizations structures existantes. Pour un visionnage de meilleure qualité, sélectionnez l'icône dans le coin inférieur droit de la vidéo pour l'afficher en plein écran. Le sous-titrage est disponible.

Activez AWS Control Tower pour les organisations existantes

Considérations relatives à IAM Identity Center et aux organisations existantes

- Si AWS IAM Identity Center (IAM Identity Center) est déjà configuré, la région d'origine d'AWS Control Tower doit être identique à la région du centre d'identité IAM.
- AWS Control Tower ne supprime pas une configuration existante.
- Si IAM Identity Center est déjà activé et si vous utilisez le répertoire IAM Identity Center, AWS Control Tower ajoute des ressources telles que des ensembles d'autorisations, des groupes, etc., et procède comme d'habitude.
- Si un autre répertoire (externe, AD, Managed AD) est configuré, AWS Control Tower ne modifie pas la configuration existante. Pour en savoir plus, consultez Considérations pour les AWS IAM Identity Center clients (IAM Identity Center).

Accès à d'autres AWS services

Une fois que vous avez intégré votre organisation à la gouvernance d'AWS Control Tower, vous avez toujours accès à tous les AWS services disponibles via AWS Organizationsla AWS Organizations console et les API. Pour de plus amples informations, veuillez consulter Services AWS connexes.

UO imbriquées dans AWS Control Tower

Ce chapitre répertorie les attentes et les considérations dont vous devez tenir compte lorsque vous travaillez avec des unités d'organisation imbriquées dans AWS Control Tower. Dans la plupart des cas, travailler avec des unités d'organisation imbriquées revient à travailler avec une structure d'unité d'organisation plate. Les fonctionnalités d'enregistrement et de réenregistrement fonctionnent avec

des unités d'organisation imbriquées, à l'exception des comportements modifiés décrits dans ce chapitre.

Vidéo de procédure

Cette vidéo (4:46) explique comment gérer les déploiements d'unités d'organisation imbriquées dans AWS Control Tower. Pour un visionnage de meilleure qualité, sélectionnez l'icône dans le coin inférieur droit de la vidéo pour l'afficher en plein écran. Le sous-titrage est disponible.

Présentation vidéo de la gestion des unités d'organisation imbriquées dans AWS Control Tower.

Pour obtenir des conseils concernant les meilleures pratiques relatives aux unités d'organisation imbriquées et à votre zone d'atterrissage, consultez le billet de blog Organizing your AWS Control Tower landing zone with nested UO.

Passez d'une structure d'unité d'organisation plate à une structure d'unité d'organisation imbriquée

Si vous avez créé votre zone de landing zone AWS Control Tower avec une structure d'UO plate, vous pouvez l'étendre à une structure d'UO imbriquée.

Ce processus comporte quatre étapes principales :

1. Créez la structure d'unité d'organisation imbriquée de votre choix dans AWS Control Tower.
2. Accédez à la AWS Organizations console et utilisez leur fonction de transfert groupé pour déplacer les comptes de l'unité d'organisation source (plate) vers l'unité d'organisation de destination (imbriquée). Voici comment procéder :
   a. Accédez à l'unité d'organisation à partir de laquelle vous souhaitez déplacer des comptes.
   b. Sélectionnez tous les comptes de l'unité d'organisation.
   c. Choisissez Déplacer.

   > **Note**
   >
   > Cette étape doit être effectuée dans la AWS Organizations console car AWS Control Tower ne possède pas de fonctionnalité Move.

3. Accédez à l'unité d'organisation imbriquée dans AWS Control Tower et enregistrez-la ou réenregistrez-la. Tous les comptes de l'unité d'organisation imbriquée seront inscrits.
   - Si vous avez créé l'unité d'organisation dans AWS Control Tower, réenregistrez-la.

- Si vous avez créé l'unité d'organisation dans AWS Organizations, enregistrez l'unité d'organisation pour la première fois.

4. Une fois vos comptes déplacés et inscrits, supprimez l'unité d'organisation de premier niveau vide, soit depuis la AWS Organizations console, soit depuis la console AWS Control Tower.

Contrôles préalables à l'enregistrement des unités d'exploitation imbriquées

Pour garantir l'enregistrement réussi de vos unités d'organisation imbriquées et de leurs comptes membres, AWS Control Tower effectue une série de vérifications préalables. Ces mêmes prévérifications sont effectuées lors de l'enregistrement d'une unité d'organisation de premier niveau ou d'une unité d'organisation imbriquée. Pour plus d'informations, consultez la section Causes courantes d'échec lors de l'enregistrement ou du réenregistrement.

- Si tous les précontrôles sont réussis, AWS Control Tower commence à enregistrer automatiquement votre unité d'organisation.
- Si l'une des vérifications préalables échoue, AWS Control Tower arrête le processus d'enregistrement et vous fournit une liste des éléments à corriger avant que vous puissiez enregistrer votre unité d'organisation.

UO et rôles imbriqués

AWS Control Tower déploie le `AWSControlTowerExecution` rôle sur les comptes de l'unité d'organisation cible et sur les comptes de toutes les unités d'organisation imbriquées sous l'unité d'organisation cible, même si votre intention est d'enregistrer uniquement l'unité d'organisation cible. Ce rôle donne à tout utilisateur du compte de gestion des autorisations d'administrateur sur tout compte doté de ce `AWSControlTowerExecution` rôle. Le rôle peut être utilisé pour effectuer des actions qui seraient normalement interdites par les contrôles d'AWS Control Tower.

Vous pouvez supprimer ce rôle des comptes non inscrits que vous n'avez pas l'intention d'inscrire. Si vous supprimez ce rôle, vous ne pouvez pas inscrire le compte auprès d'AWS Control Tower, ni enregistrer les unités d'organisation parentes immédiates, sauf si vous restaurez le rôle sur le compte. Pour supprimer le `AWSControlTowerExecution` rôle d'un compte, vous devez être connecté sous le `AWSControlTowerExecution` rôle, car aucun autre responsable IAM n'est autorisé à supprimer des rôles gérés par AWS Control Tower.

Pour plus d'informations sur la façon de restreindre l'accès aux rôles, consultez la section Conditions facultatives relatives à vos relations de confiance en matière de rôles.

Que se passe-t-il lors de l'enregistrement et du réenregistrement des unités d'organisation et des comptes imbriqués

Lorsque vous enregistrez ou réenregistrez une unité d'organisation imbriquée, AWS Control Tower inscrit tous les comptes non inscrits de l'unité d'organisation cible et met à jour tous les comptes inscrits. Voici ce à quoi vous pouvez vous attendre.

AWS Control Tower exécute les tâches suivantes

- Ajoute le `AWSControlTowerExecution` rôle à tous les comptes non inscrits dans cette unité d'organisation et à tous les comptes non inscrits dans ses unités d'organisation imbriquées.
- Enregistre les comptes de membres qui ne sont pas inscrits.
- Réinscrit les comptes des membres inscrits.
- Crée un identifiant IAM Identity Center pour les comptes de membres nouvellement inscrits.
- Met à jour les comptes des membres inscrits existants pour refléter les modifications de votre zone de landing zone.
- Met à jour les contrôles configurés pour cette unité d'organisation et ses comptes membres.

Considérations relatives à l'enregistrement des unités d'organisation imbriquées

- Vous ne pouvez pas enregistrer une UO sous l'UO principale (UO de sécurité).
- Les unités d'organisation imbriquées doivent être enregistrées séparément.
- Vous ne pouvez pas enregistrer une UO si son UO parent n'est pas enregistrée.
- Vous ne pouvez pas enregistrer une UO à moins que toutes les UO situées plus haut dans l'arborescence n'aient été enregistrées avec succès à un moment ou à un autre (certaines ont peut-être été supprimées).
- Vous pouvez enregistrer une UO située sous une UO supérieure dérivée, mais cette action ne répare pas cette dérive.

Limites de l'UO imbriquée

- Les unités d'organisation peuvent être imbriquées à un maximum de 5 niveaux de profondeur sous la racine.

- Les unités d'organisation imbriquées sous l'unité d'organisation cible doivent être enregistrées ou réenregistrées séparément.
- Si l'unité d'organisation cible se situe au niveau 2 ou inférieur dans la hiérarchie, c'est-à-dire s'il ne s'agit pas d'une unité d'organisation de niveau supérieur, les contrôles préventifs activés sur les unités d'organisation supérieures sont automatiquement appliqués à cette unité d'organisation et à toutes les unités inférieures.
- Les échecs d'enregistrement de l'unité organisationnelle ne se propagent pas dans l'arborescence hiérarchique. Vous pouvez consulter les détails relatifs à l'état des unités d'organisation imbriquées sur la page de détails des unités d'organisation du parent.
- Les échecs d'enregistrement de l'unité organisationnelle ne se propagent pas dans l'arborescence hiérarchique.
- AWS Control Tower ne modifie pas les paramètres de votre VPC pour les comptes nouveaux ou existants.

UO imbriquées et conformité

Depuis la console AWS Control Tower, vous pouvez consulter les unités d'organisation et les comptes non conformes sur la page Organisation, afin de comprendre la conformité à plus grande échelle.

Considérations relatives à la conformité des unités d'organisation et des comptes imbriqués

- La conformité d'une UO n'est pas déterminée en fonction de la conformité des UO qui lui sont imbriquées.
- L'état de conformité d'un contrôle est calculé pour toutes les unités d'organisation sur lesquelles le contrôle est activé, y compris les unités d'organisation imbriquées. Consultez l'état de conformité d'AWS Control Tower pour les unités d'organisation et les comptes.
- Une unité d'organisation est considérée comme non conforme uniquement si ses comptes ne le sont pas, quel que soit l'emplacement de l'unité d'organisation dans la hiérarchie des unités d'organisation.
- Si une UO imbriquée n'est pas conforme, son UO parent n'est pas automatiquement considérée comme non conforme.
- Sur la page de détail de l'unité d'organisation ou de détail du compte, vous pouvez consulter la liste des ressources non conformes qui peuvent être à l'origine du statut de non-conformité de vos unités d'organisation ou de vos comptes.

UO imbriquées et dérive

Dans certaines situations, la dérive peut empêcher l'enregistrement d'unités d'organisation imbriquées.

Attentes relatives à la dérive et aux unités d'organisation imbriquées

- Vous pouvez activer les contrôles sur les unités d'organisation dont les parents sont dérivés, mais pas directement sur les unités d'organisation dérivées.
- Vous êtes autorisé à activer les commandes de détection dans une unité d'organisation dérivée, à condition qu'il ne s'agisse pas d'une unité d'organisation dérivée de haut niveau.
- Les contrôles obligatoires sont activés uniquement sur les unités d'organisation de niveau supérieur. Les contrôles obligatoires sont ignorés lorsque vous enregistrez une unité d'organisation imbriquée.
- Un contrôle obligatoire protège les AWS Config ressources ; par conséquent, ce contrôle doit être dans un état non dérivé pour enregistrer des unités d'organisation imbriquées. En cas de dérive, AWS Control Tower bloque l'enregistrement des unités d'organisation imbriquées.
- Si l'unité d'organisation de niveau supérieur est en dérive, le contrôle qui protège les AWS Config ressources peut être en dérive. Dans ce cas, AWS Control Tower bloque toute action nécessitant la création ou la mise à jour de AWS Config ressources, y compris l'application de contrôles de détection.

UO et contrôles imbriqués

Lorsque vous activez un contrôle sur une unité d'organisation enregistrée, les contrôles préventifs et de détection ont des comportements différents. Pour les unités d'organisation imbriquées, les contrôles proactifs se comportent de la même manière que les contrôles de détection.

Contrôles préventifs

- Des contrôles préventifs sont appliqués aux unités d'organisation imbriquées.
- Des contrôles préventifs obligatoires sont appliqués à tous les comptes relevant de l'UO et de ses UO imbriquées.
- Les contrôles préventifs concernent tous les comptes et unités d'organisation imbriqués sous l'unité d'organisation cible, même si ces comptes et unités d'organisation ne sont pas enregistrés.

Detective et contrôles proactifs

- Les unités d'organisation imbriquées n'héritent pas automatiquement des contrôles de détection ou proactifs ; ceux-ci doivent être activés séparément.
- Les contrôles Detective et proactifs ne sont déployés que sur les comptes enregistrés dans les régions opérationnelles de votre zone d'atterrissage.

États de contrôle et héritage activés

Vous pouvez consulter les contrôles hérités pour chaque unité d'organisation sur la page de détails de l'unité d'organisation.

> **Tip**
>
> Vous pouvez utiliser l'héritage de contrôle pour vous aider à respecter le quota SCP d'une unité d'organisation. Par exemple, vous pouvez activer un contrôle au niveau de l'unité d'organisation supérieure d'une hiérarchie d'unités d'organisation, au lieu de l'activer directement pour une unité d'organisation imbriquée.

Statut hérité

- Le statut Hérité indique que le contrôle est activé uniquement par héritage et qu'il n'a pas été appliqué directement à l'unité d'organisation.
- Le statut Activé signifie que le contrôle est appliqué sur cette unité d'organisation, quel que soit son état sur les autres unités d'organisation.
- Le statut Failed signifie que le contrôle n'est pas appliqué sur cette unité d'organisation, quel que soit son état sur les autres unités d'organisation.

> **Note**
>
> Le statut Inherited indique que le contrôle a été appliqué à une UO située plus haut dans l'arborescence et qu'il est appliqué sur cette UO, mais il n'a pas été ajouté directement à cette UO.

Si votre zone d'atterrissage n'est pas la version actuelle

Chaque ligne du tableau des contrôles activés représente un contrôle activé sur une unité d'organisation individuelle.

Les unités d'organisation imbriquées et la racine

La racine n'est pas une unité d'organisation et elle ne peut pas être enregistrée ou réenregistrée. Vous ne pouvez pas non plus créer de comptes directement à la racine. La racine ne peut pas être non conforme ou présenter un état de cycle de vie, tel qu'elle est enregistrée ou en dérive.

Cependant, la racine est le conteneur de premier niveau pour tous les comptes et unités d'organisation. Dans le contexte des unités d'organisation imbriquées, il s'agit du nœud sous lequel toutes les autres unités d'organisation sont imbriquées.

Enregistrer une unité organisationnelle existante auprès d'AWS Control Tower

Un moyen efficace d'intégrer plusieurs AWS comptes existants dans AWS Control Tower consiste à étendre la gouvernance par AWS Control Tower à l'ensemble d'une unité organisationnelle (UO).

Pour activer la gouvernance d'AWS Control Tower sur une unité d'organisation existante créée avec ses comptes AWS Organizations, enregistrez l'unité d'organisation auprès de votre zone d'accueil AWS Control Tower. Vous pouvez enregistrer des unités d'organisation contenant jusqu'à 300 comptes. Si une unité d'organisation contient plus de 300 comptes, vous ne pouvez pas l'enregistrer dans AWS Control Tower.

Lorsque vous enregistrez une UO, les comptes de ses membres sont inscrits dans la zone de landing zone AWS Control Tower. Ils sont régis par les contrôles qui s'appliquent à leur unité d'organisation.

Note

Si vous ne possédez pas encore de zone d'atterrissage AWS Control Tower, commencez par configurer une zone d'atterrissage, soit dans une nouvelle organisation créée par AWS Control Tower, soit dans une AWS Organizations organisation existante. Pour plus de détails sur la configuration d'une zone d'atterrissage, consultezCommencer à utiliser AWS Control Tower.

Qu'arrive-t-il à mes comptes lorsque j'enregistre mon unité d'organisation ?

AWS Control Tower a besoin d'une autorisation pour établir un accès fiable entre vous AWS CloudFormation et en votre nom, afin de AWS CloudFormation pouvoir déployer automatiquement votre stack AWS Organizations sur les comptes de votre organisation.

- Le `AWSControlTowerExecution` rôle est ajouté à tous les comptes dont le statut est Non inscrit.
- Les contrôles obligatoires sont activés par défaut sur votre unité d'organisation et sur tous ses comptes lorsque vous enregistrez votre unité d'organisation.

Inscription partielle des comptes après l'enregistrement d'une UO

Il est possible d'enregistrer une unité d'organisation avec succès, mais certains comptes peuvent rester non inscrits. Si tel est le cas, ces comptes ne répondent pas à certaines des conditions requises pour l'inscription. Si l'inscription d'un compte dans le cadre du processus d'enregistrement de l'unité d'organisation échoue, le statut du compte sur la page des comptes indique que l'inscription a échoué. Vous pouvez également voir des informations de compte sur la page de votre UO, telles que 4 sur 5, dans le champ des comptes.

Par exemple, si vous voyez 4 sur 5, cela signifie que votre unité d'organisation possède 5 comptes au total, dont 4 se sont inscrits avec succès, mais qu'un compte n'a pas pu être inscrit pendant le processus d'enregistrement de l'unité d'organisation. Vous pouvez choisir Re-Register OU pour intégrer les comptes à l'inscription, une fois que vous vous êtes assuré qu'ils répondent aux conditions d'inscription.

Conditions requises pour l'enregistrement d'une UO par les utilisateurs IAM

Votre identité AWS Identity and Access Management (IAM) (utilisateur ou rôle) ou votre identité d'utilisateur IAM Identity Center doit être incluse dans le portefeuille Account Factory approprié lorsque vous effectuez l'opération Register OU, même si vous disposez déjà des `Admin` autorisations. Dans le cas contraire, la création des produits approvisionnés échouera lors de l'enregistrement. L'échec se produit car AWS Control Tower s'appuie sur les informations d'identification de l'utilisateur IAM ou sur l'identité de l'utilisateur IAM Identity Center lors de l'enregistrement d'une unité d'organisation.

Le portefeuille correspondant est celui créé par AWS Control Tower, appelé AWS Control Tower Account Factory Portfolio. Pour y accéder, sélectionnez Service Catalog > Account Factory > AWS Control Tower Account Factory Portfolio. Sélectionnez ensuite l'onglet Groupes, rôles et

utilisateurs pour afficher votre identité IAM ou IAM Identity Center. Pour plus d'informations sur la façon d'accorder l'accès, consultez la documentation de AWS Service Catalog.

Enregistrer une UO existante

Dans la console AWS Control Tower, sur la page Organisation, vous pouvez consulter l'ensemble des unités d'organisation et des comptes de votre organisation dans une hiérarchie, y compris les unités d'organisation enregistrées auprès d'AWS Control Tower et celles qui ne le sont pas.

En général, les UO non enregistrées ont été créées dans AWS Organizations, et elles ne sont régies par aucune autre zone d'atterrissage. Vous pouvez enregistrer des unités d'organisation existantes contenant jusqu'à 300 comptes. Si une unité d'organisation contient plus de 300 comptes, vous ne pouvez pas l'enregistrer dans AWS Control Tower.

Pour enregistrer une UO existante

1. Connectez-vous à la console AWS Control Tower à l'adresse https://console.aws.amazon.com/controltower.
2. Dans le menu de navigation du volet gauche, sélectionnez Organisation.
3. Sur la page Organisation, sélectionnez le bouton radio à côté de l'unité d'organisation que vous souhaitez enregistrer, puis sélectionnez Enregistrer l'unité organisationnelle dans le menu déroulant Actions en haut à droite, ou sélectionnez le nom de l'unité d'organisation afin de consulter la page de détails de l'unité organisationnelle correspondante.
4. Sur la page des détails de l'unité d'organisation, en haut à droite, vous pouvez sélectionner Enregistrer l'unité d'organisation dans le menu déroulant Actions.

Le processus d'enregistrement prend au moins 10 minutes pour étendre la gouvernance à l'unité d'organisation, et jusqu'à 2 minutes supplémentaires pour chaque compte supplémentaire.

Résultats de l'enregistrement d'une UO existante

Une fois que vous avez enregistré une unité d'organisation existante, le `AWSControlTowerExecution` rôle permet à AWS Control Tower d'étendre la gouvernance à ses comptes individuels. Des barrières de sécurité sont appliquées et les informations relatives aux activités du compte sont communiquées à vos comptes d'audit et de journalisation.

Parmi les autres résultats, mentionnons les suivants :

- `AWSControlTowerExecution` permet l'audit par le compte d'audit AWS Control Tower.

- `AWSControlTowerExecution`vous aide à configurer la journalisation de votre organisation, de sorte que tous les journaux de chaque compte soient envoyés au compte de journalisation.
- `AWSControlTowerExecution`garantit que les contrôles AWS Control Tower que vous avez sélectionnés s'appliquent automatiquement à chaque compte individuel de vos unités d'organisation, ainsi qu'à chaque nouveau compte que vous créez dans AWS Control Tower.

Pour une unité d'organisation enregistrée, vous pouvez fournir des rapports de conformité et de sécurité basés sur les fonctionnalités d'audit et de journalisation intégrées aux contrôles d'AWS Control Tower. Vos équipes de sécurité et de conformité peuvent vérifier que toutes les exigences sont satisfaites et qu'aucune dérive organisationnelle ne s'est produite. Pour plus d'informations sur la dérive, consultezDétectez et corrigez les dérives dans AWS Control Tower.

> **Note**
>
> Une situation inhabituelle peut se produire lorsqu'AWS Control Tower affiche les unités d'organisation et leurs comptes. Si vous avez créé un compte dans une unité organisationnelle enregistrée, puis que vous déplacez ce compte inscrit dans une autre unité d'organisation non enregistrée, en particulier si vous avez l'habitude de AWS Organizations déplacer le compte, vous pouvez voir le résultat « 1 sur 0 » comptes sur la page de détails de votre unité d'organisation. En outre, vous avez peut-être créé un autre compte non inscrit dans cette unité d'organisation non enregistrée. S'il existe un compte non enregistré, la console peut indiquer « 1 sur 1 » pour l'unité d'organisation. Il semblerait que le compte unique (nouvellement créé) soit inscrit, mais en réalité ce n'est pas le cas. Vous devez enregistrer le nouveau compte.

Création d'une nouvelle UO

Pour créer une nouvelle unité d'organisation dans AWS Control Tower

1. Accédez à la page Organisation.
2. Sélectionnez Créer une unité organisationnelle dans le menu déroulant Créer des ressources en haut à droite.
3. Spécifiez un nom dans le champ Nom de l'unité d'organisation.

4. Dans la liste déroulante des unités d'organisation parentes, vous pouvez voir la hiérarchie des unités d'organisation enregistrées. Sélectionnez une unité d'organisation parent pour la nouvelle unité d'organisation que vous créez.
5. Choisissez Ajouter.

> **Tip**
>
> Pour ajouter une UO imbriquée en moins d'étapes, sélectionnez le nom de l'UO parent indiqué dans le tableau de la page Organisation, consultez la page UO de cette UO parent, puis choisissez Ajouter une UO dans le menu déroulant Actions en haut à droite. La nouvelle UO est automatiquement créée sous la forme d'une UO imbriquée sous l'UO que vous avez sélectionnée.

> **Note**
>
> Si votre zone de landing zone n'est pas à jour, vous verrez une liste plate au lieu d'une hiérarchie dans le menu déroulant. Même si votre zone d'atterrissage inclut des unités d'organisation imbriquées, vous ne verrez pas les unités d'organisation de niveau 5 dans la liste déroulante, car vous ne pouvez pas créer de nouvelle unité d'organisation sous une unité d'organisation de niveau 5. Pour plus d'informations sur les unités d'organisation imbriquées dans AWS Control Tower, consultezUO imbriquées dans AWS Control Tower.

Causes courantes d'échec lors de l'enregistrement ou du réenregistrement

Si l'enregistrement (ou le réenregistrement) d'une UO ou de l'un de ses comptes membres échoue, vous pouvez télécharger un fichier contenant un rapport détaillé indiquant les prévérifications qui n'ont pas été validées. Vous pouvez terminer le téléchargement en cliquant sur le bouton Télécharger, qui apparaît en haut à droite de la zone d'enregistrement.

Cette section répertorie les types d'erreurs que vous pouvez recevoir en cas d'échec des vérifications préalables et indique comment les corriger.

En général, lorsque vous enregistrez ou réenregistrez une unité d'organisation, tous les comptes de cette unité d'organisation sont inscrits dans AWS Control Tower. Cependant, il est possible que l'inscription de certains comptes échoue, même si l'unité d'organisation dans son ensemble est

correctement enregistrée. Dans ces cas, vous devez résoudre l'échec de la vérification préalable lié au compte, puis essayer de réinscrire ce compte ou cette unité d'organisation.

Erreur de zone d'atterrissage

- La zone d'atterrissage n'est pas prête

  Réinitialisez votre zone d'atterrissage actuelle ou mettez-la à jour avec la dernière version.

Erreurs de l'UO

- Dépasse le nombre maximum de SCP

  Vous avez peut-être dépassé la limite des politiques de contrôle des services (SCP) par unité d'organisation, ou vous avez peut-être atteint un autre quota. Une limite de 5 SCP par unité d'organisation s'applique à toutes les unités d'organisation de votre zone d'atterrissage AWS Control Tower. Si vous avez plus de SCP que le quota ne le permet, vous devez supprimer ou combiner les SCP.
- SCP en conflit

  Les SCP existants peuvent être appliqués à l'unité d'organisation ou au compte, ce qui empêche AWS Control Tower d'enregistrer le compte. Vérifiez que les SCP appliqués ne contiennent aucune politique susceptible d'empêcher AWS Control Tower de fonctionner. Assurez-vous de vérifier les SCP hérités des unités d'organisation situées plus haut dans la hiérarchie.
- Dépasse le quota défini pour les piles

  Le quota du stack set a peut-être été dépassé. Si vous avez plus d'instances que le quota ne le permet, vous devez supprimer certaines instances de pile. Pour plus d'informations, consultez la section sur AWS CloudFormation les quotas dans le guide de AWS CloudFormation l'utilisateur.
- Dépasse la limite du compte

  AWS Control Tower limite chaque UO à 300 comptes lors de l'enregistrement.

Erreurs liées au compte

- Contrôles préalables empêchés sur les comptes

Un SCP existant sur l'UO empêche AWS Control Tower d'effectuer des vérifications préalables sur les comptes des membres de l'UO. Pour résoudre cet échec de pré-vérification, mettez à jour ou supprimez le SCP de l'unité d'organisation.

- Erreur d'adresse e-mail

  L'adresse e-mail que vous avez spécifiée pour le compte n'est pas conforme aux normes de dénomination. Voici l'expression régulière (regex) qui indique quels caractères sont autorisés : `[A-Z0-9a-z._%+-]+@[A-Za-z0-9.-]+[.]+[A-Za-z]+`

- Enregistreur de configuration ou canal de diffusion activé

  Le compte peut disposer d'un enregistreur AWS Config de configuration ou d'un canal de diffusion existant. Vous devez les supprimer ou les modifier AWS CLI dans toutes les AWS régions où le compte de gestion AWS Control Tower a régi les ressources, avant de pouvoir créer un compte.

- STS désactivé

  AWS Security Token Service (AWS STS) peut être désactivé dans le compte. AWS Les points de terminaison STS doivent être activés dans les comptes de toutes les régions prises en charge par AWS Control Tower.

- Conflit avec le centre d'identité IAM

  La région d'origine d'AWS Control Tower n'est pas la même que la région AWS IAM Identity Center (IAM Identity Center). Si le centre d'identité IAM est déjà configuré, la région d'origine d'AWS Control Tower doit être identique à la région du centre d'identité IAM.

- Sujet SNS contradictoire

  Le compte possède un nom de rubrique Amazon Simple Notification Service (Amazon SNS) que AWS Control Tower doit utiliser. AWS Control Tower crée des ressources (telles que des rubriques SNS) portant des noms spécifiques. Si ces noms sont déjà utilisés, la configuration d'AWS Control Tower échoue. Cette situation peut se produire si vous réutilisez un compte précédemment inscrit dans AWS Control Tower.

- Compte suspendu détecté

  Ce compte a été suspendu. Il ne peut pas être inscrit dans AWS Control Tower. Supprimez le compte de cette unité d'organisation et réessayez.

- L'utilisateur IAM ne figure pas dans le portefeuille

Ajoutez l'utilisateur AWS Identity and Access Management (IAM) au portefeuille Service Catalog avant d'enregistrer votre unité d'organisation. Cette erreur concerne uniquement le compte de gestion.

- Le compte ne répond pas aux prérequis

  Le compte ne répond pas aux conditions requises pour l'inscription au compte. Par exemple, il se peut que le compte ne comporte pas les rôles et les autorisations nécessaires pour l'inscrire dans AWS Control Tower. Les instructions pour ajouter un rôle sont disponibles dansAjoutez manuellement le rôle IAM requis à un rôle existant Compte AWS et inscrivez-le.

Pour rappel, elle AWS CloudTrail est automatiquement activée sur tous vos AWS comptes lorsque vous les inscrivez dans AWS Control Tower. Si cette option CloudTrail est activée sur un compte avant l'inscription, vous risquez de subir une double facturation, sauf si vous la désactivez CloudTrail avant de commencer le processus d'inscription.

Mettre à jour les organisations

Le moyen le plus rapide de mettre à jour une unité organisationnelle (UO) ou de mettre à jour plusieurs comptes au sein d'une UO est de réenregistrer l'UO.

Quand mettre à jour les unités d'organisation et les comptes AWS Control Tower

Lorsque vous effectuez une mise à jour de la zone d'atterrissage, vous devez mettre à jour vos comptes inscrits afin d'appliquer de nouveaux contrôles à ces comptes.

- Vous pouvez mettre à jour tous les comptes d'une unité d'organisation à l'aide de l'option Réenregistrement.
- Si vous avez plusieurs unités d'organisation enregistrées dans votre zone de landing, réenregistrez toutes vos unités d'organisation pour mettre à jour tous vos comptes.
- Pour mettre à jour un seul compte, vous pouvez effectuer la mise à jour depuis la console AWS Control Tower ou sélectionner l'option Mettre à jour le produit provisionné dans AWS Service Catalog. veuillez consulter Mettre à jour le compte dans la console.

Mettre à jour plusieurs comptes dans la même unité d'organisation

Pour mettre à jour plusieurs comptes dans une unité d'organisation, en une seule action

1. Connectez-vous à la console AWS Control Tower à l'adresse https://console.aws.amazon.com/controltower.
2. Dans le menu de navigation du volet gauche, sélectionnez Organisation.
3. Sur la page Organisation, choisissez n'importe quelle unité d'organisation pour afficher la page de détails de l'unité d'organisation.
4. Sous Actions dans le coin supérieur droit, sélectionnez Ré-enregistrer l'OU.

Répétez ces étapes pour chaque unité d'organisation de votre organisation AWS Control Tower, si vous devez mettre à jour tous vos comptes et unités d'organisation.

Vous pouvez également sélectionner n'importe quel compte dont l'état de mise à jour est disponible, puis choisir Mettre à jour le compte pour autant de comptes que nécessaire.

Que se passe-t-il lors du réenregistrement

Lorsque vous réenregistrez une UO :

- Le champ État indique si le compte est actuellement inscrit auprès d'AWS Control Tower (inscrit), s'il n'a jamais été inscrit (Non inscrit) ou si l'inscription a échoué précédemment (échec de l'inscription).
- Lorsque vous réenregistrez l'unité d'organisation, le `AWSControlTowerExecution` rôle est ajouté à tous les comptes ayant le statut Non inscrit ou Échec de l'inscription.
- AWS Control Tower crée un identifiant d'authentification unique (IAM Identity Center) pour les nouveaux comptes inscrits.
- Les comptes inscrits sont réinscrits dans AWS Control Tower.
- La dérive des contrôles préventifs appliqués à l'UO est corrigée, car les SCP retrouvent leurs définitions par défaut.
- Tous les comptes sont mis à jour pour refléter les derniers changements de zone d'atterrissage.

Pour de plus amples informations, veuillez consulter Inscrire un existant Compte AWS.

> **Tip**
>
> Lorsque vous réenregistrez une unité d'organisation, ou lorsque vous mettez à jour la version de votre zone d'atterrissage et que vous mettez à jour plusieurs comptes membres, vous pouvez voir un message d'échec mentionnant le StackSet-AWSControlTowerExecutionRole. Cela peut échouer StackSet dans le compte de gestion car le rôle AWSControlTowerExecutionIAM existe déjà dans tous les comptes de membres inscrits. Ce message d'erreur est un comportement attendu, et il peut être ignoré.

Mettre à jour un seul compte

Vous pouvez mettre à jour des comptes AWS Control Tower individuels dans la console AWS Control Tower ou dans la console Service Catalog.

Pour mettre à jour un seul compte dans la console AWS Control Tower, consultezMettre à jour le compte dans la console.

Pour mettre à jour un seul compte dans AWS Service Catalog

1. Accédez à AWS Service Catalog.
2. Dans le menu de navigation du volet gauche, choisissez Provisioned products.
3. Sur la page Produits approvisionnés, sélectionnez le bouton radio à côté du produit approvisionné que vous souhaitez mettre à jour.
4. Dans le coin supérieur droit, choisissez le menu déroulant Actions pour mettre à jour.

Pour en savoir plus sur la mise à jour dans AWS Service Catalog, consultez Mettre à jour le produit approvisionné la section « Mise à jour des produits » dans le Guide de l'administrateur du Service Catalog.

Services intégrés

AWS Control Tower est un service qui s'appuie sur d'autres AWS services pour vous aider à configurer un environnement bien conçu. Ce chapitre fournit un bref aperçu de ces services, y compris des informations de configuration concernant les services sous-jacents et leur fonctionnement dans AWS Control Tower.

Pour plus d'informations sur la façon de mesurer un environnement bien architecturé, découvrez l'outil Well-Architected AWS . Consultez également le Guide de l'environnement cloud de gestion et de gouvernance.

Rubriques

- Déployez des environnements avec AWS CloudFormation
- Surveillez les événements avec CloudTrail
- Surveillez les ressources et les services avec CloudWatch
- Gérez les configurations des ressources avec AWS Config
- Gérer les autorisations pour les entités avec IAM
- AWS Key Management Service
- Exécutez des fonctions de calcul sans serveur avec Lambda
- Gérez les comptes via AWS Organizations
- Stockez des objets avec Amazon S3
- Surveillez votre environnement avec Security Hub
- Provisionner des comptes via AWS Service Catalog
- Suivez les alertes via Amazon Simple Notification Service
- Créez des applications distribuées avec AWS Step Functions

Déployez des environnements avec AWS CloudFormation

AWS CloudFormation vous permet de créer et de provisionner des déploiements AWS d'infrastructure de manière prévisible et répétée. Il vous aide à tirer parti AWS des produits pour créer des applications hautement fiables, hautement évolutives et rentables dans le cloud sans vous soucier de la création et de la configuration de l' AWS infrastructure sous-jacente. AWS CloudFormation vous permet d'utiliser un fichier modèle pour créer et supprimer un ensemble de

ressources en une seule unité (une pile). Pour plus d'informations, consultez le AWS CloudFormation guide de l'utilisateur.

AWS Control Tower utilise des AWS CloudFormation stacksets pour appliquer des contrôles aux comptes. Pour plus d'informations sur la manière dont AWS CloudFormation AWS Control Tower fonctionne ensemble, consultez Création de AWS Control Tower ressources avec AWS CloudFormation.

Surveillez les événements avec CloudTrail

AWS Control Tower se configure AWS CloudTrail pour permettre une journalisation et un audit centralisés. Le compte de gestion peut ainsi consulter les actions administratives et les événements du cycle de vie des comptes membres. CloudTrail

CloudTrail vous aide à surveiller votre AWS environnement dans le cloud en conservant un historique des appels d' AWS API pour vos comptes. Par exemple, vous pouvez identifier les utilisateurs et les comptes qui ont appelé les AWS API pour les services compatibles CloudTrail, l'adresse IP source à partir de laquelle les appels ont été effectués et l'heure à laquelle les appels ont eu lieu. Vous pouvez CloudTrail intégrer des applications à l'aide de l'API, automatiser la création de traces pour votre organisation, vérifier l'état de vos pistes et contrôler la manière dont les administrateurs activent et désactivent la CloudTrail connexion. Pour plus d'informations, consultez le AWS CloudTrail guide de l'utilisateur.

Surveillez les ressources et les services avec CloudWatch

Amazon CloudWatch fournit une solution de surveillance fiable, évolutive et flexible que vous pouvez commencer à utiliser en quelques minutes. Vous n'avez plus besoin de régler, gérer et redimensionner vos propres systèmes et infrastructures de surveillance. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

Pour plus d'informations sur la façon dont Amazon CloudWatch travaille avec AWS Control Tower, consultez Monitoring.

Gérez les configurations des ressources avec AWS Config

AWS Config fournit une vue détaillée des ressources associées à votre AWS compte, notamment de leur configuration, de leur relation entre elles et de l'évolution des configurations et de leurs relations au fil du temps. Pour de plus amples informations, consultez le Guide du développeur AWS Config.

AWS Config les ressources mises en service par AWS Control Tower sont automatiquement `aws-control-tower` étiquetées avec une valeur de`managed-by-control-tower`.

Pour plus d'informations sur la façon dont AWS Config les ressources sont surveillées et enregistrées dans AWS Control Tower, ainsi que sur la façon dont elles sont facturées, consultezSurveillez l'évolution des ressources avec AWS Config.

AWS Control Tower utilise AWS Config Rules pour implémenter des contrôles de détection. Pour plus d'informations, consultez À propos des contrôles dans AWS Control Tower.

Gérer les autorisations pour les entités avec IAM

AWS Identity and Access Management (IAM) est un AWS service permettant de contrôler l'accès à d'autres AWS services. Avec IAM, vous pouvez gérer de manière centralisée les utilisateurs, les informations d'identification de sécurité, telles que les clés d'accès et les autorisations, qui désignent les AWS ressources auxquelles vos utilisateurs et applications ont accès.

Lorsque vous configurez votre zone de landing zone, un certain nombre de groupes peuvent être créés AWS IAM Identity Center automatiquement, si vous sélectionnez IAM comme fournisseur d'identité. Ces groupes disposent d'ensembles d'autorisations qui sont des politiques d'autorisation prédéfinies par IAM. Vos utilisateurs finaux peuvent également utiliser IAM pour définir l'étendue des autorisations accordées aux utilisateurs IAM et aux autres entités au sein des comptes membres.

AWS Identity and Access Management (IAM) simplifie la façon dont vous gérez l'accès aux AWS comptes et aux applications professionnelles. Vous pouvez contrôler l'accès à l'IAM Identity Center et les autorisations des utilisateurs sur tous vos AWS comptes dans AWS Control Tower.

Pour plus d'informations, consultez le AWS IAM Identity Center guide de l'utilisateur.

Si vous êtes basé dans un pays Région AWS qui ne prend pas en charge l'IAM, vous pouvez faire appel à un autre fournisseur d'identité, pour configurer et gérer manuellement vos propres utilisateurs et groupes.

AWS Key Management Service

AWS Key Management Service (AWS KMS) vous permet de créer et de contrôler des clés qui protègent vos données. AWS Control Tower vous permet éventuellement de chiffrer vos données à l'aide de clés de AWS KMS chiffrement. Pour plus d'informations à ce sujet AWS KMS, consultez le guide du développeur AWS KMS.

Pour plus d'informations sur la configuration des AWS KMS clés avec AWS Control Tower, consultez la section Configuration facultative AWS KMS des clés.

Exécutez des fonctions de calcul sans serveur avec Lambda

Avec AWS Lambda, vous pouvez exécuter du code sans provisionner ni gérer de serveurs. Vous pouvez exécuter du code pour de nombreux types d'applications ou de services principaux, sans nécessiter de frais d'administration supplémentaires. Lorsque vous téléchargez votre code, Lambda peut exécuter et dimensionner le code avec une haute disponibilité. Vous pouvez configurer votre code pour qu'il se déclenche automatiquement à partir d'autres AWS services, ou vous pouvez l'appeler directement depuis n'importe quelle application Web ou mobile.

Par exemple, certains rôles dans le compte d'audit AWS Control Tower peuvent être assumés par programmation, afin que vous puissiez consulter d'autres comptes à l'aide de Lambda. Vous pouvez également utiliser les événements du cycle de vie d'AWS Control Tower pour déclencher des fonctions Lambda.

Gérez les comptes via AWS Organizations

AWS Organizations est un service de gestion de comptes qui vous permet de consolider plusieurs AWS comptes au sein d'une organisation que vous créez et gérez de manière centralisée. Avec Organizations, vous pouvez créer des comptes membres et inviter des comptes existants à rejoindre votre organisation. Vous pouvez organiser ces comptes en groupes et joindre des contrôles basés sur des stratégies. Pour plus d'informations, consultez le AWS Organizations guide de l'utilisateur.

Dans AWS Control Tower, Organizations permet de gérer de manière centralisée la facturation, de contrôler l'accès, la conformité et la sécurité, et de partager les ressources entre vos AWS comptes membres. Les comptes sont répartis en groupes logiques, nommés unités d'organisation (UO). Pour plus d'informations sur les Organizations, consultez le Guide de AWS Organizations l'utilisateur.

AWS Control Tower utilise les unités d'organisation suivantes :

- Root : conteneur parent pour tous les comptes et toutes les autres unités d'organisation de votre zone de landing zone.
- Sécurité — Cette unité d'organisation contient le compte d'archivage du journal, le compte d'audit et les ressources qu'ils possèdent.
- Sandbox — Cette unité d'organisation est créée lorsque vous configurez votre zone de landing zone. Elle et les autres UO pour enfants de votre zone de landing zone contiennent vos comptes

de membre. Il s'agit des comptes auxquels vos utilisateurs finaux accèdent pour travailler sur les AWS ressources.

> **Note**
>
> Vous pouvez ajouter des unités d'organisation supplémentaires dans votre zone de landing via la console AWS Control Tower sur la page Organizational units.

Considérations

Des contrôles peuvent être appliqués aux unités d'organisation créées par le biais d'AWS Control Tower. Les unités d'organisation créées en dehors d'AWS Control Tower ne le peuvent pas, par défaut. Vous pouvez toutefois enregistrer de telles unités d'organisation. Une fois que vous avez enregistré une unité d'organisation, vous pouvez appliquer des contrôles à celle-ci et à ses comptes. Pour plus d'informations sur l'enregistrement d'une UO, consultez Enregistrer une unité organisationnelle existante auprès d'AWS Control Tower.

Stockez des objets avec Amazon S3

Amazon Simple Storage Service (Amazon S3) est une solution de stockage sur Internet. Vous pouvez utiliser Amazon S3 pour stocker et récupérer n'importe quelle quantité de données, n'importe quand et depuis n'importe quel emplacement sur le Web. Toutes ces tâches peuvent être réalisées à partir de l'interface Web simple et intuitive de AWS Management Console. Pour plus d'informations, consultez le guide de l'utilisateur d'Amazon Simple Storage Service.

Lorsque vous configurez votre zone de destination, un compartiment Amazon S3 est créé dans votre compte d'archive de journaux pour contenir tous les journaux de tous les comptes de votre zone de destination.

Surveillez votre environnement avec Security Hub

AWS Control Tower est intégré à AWS Security Hub au moyen de la norme Security Hub appelée Service-Managed Standard : AWS Control Tower. Pour plus d'informations, consultez la norme Security Hub.

Provisionner des comptes via AWS Service Catalog

AWS Service Catalog permet aux administrateurs informatiques de créer, de gérer et de distribuer des portefeuilles de produits approuvés aux utilisateurs finaux, qui ont ensuite accès aux produits dont ils ont besoin sur un portail personnalisé. Les produits typiques incluent les serveurs, les bases de données, les sites Web ou les applications déployés à l'aide de AWS ressources.

Vous pouvez contrôler les utilisateurs qui ont accès à des produits spécifiques, ce qui vous permet de faire respecter les normes commerciales de l'organisation, de gérer le cycle de vie des produits et d'aider les utilisateurs à trouver et à lancer des produits en toute confiance. Pour plus d'informations, consultez le Guide de l'administrateur du Service Catalog.

Dans AWS Control Tower, vos administrateurs cloud centraux et vos utilisateurs finaux peuvent créer des comptes personnalisés dans votre zone de landing zone à l'aide de AWS Service Catalog produits appelés « plans personnalisés ». Pour plus d'informations, reportez-vous à l'étape 2. Créez le AWS Service Catalog produit.

AWS Control Tower peut également utiliser les API Service Catalog pour automatiser davantage le provisionnement et la mise à jour des comptes. Pour plus de détails, consultez le guide du AWS Service Catalog développeur.

Transition vers le type de produit AWS Service Catalog externe

AWS Service Catalog a modifié le support pour les produits Open Source Terraform et a approvisionné les produits vers un nouveau type de produit, appelé External. Pour en savoir plus sur cette transition, consultez la section Mise à jour des produits Open Source Terraform existants et des produits provisionnés vers le type de produit externe dans le guide de l'AWS Service Catalog administrateur.

Cette modification affecte les comptes existants que vous avez créés ou inscrits dans le cadre de la personnalisation en usine des comptes AWS Control Tower. Pour transférer ces comptes vers le type de produit externe, vous devez apporter des modifications à la fois dans AWS Control Tower AWS Service Catalog et dans AWS Control Tower.

Pour passer au type de produit externe

1. Mettez à niveau votre moteur de référence Terraform existant AWS Service Catalog pour inclure la prise en charge des types de produits externes et open source Terraform. Pour obtenir des instructions sur la mise à jour de votre moteur de référence Terraform, consultez le AWS Service Catalog GitHub référentiel.

2. Dans AWS Service Catalog, dupliquez tous les produits Open Source Terraform existants (plans), les doublons utilisant le nouveau type de produit externe. Ne mettez pas fin aux plans Open Source Terraform existants.
3. Dans AWS Control Tower, mettez à jour chaque compte à l'aide d'un plan Open Source Terraform afin d'utiliser le nouveau plan externe.

   a. Pour mettre à jour un plan, vous devez d'abord supprimer complètement le plan Open Source Terraform. Pour plus de détails, consultez Supprimer un plan d'un compte.

   b. Ajoutez le nouveau plan externe au même compte. Pour plus de détails, consultez l'article Ajouter un plan à un compte AWS Control Tower.
4. Une fois que tous les comptes utilisant les plans Open Source de Terraform ont été mis à jour vers les plans externes, retournez AWS Service Catalog et résiliez tous les produits qui utilisent Terraform Open Source comme type de produit.
5. À l'avenir, tous les comptes créés ou inscrits à l'aide de la personnalisation des comptes AWS Control Tower en usine devront faire référence à des plans utilisant le type de produit AWS CloudFormationou le type de produit externe.

   Pour les plans créés à l'aide du type de produit externe, AWS Control Tower prend uniquement en charge les personnalisations de compte qui utilisent des modèles Terraform et le moteur de référence Terraform. Pour en savoir plus, consultez la section Configurer pour la personnalisation.

> **Note**
>
> AWS Control Tower ne prend pas en charge Terraform Open Source en tant que type de produit lors de la création de nouveaux comptes. Pour en savoir plus sur ces modifications, consultez la section Mise à jour des produits Open Source Terraform existants et des produits provisionnés vers le type de produit externe dans le guide de l'AWS Service Catalog administrateur. AWS Service Catalog aidera les clients tout au long de cette transition de type de produit, selon les besoins. Contactez le représentant de votre compte pour demander de l'aide.

Suivez les alertes via Amazon Simple Notification Service

Amazon Simple Notification Service (Amazon SNS) est un service Web qui permet aux applications, aux utilisateurs finaux et aux appareils d'envoyer et de recevoir des notifications instantanément depuis le cloud. Pour plus d'informations, consultez le Guide du développeur Amazon Simple Notification Service.

AWS Control Tower utilise Amazon SNS pour envoyer des alertes programmatiques aux adresses e-mail de votre compte de gestion et de votre compte d'audit. Ces alertes vous aident à prévenir la dérive dans votre zone d'atterrissage. Pour plus d'informations, consultez Détectez et corrigez les dérives dans AWS Control Tower.

Nous utilisons également Amazon Simple Notification Service pour envoyer des notifications de conformité depuis AWS Config.

> **Tip**
>
> L'un des meilleurs moyens de recevoir les notifications de conformité du contrôle AWS Control (sur votre compte d'audit) est de vous abonner à`AggregateConfigurationNotifications`. Il s'agit d'un service qui vous aide à contrôler la conformité. Il vous fournit des données réelles sur AWS Config les règles qui ne sont pas conformes. AWS Config gère automatiquement la liste des comptes de votre unité d'organisation.
>
> Vous devez vous abonner manuellement, par e-mail ou par tout autre type d'abonnement autorisé par le réseau social. Le relevé `arn:aws:sns:`*`homeregion`*`:`*`account`*`:aws-controltower-AggregateSecurityNotifications` mène à votre compte d'audit.

Créez des applications distribuées avec AWS Step Functions

AWS Step Functions permet de coordonner facilement les composants des applications distribuées sous la forme d'une série d'étapes dans un flux de travail visuel. Vous pouvez rapidement créer et exécuter des machines d'état pour effectuer les étapes de votre application de façon fiable et scalable. Pour plus d'informations, consultez le Guide du développeur AWS Step Functions.

Gestion des identités et des accès dans AWS Control Tower

Pour effectuer n'importe quelle opération dans votre zone de landing zone, telle que la mise en service de comptes dans Account Factory ou la création de nouvelles unités organisationnelles (UO) dans la console AWS Control Tower, vous devez soit AWS Identity and Access Management (IAM) soit vous AWS IAM Identity Center demander de vous authentifier en tant qu'utilisateur approuvé. AWS Par exemple, si vous utilisez la console AWS Control Tower, vous authentifiez votre identité en fournissant vos AWS informations d'identification, telles que fournies par votre administrateur.

Une fois que vous avez authentifié votre identité, IAM contrôle votre accès AWS à un ensemble défini d'autorisations sur un ensemble spécifique d'opérations et de ressources. Si vous êtes administrateur de compte, vous pouvez utiliser IAM pour contrôler l'accès des autres utilisateurs IAM aux ressources associées à votre compte.

Rubriques

Authentification

Vous avez accès à AWS l'un des types d'identités suivants :

- AWS utilisateur root du compte : lorsque vous créez un AWS compte pour la première fois, vous devez disposer d'une identité qui donne un accès complet à tous les AWS services et ressources du compte. Cette identité est appelée utilisateur root du AWS compte. Vous avez accès à cette identité lorsque vous vous connectez avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes, y compris pour les tâches administratives. Adhérez plutôt à la meilleure pratique qui consiste à utiliser l'utilisateur root uniquement pour créer votre premier utilisateur IAM Identity Center (recommandé) ou utilisateur IAM (ce n'est pas une bonne pratique dans la plupart des cas d'utilisation). Ensuite, mettez en sécurité les informations d'identification de l'utilisateur

racine et utilisez-les uniquement pour effectuer certaines tâches de gestion des comptes et des services. Pour plus d'informations, consultez Quand se connecter en tant qu'utilisateur root.

- Utilisateur IAM : un utilisateur IAM est une identité au sein de votre AWS compte dotée d'autorisations spécifiques et personnalisées. Vous pouvez utiliser les informations d'identification de l'utilisateur IAM pour vous connecter à des AWS pages Web sécurisées telles que la console de AWS gestion, les forums de AWS discussion ou le centre de AWS support. AWS les meilleures pratiques recommandent de créer un utilisateur IAM Identity Center au lieu d'un utilisateur IAM, car le risque de sécurité augmente lorsque vous créez un utilisateur IAM doté d'informations d'identification à long terme.

  Si vous devez créer un utilisateur IAM dans un certain but, outre les informations d'identification, vous pouvez générer des clés d'accès pour chaque utilisateur IAM. Vous pouvez utiliser ces touches lorsque vous appelez AWS des services par programmation, soit par le biais de l'un des nombreux SDK, soit à l'aide de l'interface de ligne de AWS commande (CLI). Les outils SDK et CLI utilisent les clés d'accès pour signer de façon cryptographique votre demande. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même la demande. AWS Control Tower prend en charge Signature Version 4, un protocole permettant d'authentifier les demandes d'API entrantes. Pour plus d'informations sur l'authentification des demandes, voir Processus de signature de la version 4 de Signature dans la référence AWS générale.
- Rôle IAM : un rôle IAM est une identité IAM que vous pouvez créer dans votre compte et qui dispose d'autorisations spécifiques. Un rôle IAM est similaire à un utilisateur IAM en ce sens qu'il s'agit d'une AWS identité et qu'il possède des politiques d'autorisation qui déterminent ce que l'identité peut et ne peut pas faire. AWS En revanche, au lieu d'être associé de manière unique à une personne, un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. En outre, un rôle ne dispose pas d'informations d'identification standard à long terme comme un mot de passe ou des clés d'accès associées. Au lieu de cela, lorsque vous adoptez un rôle, il vous fournit des informations d'identification de sécurité temporaires pour votre session de rôle. Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :
  - Accès utilisateur fédéré : au lieu de créer un utilisateur IAM, vous pouvez utiliser des identités existantes provenant du AWS Directory Service répertoire des utilisateurs de votre entreprise ou d'un fournisseur d'identité Web. Ils sont appelés utilisateurs fédérés. AWS attribue un rôle à un utilisateur fédéré lorsque l'accès est demandé par le biais d'un fournisseur d'identité. Pour plus d'informations sur les utilisateurs fédérés, consultez Utilisateurs fédérés et rôles dans le Guide de l'utilisateur IAM.
  - AWS accès au service — Un rôle de service est un rôle IAM qu'un service suppose d'effectuer des actions sur votre compte en votre nom. Lorsque vous configurez certains environnements

de AWS service, vous devez définir le rôle que le service doit assumer. Ce rôle de service doit inclure toutes les autorisations requises pour que le service puisse accéder aux AWS ressources dont il a besoin. Les rôles de service varient d'un service à un service, mais nombre d'entre eux vous permettent de choisir vos autorisations, tant que vous respectez les exigences documentées pour le service en question. Les rôles de service fournissent un accès uniquement au sein de votre compte et ne peuvent pas être utilisés pour accorder l'accès à des services dans d'autres comptes. Vous pouvez créer, modifier et supprimer un rôle de service depuis IAM. Par exemple, vous pouvez créer un rôle qui autorise Amazon Redshift à accéder à un compartiment Amazon S3 en votre nom, puis à charger les données de ce compartiment dans un cluster Amazon Redshift. Pour plus d'informations, consultez la section Création d'un rôle pour déléguer des autorisations à un AWS service dans le guide de l'utilisateur IAM.

  - Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance Amazon EC2 et qui envoient des requêtes CLI AWS ou API. AWS Cela est préférable au stockage des clés d'accès dans l'instance Amazon EC2. Pour attribuer un AWS rôle à une instance Amazon EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance Amazon EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

- L'authentification des utilisateurs d'IAM Identity Center sur le portail utilisateur d'IAM Identity Center est contrôlée par le répertoire que vous avez connecté à IAM Identity Center. Toutefois, l'autorisation AWS des comptes accessibles aux utilisateurs finaux depuis le portail utilisateur est déterminée par deux facteurs :
  - Qui a obtenu l'accès à ces AWS comptes dans la console AWS IAM Identity Center. Pour plus d'informations, consultez la section Accès par authentification unique dans le guide de l'AWS IAM Identity Center utilisateur.
  - Quel niveau d'autorisations a été accordé aux utilisateurs finaux dans la console AWS IAM Identity Center pour leur permettre l'accès approprié à ces AWS comptes. Pour plus d'informations, consultez la section Ensembles d'autorisations dans le guide de AWS IAM Identity Center l'utilisateur.

Contrôle d'accès

Pour créer, mettre à jour, supprimer ou répertorier des ressources AWS Control Tower, ou d'autres AWS ressources dans votre zone de landing zone, vous devez disposer d'autorisations pour effectuer l'opération et d'autorisations pour accéder aux ressources correspondantes. En outre, pour effectuer l'opération par programmation, vous avez besoin de clés d'accès rapide valides.

Les sections suivantes décrivent comment gérer les autorisations pour AWS Control Tower :

Rubriques

- Présentation de la gestion des autorisations d'accès à vos ressources AWS Control Tower
- Utilisation de politiques basées sur l'identité (politiques IAM) pour AWS Control Tower

Travailler avec AWS IAM Identity Center et AWS Control Tower

Dans AWS Control Tower, l'IAM Identity Center permet aux administrateurs cloud centraux et aux utilisateurs finaux de gérer l'accès à plusieurs AWS comptes et applications professionnelles. Par défaut, AWS Control Tower utilise ce service pour configurer et gérer l'accès aux comptes créés via Account Factory, sauf si vous avez sélectionné l'option permettant de gérer vous-même votre identité et votre contrôle d'accès.

Pour plus d'informations sur la sélection d'un fournisseur d'identité, consultezConseils relatifs à l'IAM Identity Center.

Pour un bref didacticiel expliquant comment configurer les utilisateurs et les autorisations de votre IAM Identity Center dans AWS Control Tower, vous pouvez visionner cette vidéo (6:23). Pour un visionnage de meilleure qualité, sélectionnez l'icône dans le coin inférieur droit de la vidéo pour l'afficher en plein écran. Le sous-titrage est disponible.

Présentation vidéo de la configuration du centre d'identité AWS IAM dans AWS Control Tower.

À propos de la configuration d'AWS Control Tower avec IAM Identity Center

Lors de la configuration initiale d'AWS Control Tower, seuls l'utilisateur root et les utilisateurs IAM disposant des autorisations appropriées peuvent ajouter des utilisateurs IAM Identity Center. Toutefois, une fois que les utilisateurs finaux ont été ajoutés au AWSAccountFactorygroupe, ils peuvent créer de nouveaux utilisateurs IAM Identity Center à l'aide de l'assistant Account Factory.

Pour de plus amples informations, veuillez consulter Provisionner et gérer des comptes avec Account Factory.

Si vous choisissez la valeur par défaut recommandée, AWS Control Tower configure votre zone de landing zone avec un répertoire préconfiguré qui vous aide à gérer les identités des utilisateurs et l'authentification unique, afin que vos utilisateurs disposent d'un accès fédéré entre les comptes. Lorsque vous configurez votre zone de landing zone, ce répertoire par défaut est créé pour contenir les groupes d'utilisateurs et les ensembles d'autorisations.

> **Note**
>
> Vous pouvez déléguer l'administration de AWS IAM Identity Center votre organisation à un compte autre que le compte de gestion, en utilisant la fonctionnalité d'administrateur délégué d'IAM Identity Center. Si vous choisissez d'utiliser cette fonctionnalité, sachez que les administrateurs autorisés à gérer l'appartenance à un groupe peuvent également gérer les groupes assignés au compte de gestion. Pour plus d'informations, consultez ce billet de blog intitulé Getting started with AWS SSO Delegated Administration

Groupes d'utilisateurs, rôles et ensembles d'autorisations

Les groupes d'utilisateurs gèrent les rôles spécialisés définis dans vos comptes partagés. Les rôles établissent des jeux d'autorisations qui sont liés entre eux. Tous les membres d'un groupe héritent des jeux d'autorisations, ou rôles, associés à ce groupe. Vous pouvez créer d'autres groupes pour les utilisateurs finaux de vos comptes membres. De cette façon, vous pouvez personnaliser l'affectation des rôles en n'affectant que ceux qui sont nécessaires aux tâches spécifiques effectuées par un groupe.

Les ensembles d'autorisations disponibles couvrent un large éventail d'exigences d'autorisation utilisateur distinctes, telles que l'accès en lecture seule, l'accès administratif à AWS Control Tower et l'accès au Service Catalog. Ces ensembles d'autorisations permettent à vos utilisateurs finaux de créer rapidement leurs propres AWS comptes dans votre zone de landing zone, conformément aux directives de votre entreprise.

Pour obtenir des conseils sur la planification des allocations d'utilisateurs, de groupes et d'autorisations, consultez Recommandations pour configurer des groupes, des rôles et des politiques .

Pour plus d'informations sur l'utilisation de ce service dans le contexte d'AWS Control Tower, consultez les rubriques suivantes du guide de l'AWS IAM Identity Center utilisateur.

- Pour ajouter des utilisateurs, veuillez consulter Ajouter des utilisateurs.
- Pour ajouter des utilisateurs à des groupes, veuillez consulter Ajouter des utilisateurs aux groupes.
- Pour modifier les propriétés de l'utilisateur, veuillez consulter la section Modifier les propriétés d'un utilisateur.
- Pour ajouter un groupe, consultez Ajout de groupes.

> **Warning**
>
> AWS Control Tower configure le répertoire de votre centre d'identité IAM dans votre région d'origine. Si vous configurez votre zone d'atterrissage dans une autre région, puis que vous accédez à la console IAM Identity Center, vous devez remplacer la région par votre région d'origine. Ne supprimez pas la configuration de votre centre d'identité IAM dans votre région d'origine.

Ce qu'il faut savoir sur les comptes IAM Identity Center et AWS Control Tower

Voici quelques informations utiles à connaître lorsque vous travaillez avec des comptes utilisateur IAM Identity Center dans AWS Control Tower.

- Si votre compte utilisateur AWS IAM Identity Center est désactivé, vous recevrez un message d'erreur lorsque vous tenterez de configurer de nouveaux comptes dans Account Factory. Vous pouvez réactiver votre utilisateur IAM Identity Center dans la console IAM Identity Center.
- Si vous spécifiez une nouvelle adresse e-mail utilisateur IAM Identity Center lorsque vous mettez à jour le produit provisionné associé à un compte vendu par Account Factory, AWS Control Tower crée un nouveau compte utilisateur IAM Identity Center. Le compte d'utilisateur créé précédemment n'est pas supprimé. Si vous préférez supprimer l'ancienne adresse e-mail de l'utilisateur IAM Identity Center d' AWS IAM Identity Center, consultez la section Désactivation d'un utilisateur.
- AWS IAM Identity Center a été intégré à Azure Active Directory, et vous pouvez connecter votre Azure Active Directory existant à AWS Control Tower.

- Pour plus d'informations sur la manière dont le comportement d'AWS Control Tower interagit avec AWS IAM Identity Center et les différentes sources d'identité, consultez les considérations relatives à la modification de votre source d'identité dans la documentation d' AWS IAM Identity Center.

Groupes de centres d'identité IAM pour AWS Control Tower

AWS Control Tower propose des groupes préconfigurés pour organiser les utilisateurs qui effectuent des tâches spécifiques dans vos comptes. Vous pouvez ajouter des utilisateurs et les affecter à ces groupes directement dans IAM Identity Center. Cela permet de faire correspondre les jeux d'autorisations aux utilisateurs dans des groupes au sein de vos comptes. Les groupes suivants sont créés lorsque vous configurez votre zone de landing zone.

AWSAccountFactory

Compte	Jeux d'autorisations	Description
Compte de gestion	AWSServiceCatalogEndUserAccess	Ce groupe est uniquement utilisé dans ce compte pour approvisionner de nouveaux comptes à l'aide de Account Factory.

AWSServiceCatalogAdmins

Compte	Jeux d'autorisations	Description
Compte de gestion	AWSServiceCatalogAdminFullAccess	Ce groupe est uniquement utilisé dans ce compte pour apporter des modifications administratives à Account Factory. Les utilisateurs de ce groupe ne peuvent pas créer de nouveaux comptes s'ils ne font pas également partie du AWSAccountFactorygroupe.

AWSControlTowerAdmins

Compte	Jeux d'autorisations	Description
Compte de gestion	AWSAdministratorAccess	Les utilisateurs de ce groupe dans ce compte sont les seuls à avoir accès à la console AWS Control Tower.
Compte d'archivage des journaux	AWSAdministratorAccess	Les utilisateurs ont un accès administrateur dans ce compte.
Compte d'audit	AWSAdministratorAccess	Les utilisateurs ont un accès administrateur dans ce compte.
Comptes membres	AWSOrganizationsFullAccess	Les utilisateurs ont un accès complet aux Organizations dans ce compte.

AWSSecurityAuditPowerUsers

Compte	Jeux d'autorisations	Description
Compte de gestion	AWSPowerUserAccess	Les utilisateurs peuvent effectuer des tâches de développement d'applications et créer et configurer des ressources et des services qui prennent en charge le AWS développement d'applications avisées.
Compte d'archivage des journaux	AWSPowerUserAccess	Les utilisateurs peuvent effectuer des tâches de développement d'applications et créer et configurer des

Compte	Jeux d'autorisations	Description
		ressources et des services qui prennent en charge le AWS développement d'applications avisées.
Compte d'audit	AWSPowerUserAccess	Les utilisateurs peuvent effectuer des tâches de développement d'applications et créer et configurer des ressources et des services qui prennent en charge le AWS développement d'applications avisées.
Comptes membres	AWSPowerUserAccess	Les utilisateurs peuvent effectuer des tâches de développement d'applications et créer et configurer des ressources et des services qui prennent en charge le AWS développement d'applications avisées.

AWSSecurityAuditors

Compte	Jeux d'autorisations	Description
Compte de gestion	AWSReadOnlyAccess	Les utilisateurs ont un accès en lecture seule à tous les AWS services et ressources de ce compte.
Compte d'archivage des journaux	AWSReadOnlyAccess	Les utilisateurs ont un accès en lecture seule à tous les

Compte	Jeux d'autorisations	Description
		AWS services et ressources de ce compte.
Compte d'audit	AWSReadOnlyAccess	Les utilisateurs ont un accès en lecture seule à tous les AWS services et ressources de ce compte.
Comptes membres	AWSReadOnlyAccess	Les utilisateurs ont un accès en lecture seule à tous les AWS services et ressources de ce compte.

AWSLogArchiveAdmins

Compte	Jeux d'autorisations	Description
Compte d'archivage des journaux	AWSAdministratorAccess	Les utilisateurs ont un accès administrateur dans ce compte.

AWSLogArchiveViewers

Compte	Jeux d'autorisations	Description
Compte d'archivage des journaux	AWSReadOnlyAccess	Les utilisateurs ont un accès en lecture seule à tous les AWS services et ressources de ce compte.

AWSAuditAccountAdmins

Compte	Jeux d'autorisations	Description
Compte d'audit	AWSAdministratorAccess	Les utilisateurs ont un accès administrateur dans ce compte.

Présentation de la gestion des autorisations d'accès à vos ressources AWS Control Tower

Chaque AWS ressource appartient à un Compte AWS, et les autorisations permettant de créer une ressource ou d'y accéder sont régies par des politiques d'autorisation. Un compte administrateur peut attacher des politiques d'autorisations à des identités IAM (c'est-à-dire des utilisateurs, des groupes et des rôles). Certains services (tels que AWS Lambda) permettent également d'associer des politiques d'autorisation aux ressources.

> **Note**
>
> Un administrateur de compte (ou utilisateur administrateur) est un utilisateur doté des privilèges d'administrateur. Pour plus d'informations, consultez Bonnes pratiques IAM dans le Guide de l'utilisateur IAM.

Lorsque vous êtes chargé d'accorder des autorisations à un utilisateur ou à un rôle, vous devez connaître et suivre les utilisateurs et les rôles qui nécessitent des autorisations, les ressources pour lesquelles chaque utilisateur et chaque rôle ont besoin d'autorisations, ainsi que les actions spécifiques qui doivent être autorisées pour exploiter ces ressources.

Rubriques

- Ressources et opérations d'AWS Control Tower
- À propos de la propriété des ressources
- Gérez l'accès aux ressources
- Spécifiez les éléments de politique : actions, effets et principes
- Spécification de conditions dans une politique

Ressources et opérations d'AWS Control Tower

Dans AWS Control Tower, la ressource principale est une zone d'atterrissage. AWS Control Tower prend également en charge un type de ressource supplémentaire, les contrôles, parfois appelés barrières de sécurité. Toutefois, pour AWS Control Tower, vous ne pouvez gérer les contrôles que dans le contexte d'une zone de landing zone existante. Les contrôles peuvent être considérés comme des sous-ressources.

Les ressources et sous-ressources de AWS sont associées à des noms de ressources Amazon (ARN) uniques, comme indiqué dans l'exemple suivant.

AWS Control Tower fournit un ensemble d'opérations d'API destinées à fonctionner avec les ressources d'AWS Control Tower. Pour obtenir la liste des opérations disponibles, consultez AWS Control Tower the AWS Control Tower API Reference.

Pour plus d'informations sur les AWS CloudFormation ressources d'AWS Control Tower, consultez le guide de AWS CloudFormation l'utilisateur.

À propos de la propriété des ressources

Le AWS compte possède les ressources créées dans le compte, quelle que soit la personne qui les a créées. Plus précisément, le propriétaire de la ressource est le AWS compte de l'entité principale (c'est-à-dire l'utilisateur Compte AWS root, un utilisateur IAM Identity Center, un utilisateur IAM ou un rôle IAM) qui authentifie la demande de création de ressource. Les exemples suivants illustrent comment cela fonctionne :

- Si vous utilisez les AWS informations d'identification de l'utilisateur root de votre AWS compte pour configurer une zone d'atterrissage, votre AWS compte est le propriétaire de la ressource.
- Si vous créez un utilisateur IAM dans votre AWS compte et que vous accordez à cet utilisateur l'autorisation de configurer une zone d'atterrissage, celui-ci peut configurer une zone d'atterrissage à condition que son compte réponde aux conditions requises. Cependant, votre AWS compte, auquel appartient l'utilisateur, possède la ressource de la zone d'atterrissage.
- Si vous créez un rôle IAM dans votre AWS compte avec les autorisations nécessaires pour configurer une zone d'atterrissage, toute personne habilitée à assumer ce rôle peut configurer une zone d'atterrissage. Votre AWS compte, auquel appartient le rôle, possède la ressource de la zone d'atterrissage.

Gérez l'accès aux ressources

Une politique d'autorisation décrit qui a accès à quoi. La section suivante explique les options disponibles pour créer des politiques d'autorisations.

> **Note**
>
> Cette section décrit l'utilisation d'IAM dans le contexte d'AWS Control Tower. Elle ne fournit pas d'informations détaillées sur le service IAM. Pour une documentation complète sur IAM, consultez Qu'est-ce que IAM ? dans le Guide de l'utilisateur IAM. Pour plus d'informations sur la syntaxe et les descriptions des stratégies IAM, consultez Référence de stratégie AWS IAM dans le Guide de l'utilisateur IAM.

Les politiques associées à une identité IAM sont appelées politiques basées sur l'identité (politiques IAM). Les stratégies attachées à une ressource sont appelées stratégies basées sur une ressource.

> **Note**
>
> AWS Control Tower prend uniquement en charge les politiques basées sur l'identité (politiques IAM).

Rubriques

À propos des politiques basées sur l'identité (politiques IAM)

Vous pouvez attacher des politiques à des identités IAM. Par exemple, vous pouvez effectuer les opérations suivantes :

- Associer une politique d'autorisations à un utilisateur ou à un groupe de votre compte : pour accorder à un utilisateur l'autorisation de créer une ressource AWS Control Tower, par exemple pour configurer une zone de landing zone, vous pouvez associer une politique d'autorisations à un utilisateur ou à un groupe auquel appartient l'utilisateur.

- Attacher une politique d'autorisations à un rôle (accorder des autorisations entre comptes) : vous pouvez attacher une politique d'autorisation basée sur une identité à un rôle IAM afin d'accorder des autorisations entre comptes. Par exemple, l'administrateur d'un AWS compte (compte A) peut créer un rôle qui accorde des autorisations entre comptes à un autre AWS compte (compte B), ou l'administrateur peut créer un rôle qui accorde des autorisations à un autre AWS service.
  1. L'administrateur du compte A crée un rôle IAM et associe une politique d'autorisation au rôle qui accorde des autorisations pour gérer les ressources du compte A.
  2. L'administrateur du compte A attache une politique de confiance au rôle. La politique indique que le compte B est le principal habilité à assumer ce rôle.
  3. En tant que principal, l'administrateur du compte B peut autoriser n'importe quel utilisateur du compte B à assumer ce rôle. En assumant le rôle, les utilisateurs du compte B peuvent créer ou accéder aux ressources du compte A.
  4. Pour accorder à un AWS service la capacité (autorisations) d'assumer le rôle, le principal que vous spécifiez dans la politique de confiance peut être un AWS service.

Création de rôles et attribution d'autorisations

Les rôles et les autorisations vous donnent accès aux ressources, dans AWS Control Tower et dans d'autres AWS services, y compris l'accès programmatique aux ressources.

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

  Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center .
- Utilisateurs gérés dans IAM par un fournisseur d'identité :

  Créez un rôle pour la fédération d'identité. Pour plus d'informations, voir la rubrique Création d'un rôle pour un fournisseur d'identité tiers (fédération) du Guide de l'utilisateur IAM.
- Utilisateurs IAM :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique Création d'un rôle pour un utilisateur IAM du Guide de l'utilisateur IAM.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique Ajout d'autorisations à un utilisateur (console) du Guide de l'utilisateur IAM.

Pour en savoir plus sur l'utilisation d'IAM pour déléguer des autorisations, consultez Gestion des accès dans le Guide de l'utilisateur IAM.

> **Note**
>
> Lorsque vous configurez une zone de landing zone AWS Control Tower, vous aurez besoin d'un utilisateur ou d'un rôle associé AdministratorAccessà la politique gérée. (arn:aws:iam : :aws:policy/) AdministratorAccess

Pour créer un rôle pour une Service AWS (console IAM)

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation de la console IAM, sélectionnez Roles (Rôles), puis Create role (Créer un rôle).
3. Pour Trusted entity (Entité de confiance), choisissez Service AWS.
4. Pour Service ou cas d'utilisation, choisissez un service, puis choisissez le cas d'utilisation. Les cas d'utilisation sont définis par le service pour inclure la politique d'approbation nécessaire au service.
5. Choisissez Suivant.
6. Pour les politiques d'autorisations, les options dépendent du cas d'utilisation que vous avez sélectionné :

   - Si le service définit les autorisations pour le rôle, vous ne pouvez pas sélectionner de politiques d'autorisation.
   - Choisissez parmi un ensemble limité de politiques d'autorisation.
   - Choisissez parmi toutes les politiques d'autorisation.
   - Sélectionnez aucune politique d'autorisation, créez les politiques une fois le rôle créé, puis attachez les politiques au rôle.
7. (Facultatif) Définissez une limite d'autorisations. Il s'agit d'une fonctionnalité avancée disponible pour les fonctions de service, mais pas pour les rôles liés à un service.

   a. Ouvrez la section Définir les limites des autorisations, puis choisissez Utiliser une limite d'autorisations pour contrôler le nombre maximal d'autorisations de rôle.

      IAM inclut une liste des politiques AWS gérées et gérées par le client dans votre compte.

b. Sélectionnez la politique à utiliser comme limite d'autorisations.

8. Choisissez Suivant.
9. Pour le nom du rôle, les options dépendent du service :

   - Si le service définit le nom du rôle, vous ne pouvez pas le modifier.
   - Si le service définit un préfixe pour le nom du rôle, vous pouvez saisir un suffixe facultatif.
   - Si le service ne définit pas le nom du rôle, vous pouvez le nommer.

   > **Important**
   >
   > Lorsque vous nommez un rôle, tenez compte des points suivants :
   >
   > - Les noms de rôles doivent être uniques au sein du Compte AWS vôtre et ne peuvent pas être rendus uniques au cas par cas.
   >
   >   Par exemple, ne créez pas de rôles nommés à la fois **`PRODROLE`** et**`prodrole`**. Lorsqu'un nom de rôle est utilisé dans une politique ou dans le cadre d'un ARN, il distingue les majuscules et minuscules, mais lorsqu'un nom de rôle apparaît aux clients dans la console, par exemple pendant le processus de connexion, le nom du rôle ne fait pas la distinction entre majuscules et minuscules.
   > - Vous ne pouvez pas modifier le nom du rôle une fois qu'il a été créé car d'autres entités peuvent y faire référence.

10. (Facultatif) Dans Description, entrez une description pour le rôle.
11. (Facultatif) Pour modifier les cas d'utilisation et les autorisations du rôle, dans les sections Étape 1 : Sélection des entités de confiance ou Étape 2 : Ajouter des autorisations, choisissez Modifier.
12. (Facultatif) Pour identifier, organiser ou rechercher le rôle, ajoutez des balises sous forme de paires clé-valeur. Pour plus d'informations sur l'utilisation des balises dans IAM, consultez la rubrique Balisage des ressources IAM dans le Guide de l'utilisateur IAM.
13. Passez en revue les informations du rôle, puis choisissez Create role (Créer un rôle).

Pour utiliser l'éditeur de politique JSON afin de créer une politique

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation de gauche, sélectionnez Policies (Politiques).

Si vous sélectionnez Politiques pour la première fois, la page Bienvenue dans les politiques gérées s'affiche. Sélectionnez Mise en route.

3. En haut de la page, sélectionnez Créer une politique.
4. Dans la section Éditeur de politiques, choisissez l'option JSON.
5. Saisissez ou collez un document de politique JSON. Pour de plus amples informations sur le langage de la stratégie IAM, consultez la référence de politique JSON IAM.
6. Résolvez les avertissements de sécurité, les erreurs ou les avertissements généraux générés durant la validation de la politique, puis choisissez Suivant.

> **Note**
>
> Vous pouvez basculer à tout moment entre les options des éditeurs visuel et JSON. Toutefois, si vous apportez des modifications ou si vous choisissez Suivant dans l'éditeur visuel, IAM peut restructurer votre politique afin de l'optimiser pour l'éditeur visuel. Pour de plus amples informations, consultez la page Restructuration de politique dans le Guide de l'utilisateur IAM.

7. (Facultatif) Lorsque vous créez ou modifiez une politique dans le AWS Management Console, vous pouvez générer un modèle de stratégie JSON ou YAML que vous pouvez utiliser dans les AWS CloudFormation modèles.

   Pour ce faire, dans l'éditeur de politiques, sélectionnez Actions, puis sélectionnez Générer CloudFormation un modèle. Pour en savoir plus AWS CloudFormation, consultez la référence aux types de AWS Identity and Access Management ressources dans le Guide de AWS CloudFormation l'utilisateur.
8. Lorsque vous avez fini d'ajouter des autorisations à la politique, choisissez Suivant.
9. Sur la page Vérifier et créer, tapez un Nom de politique et une Description (facultative) pour la politique que vous créez. Vérifiez les Autorisations définies dans cette politique pour voir les autorisations accordées par votre politique.
10. (Facultatif) Ajoutez des métadonnées à la politique en associant les balises sous forme de paires clé-valeur. Pour plus d'informations sur l'utilisation des balises dans IAM, consultez la rubrique Balisage des ressources IAM dans le Guide de l'utilisateur IAM.
11. Choisissez Create policy (Créer une politique) pour enregistrer votre nouvelle politique.

Pour utiliser l'éditeur visuel afin de créer une politique

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation de gauche, sélectionnez Policies (Politiques).

   Si vous sélectionnez Politiques pour la première fois, la page Bienvenue dans les politiques gérées s'affiche. Sélectionnez Get started (Mise en route).
3. Sélectionnez Créer une politique.
4. Dans la section Éditeur de politiques, recherchez la section Sélectionner un service, puis choisissez un Service AWS. Vous pouvez utiliser le menu Filtre ou la zone de recherche en haut de l'écran pour limiter les résultats dans la liste des services. Vous pouvez choisir un seul service par bloc d'autorisation de l'éditeur visuel. Pour accorder l'accès à plusieurs services, ajoutez de multiples blocs d'autorisation en sélectionnant Ajouter d'autres autorisations.
5. Dans Actions autorisées, choisissez les actions à ajouter à la politique. Vous pouvez choisir des actions de différentes manières :

   - Activez la case à cocher pour toutes les actions.
   - Choisissez Ajouter des actions pour saisir le nom d'une action spécifique. Vous pouvez utiliser un caractère générique (*) pour spécifier plusieurs actions.
   - Sélectionnez l'un des groupes de niveau Accès pour choisir toutes les actions pour le niveau d'accès (par exemple, Lecture, Écriture ou Liste).
   - Développez chacun des groupes de Niveaux d'accès pour choisir des actions individuelles.

   Par défaut, la politique que vous créez autorise les actions que vous choisissez. Pour refuser les actions choisies, sélectionnez Switch to deny permissions (Basculer vers le refus des autorisations). Le comportement par défaut d'IAM étant le refus, nous vous recommandons comme bonne pratique de sécurité de n'autoriser un utilisateur à accéder qu'aux actions et aux ressources nécessaires. Créez une instruction JSON pour refuser les autorisations uniquement si vous souhaitez remplacer une autorisation autorisée séparément par une autre déclaration ou politique. Nous vous recommandons de limiter le nombre de refus d'autorisation au minimum, car ils peuvent rendre la résolution des problèmes d'autorisation plus complexe.
6. Pour Ressources, si le service et les actions que vous avez sélectionnés lors des étapes précédentes ne prennent pas en charge le choix de ressources spécifiques, toutes les ressources sont autorisées et vous ne pouvez pas modifier cette section.

Si vous avez choisi une ou plusieurs actions qui prennent en charge les autorisations de niveau ressource, l'éditeur visuel affiche la liste de ces ressources. Vous pouvez alors développer Ressources pour spécifier les ressources de votre politique.

Vous pouvez spécifier des ressources de la manière suivante :

- Choisissez Ajouter des ARN pour spécifier des ressources par leur Amazon Resource Name (ARN). Vous pouvez utiliser l'éditeur visuel ARN ou répertorier les ARN manuellement. Pour plus d'informations sur la syntaxe des ARN, consultez Amazon Resource Names (ARNs) dans le guide de l'utilisateur IAM. Pour plus d'informations sur l'utilisation des ARN dans l'`Resource`élément d'une politique, voir Éléments de stratégie IAM JSON : ressource dans le guide de l'utilisateur IAM.
- Choisissez Toute ressource dans ce compte en regard d'une ressource pour accorder des autorisations à toutes les ressources de ce type.
- Choisissez Toutes pour choisir toutes les ressources pour le service.

7. (Facultatif) Choisissez Demander des conditions – facultatif pour ajouter des conditions à la politique que vous créez. Des conditions limitent l'effet d'une instruction de politique JSON. Par exemple, vous pouvez spécifier qu'un utilisateur est autorisé à effectuer des actions sur les ressources uniquement si la demande de cet utilisateur se produit au cours d'une période spécifiée. Vous pouvez également utiliser des conditions couramment utilisées pour limiter l'authentification d'un utilisateur à l'aide d'un dispositif d'authentification multifactorielle (MFA). Ou vous pouvez exiger que la demande provienne d'une certaine plage d'adresses IP. Pour obtenir la liste de toutes les clés contextuelles que vous pouvez utiliser dans une condition de politique, consultez la section Actions, ressources et clés de condition pour les AWS services dans la référence d'autorisation de service.

   Vous pouvez choisir des conditions de différentes manières :

   - Utilisez les cases à cocher pour sélectionner les conditions couramment utilisées.
   - Choisissez Ajouter une autre condition pour spécifier d'autres conditions. Choisissez la clé de condition, le qualificatif et l'opérateur de la condition, puis entrez une valeur. Pour ajouter plusieurs valeurs, choisissez Ajouter. Vous pouvez considérer que les valeurs sont connectées par un `OR` opérateur logique. Lorsque vous avez fini, choisissez Ajouter une condition.

   Pour ajouter plusieurs conditions, choisissez de nouveau Ajouter une autre condition. Répétez l'opération si nécessaire. Chaque condition s'applique uniquement à ce bloc d'autorisation de

l'éditeur visuel. Toutes les conditions doivent être remplies pour que le bloc d'autorisation soit considérée comme réussi. En d'autres termes, considérez les conditions à connecter par un `AND` opérateur logique.

Pour plus d'informations sur l'élément Condition, voir Éléments de politique IAM JSON : Condition dans le guide de l'utilisateur IAM.

8. Pour ajouter d'autres blocs d'autorisation, choisissez Ajouter d'autres autorisations. Pour chaque bloc, répétez les étapes 2 à 5.

> **Note**
>
> Vous pouvez basculer à tout moment entre les options des éditeurs visuel et JSON. Toutefois, si vous apportez des modifications ou si vous choisissez Suivant dans l'éditeur visuel, IAM peut restructurer votre politique afin de l'optimiser pour l'éditeur visuel. Pour de plus amples informations, consultez la page Restructuration de politique dans le Guide de l'utilisateur IAM.

9. (Facultatif) Lorsque vous créez ou modifiez une politique dans le AWS Management Console, vous pouvez générer un modèle de stratégie JSON ou YAML que vous pouvez utiliser dans les AWS CloudFormation modèles.

   Pour ce faire, dans l'éditeur de politiques, sélectionnez Actions, puis sélectionnez Générer CloudFormation un modèle. Pour en savoir plus AWS CloudFormation, consultez la référence aux types de AWS Identity and Access Management ressources dans le Guide de AWS CloudFormation l'utilisateur.

10. Lorsque vous avez fini d'ajouter des autorisations à la politique, choisissez Suivant.
11. Sur la page Vérifier et créer, tapez un Nom de politique et une Description (facultative) pour la politique que vous créez. Vérifiez les Autorisations définies dans cette politique pour vous assurer que vous les avez accordées comme prévu.
12. (Facultatif) Ajoutez des métadonnées à la politique en associant les balises sous forme de paires clé-valeur. Pour plus d'informations sur l'utilisation des balises dans IAM, consultez la rubrique Balisage des ressources IAM dans le Guide de l'utilisateur IAM.
13. Choisissez Create policy (Créer une politique) pour enregistrer votre nouvelle politique.

Pour accorder un accès programmatique

Les utilisateurs ont besoin d'un accès programmatique s'ils souhaitent interagir avec AWS l'extérieur du AWS Management Console. La manière d'accorder un accès programmatique dépend du type d'utilisateur qui y accède AWS.

Pour accorder aux utilisateurs un accès programmatique, choisissez l'une des options suivantes.

Quel utilisateur a besoin d'un accès programmatique ?	Pour	Par
Identité de la main-d'œuvre (Utilisateurs gérés dans IAM Identity Center)	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour le AWS CLI, voir Configuration du AWS CLI à utiliser AWS IAM Identity Center dans le guide de AWS Command Line Interface l'utilisateur. • Pour les AWS SDK, les outils et les AWS API, consultez la section Authentification IAM Identity Center dans le Guide de référence AWS des SDK et des outils.
IAM	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de la section Utilisation d'informations d'identification temporaires avec AWS les ressources du Guide de l'utilisateur IAM.
IAM	(Non recommandé) Utilisez des informations d'identification à long terme pour signer les AWS CLI	Suivez les instructions de l'interface que vous souhaitez utiliser.

Quel utilisateur a besoin d'un accès programmatique ?	Pour	Par
	demandes programmatiques adressées aux AWS SDK ou AWS aux API.	• Pour le AWS CLI, voir Authentification à l'aide des informations d'identification utilisateur IAM dans le Guide de l'AWS Command Line Interface utilisateur. • Pour les AWS SDK et les outils, voir Authentifier à l'aide d'informations d'identification à long terme dans le Guide de AWS référence des SDK et des outils. • Pour les AWS API, consultez la section Gestion des clés d'accès pour les utilisateurs IAM dans le guide de l'utilisateur IAM.

Protégez-vous contre les attaquants

Pour plus d'informations sur la manière de vous protéger contre les attaquants lorsque vous accordez des autorisations à d'autres responsables de AWS service, consultez la section Conditions facultatives relatives à vos relations de confiance en matière de rôles. En ajoutant certaines conditions à vos politiques, vous pouvez contribuer à empêcher un type d'attaque spécifique, connu sous le nom d'attaque adjointe confuse, qui se produit lorsqu'une entité contraint une entité plus privilégiée à effectuer une action, par exemple dans le cas d'une usurpation d'identité interservices. Pour des informations générales sur les conditions du contrat, voir égalementSpécification de conditions dans une politique.

Pour plus d'informations sur l'utilisation de politiques basées sur l'identité avec AWS Control Tower, consultez. Utilisation de politiques basées sur l'identité (politiques IAM) pour AWS Control Tower Pour de plus amples informations sur les utilisateurs, les groupes, les rôles et les autorisations, consultez Identités (utilisateurs, groupes et rôles) dans le Guide de l'utilisateur IAM.

Politiques basées sur les ressources

D'autres services, tels qu'Amazon S3, prennent également en charge les politiques d'autorisation basées sur une ressource. Par exemple, vous pouvez attacher une politique à un compartiment S3 pour gérer les autorisations d'accès à ce compartiment. AWS Control Tower ne prend pas en charge les politiques basées sur les ressources.

Spécifiez les éléments de politique : actions, effets et principes

Vous pouvez configurer et gérer votre zone d'atterrissage via la console AWS Control Tower ou les API de zone d'atterrissage. Pour configurer votre zone de landing zone, vous devez être un utilisateur IAM doté des autorisations administratives définies dans une politique IAM.

Les éléments suivants sont les plus élémentaires que vous pouvez identifier dans une politique :

- Ressource : dans une politique, vous utilisez un Amazon Resource Name (ARN) pour identifier la ressource à laquelle la politique s'applique. Pour plus d'informations, consultez Ressources et opérations d'AWS Control Tower.
- Action : vous utilisez des mots clés d'action pour identifier les opérations de ressource que vous voulez accorder ou refuser. Pour plus d'informations sur les types d'actions pouvant être effectuées, consultez la section Actions définies par AWS Control Tower.
- Effet – Vous spécifiez l'effet produit lorsque l'utilisateur demande l'action spécifique, qui peut être une autorisation ou un refus. Si vous n'accordez pas explicitement l'accès pour (autoriser) une ressource, l'accès est implicitement refusé. Vous pouvez aussi explicitement refuser l'accès à une ressource, ce que vous pouvez faire afin de vous assurer qu'un utilisateur n'y a pas accès, même si une politique différente accorde l'accès.
- Principal — Dans les politiques basées sur l'identité (politiques IAM), l'utilisateur auquel la politique est attachée est le principal implicite. Pour les politiques basées sur une ressource, vous spécifiez l'utilisateur, le compte, le service ou une autre entité qui doit recevoir les autorisations (s'applique uniquement aux politiques basées sur une ressource). AWS Control Tower ne prend pas en charge les politiques basées sur les ressources.

Pour en savoir plus sur la syntaxe des stratégies IAM et pour obtenir des descriptions, consultez Référence de stratégie IAM AWS dans le Guide de l'utilisateur IAM.

Spécification de conditions dans une politique

Lorsque vous accordez des autorisations, vous pouvez utiliser le langage des politiques IAM afin de spécifier les conditions définissant à quel moment une politique doit prendre effet. Par exemple, il est possible d'appliquer une politique après seulement une date spécifique. Pour plus d'informations sur la spécification de conditions dans un langage de politique, consultez Condition dans le Guide de l'utilisateur IAM.

Pour exprimer des conditions, vous pouvez utiliser des clés de condition prédéfinies. Il n'existe aucune clé de condition spécifique à AWS Control Tower. Cependant, il existe des AWS clés de condition larges que vous pouvez utiliser le cas échéant. Pour obtenir la liste complète des touches AWS-wide, consultez la section Clés disponibles pour les conditions dans le guide de l'utilisateur IAM.

Empêchez l'usurpation d'identité entre services

En AWS, l'usurpation d'identité interservices peut entraîner la confusion des adjoints. Lorsqu'un service appelle un autre service, l'usurpation d'identité entre services se produit si un service manipule un autre service pour utiliser ses autorisations afin d'agir sur les ressources d'un client d'une manière qui n'est pas autorisée autrement. Pour empêcher cette attaque, AWS fournit des outils pour vous aider à protéger vos données, afin que seuls les services disposant d'une autorisation légitime puissent accéder aux ressources de votre compte.

Nous vous recommandons d'utiliser les `aws:SourceAccount` conditions `aws:SourceArn` et de vos politiques afin de limiter les autorisations qu'AWS Control Tower accorde à un autre service pour accéder à vos ressources.

- À utiliser `aws:SourceArn` si vous souhaitez qu'une seule ressource soit associée à un accès multiservice.
- À utiliser `aws:SourceAccount` si vous souhaitez autoriser l'association d'une ressource de ce compte à une utilisation interservices.
- Si la `aws:SourceArn` valeur ne contient pas l'ID de compte, tel que l'ARN d'un compartiment Amazon S3, vous devez utiliser les deux conditions pour limiter les autorisations.
- Si vous utilisez les deux conditions, et si la `aws:SourceArn` valeur contient l'identifiant du compte, la `aws:SourceAccount` valeur et le compte inclus dans la `aws:SourceArn` valeur doivent présenter le même identifiant de compte lorsqu'ils sont utilisés dans la même déclaration de politique

Pour plus d'informations et d'exemples, consultez https://docs.aws.amazon.com/controltower/latest/userguide/conditions-for-role-trust.html.

Utilisation de politiques basées sur l'identité (politiques IAM) pour AWS Control Tower

Cette rubrique fournit des exemples de politiques basées sur l'identité qui montrent comment un administrateur de compte peut associer des politiques d'autorisations aux identités IAM (c'est-à-dire aux utilisateurs, aux groupes et aux rôles) et ainsi accorder des autorisations pour effectuer des opérations sur les ressources de l'AWS Control Tower.

> **Important**
>
> Nous vous recommandons de consulter d'abord les rubriques d'introduction qui expliquent les concepts de base et les options disponibles pour gérer l'accès aux ressources de votre AWS Control Tower. Pour plus d'informations, consultez Présentation de la gestion des autorisations d'accès à vos ressources AWS Control Tower.

Autorisations requises pour utiliser la console AWS Control Tower

AWS Control Tower crée automatiquement trois rôles lorsque vous configurez une zone de landing zone. Les trois rôles sont obligatoires pour autoriser l'accès à la console. AWS Control Tower divise les autorisations en trois rôles. Il s'agit d'une bonne pratique pour restreindre l'accès aux ensembles minimaux d'actions et de ressources.

Trois rôles obligatoires

- AWS ControlTowerAdmin rôle
- AWS ControlTowerStackSetRole
- AWS ControlTowerCloudTrailRole

Nous vous recommandons de restreindre l'accès à vos politiques d'approbation des rôles pour ces rôles. Pour plus d'informations, consultez la section Conditions facultatives relatives à vos relations de confiance.

AWS ControlTowerAdmin rôle

Ce rôle permet à AWS Control Tower d'accéder à l'infrastructure essentielle au maintien de la zone d'atterrissage. Le `AWS ControlTowerAdmin` rôle nécessite une politique gérée attachée et une politique de confiance de rôle pour le rôle IAM. Une politique de confiance dans les rôles est une politique basée sur les ressources, qui spécifie quels principaux peuvent assumer le rôle.

Voici un exemple d'extrait de cette politique de confiance des rôles :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "controltower.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Pour créer ce rôle à partir de la AWS CLI et le placer dans un fichier appelé`trust.json`, voici un exemple de commande CLI :

```
aws iam create-role --role-name AWSControlTowerAdmin --path /service-role/ --assume-
role-policy-document file://trust.json
```

Ce rôle nécessite deux politiques IAM.

1. Une politique en ligne, par exemple :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*"
        }
    ]
```

```
}
```

2. La politique gérée qui suit, qui est la`AWS ControlTowerServiceRolePolicy`.

AWS ControlTowerServiceRolePolicy

AWS ControlTowerServiceRolePolicyIl s'agit d'une politique AWS gérée qui définit les autorisations pour créer et gérer les ressources de la tour de contrôle AWS, telles que les AWS CloudFormation stacksets et les instances de pile, les fichiers AWS CloudTrail journaux, un agrégateur de configuration pour AWS Control Tower, ainsi que les AWS Organizations comptes et les unités organisationnelles (UO) régis par AWS Control Tower.

Les mises à jour de cette politique gérée sont résumées dans le tableauPolitiques gérées pour AWS Control Tower.

Pour plus d'informations, consultez `AWSControlTowerServiceRolePolicy`le guide de référence des politiques gérées par AWS.

Nom de la politique gérée : `AWS ControlTowerServiceRolePolicy`

L'artefact JSON pour `AWS ControlTowerServiceRolePolicy` est le suivant :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:CreateStackInstances",
                "cloudformation:CreateStackSet",
                "cloudformation:DeleteStack",
                "cloudformation:DeleteStackInstances",
                "cloudformation:DeleteStackSet",
                "cloudformation:DescribeStackInstance",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackSet",
                "cloudformation:DescribeStackSetOperation",
                "cloudformation:ListStackInstances",
                "cloudformation:UpdateStack",
                "cloudformation:UpdateStackInstances",
                "cloudformation:UpdateStackSet"
```

```
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:type/resource/AWS-IAM-Role"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "account:EnableRegion",
                "account:ListRegions",
                "account:GetRegionOptStatus"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:CreateStackInstances",
                "cloudformation:CreateStackSet",
                "cloudformation:DeleteStack",
                "cloudformation:DeleteStackInstances",
                "cloudformation:DeleteStackSet",
                "cloudformation:DescribeStackInstance",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackSet",
                "cloudformation:DescribeStackSetOperation",
                "cloudformation:GetTemplate",
                "cloudformation:ListStackInstances",
                "cloudformation:UpdateStack",
                "cloudformation:UpdateStackInstances",
                "cloudformation:UpdateStackSet"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:stack/AWSControlTower*/*",
                "arn:aws:cloudformation:*:*:stack/StackSet-AWSControlTower*/*",
                "arn:aws:cloudformation:*:*:stackset/AWSControlTower*:*",
                "arn:aws:cloudformation:*:*:stackset-target/AWSControlTower*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:CreateTrail",
```

```
                "cloudtrail:DeleteTrail",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail",
                "cloudtrail:PutEventSelectors",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:PutRetentionPolicy"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
                "arn:aws:cloudtrail:*:*:trail/aws-controltower*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::aws-controltower*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution",
                "arn:aws:iam::*:role/AWSControlTowerBlueprintAccess"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "ec2:DescribeAvailabilityZones",
                "iam:ListRoles",
                "logs:CreateLogGroup",
                "logs:DescribeLogGroups",
                "organizations:CreateAccount",
                "organizations:DescribeAccount",
```

```
                "organizations:DescribeCreateAccountStatus",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribePolicy",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy",
                "organizations:ListRoots",
                "organizations:MoveAccount",
                "servicecatalog:AssociatePrincipalWithPortfolio"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "iam:GetUser",
                "iam:ListAttachedRolePolicies",
                "iam:GetRolePolicy"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/service-role/AWSControlTowerStackSetRole",
                "arn:aws:iam::*:role/service-role/AWSControlTowerCloudTrailRole",
                "arn:aws:iam::*:role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "config:DeleteConfigurationAggregator",
```

```
                "config:PutConfigurationAggregator",
                "config:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/aws-control-tower": "managed-by-control-tower"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "organizations:ServicePrincipal": [
                        "config.amazonaws.com",
                        "cloudtrail.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "cloudtrail.amazonaws.com"
                }
            }
        }
    ]
}
```

Politique de confiance dans les rôles :

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
         ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

La politique en ligne est `AWSControlTowerAdminPolicy` la suivante :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

AWS ControlTowerStackSetRole

AWS CloudFormation assume ce rôle pour déployer des ensembles de piles dans les comptes créés par AWS Control Tower. Stratégie en ligne :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution"
            ],
```

```
            "Effect": "Allow"
        }
    ]
}
```

Politique d'approbation

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudformation.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWS ControlTowerCloudTrailRole

AWS Control Tower l'autorise CloudTrail en tant que bonne pratique et fournit ce rôle à CloudTrail. CloudTrailassume ce rôle pour créer et publier CloudTrail des journaux. Stratégie en ligne :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "logs:CreateLogStream",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
            "Effect": "Allow"
        },
        {
            "Action": "logs:PutLogEvents",
            "Resource": "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
            "Effect": "Allow"
        }
    ]
}
```

Politique d'approbation

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWSControlTowerBlueprintAccess exigences relatives aux rôles

AWS Control Tower vous demande de créer le `AWSControlTowerBlueprintAccess` rôle dans le compte Blueprint Hub désigné, au sein de la même organisation.

Nom de rôle

Le nom du rôle doit êtreAWSControlTowerBlueprintAccess.

Politique de confiance dans les rôles

Le rôle doit être configuré de manière à faire confiance aux principes suivants :

- Le principal qui utilise AWS Control Tower dans le compte de gestion.
- Le `AWSControlTowerAdmin` rôle dans le compte de gestion.

L'exemple suivant illustre une politique de confiance fondée sur le principe du moindre privilège. Lorsque vous établissez votre propre politique, remplacez le terme *YourManagementAccountId*par l'identifiant de compte réel de votre compte de gestion AWS Control Tower, et remplacez le terme *YourControlTowerUserRole*par l'identifiant du rôle IAM pour votre compte de gestion.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
```

```
                "AWS": [
                    "arn:aws:iam::YourManagementAccountId:role/service-role/
AWSControlTowerAdmin",

 "arn:aws:iam::YourManagementAccountId:role/YourControlTowerUserRole"
                ]
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

Autorisations relatives aux rôles

Vous devez associer la politique gérée AWSServiceCatalogAdminFullAccessau rôle.

AWSServiceRoleForAWSControlTower

Ce rôle permet à AWS Control Tower d'accéder au compte Log Archive, au compte d'audit et aux comptes des membres, pour les opérations essentielles au maintien de la zone de landing zone, telles que la notification des ressources dérivées.

Le `AWSServiceRoleForAWSControlTower` rôle nécessite une politique gérée attachée et une politique de confiance de rôle pour le rôle IAM.

Politique gérée pour ce rôle : `AWSControlTowerAccountServiceRolePolicy`

Politique de confiance dans les rôles :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "controltower.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWSControlTowerAccountServiceRolePolicy

Cette politique AWS gérée permet à AWS Control Tower d'appeler AWS des services qui fournissent une configuration de compte automatisée et une gouvernance centralisée en votre nom.

La politique contient les autorisations minimales permettant à AWS Control Tower de mettre en œuvre le transfert des AWS Security Hub résultats pour les ressources gérées par les contrôles Security Hub qui font partie de la norme gérée par le Security Hub Service : AWS Control Tower, et elle empêche les modifications qui limitent la capacité à gérer les comptes clients. Cela fait partie du processus de détection de la AWS Security Hub dérive de fond qui n'est pas directement initié par le client.

La politique donne l'autorisation de créer des EventBridge règles Amazon, en particulier pour les contrôles Security Hub, dans chaque compte membre, et ces règles doivent en spécifier une exacte EventPattern. De plus, une règle ne peut fonctionner que sur des règles gérées par notre directeur de service.

Principal du service : `controltower.amazonaws.com`

L'artefact JSON pour `AWSControlTowerAccountServiceRolePolicy` est le suivant :

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
  //For creating the managed rule
   "Sid": "AllowPutRuleOnSpecificSourcesAndDetailTypes",
   "Effect": "Allow",
   "Action": "events:PutRule",
   "Resource": "arn:aws:events:*:*:rule/*ControlTower*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "events:source": "aws.securityhub"
    },
    "Null": {
     "events:detail-type": "false"
    },
    "StringEquals": {
     "events:ManagedBy": "controltower.amazonaws.com",
     "events:detail-type": "Security Hub Findings - Imported"
    }
   }
```

```
  },
  // Other operations to manage the managed rule
  {
   "Sid": "AllowOtherOperationsOnRulesManagedByControlTower",
   "Effect": "Allow",
   "Action": [
    "events:DeleteRule",
    "events:EnableRule",
    "events:DisableRule",
    "events:PutTargets",
    "events:RemoveTargets"
   ],
   "Resource": "arn:aws:events:*:*:rule/*ControlTower*",
   "Condition": {
    "StringEquals": {
     "events:ManagedBy": "controltower.amazonaws.com"
    }
   }
  },
  // More managed rule permissions
  {
   "Sid": "AllowDescribeOperationsOnRulesManagedByControlTower",
   "Effect": "Allow",
   "Action": [
    "events:DescribeRule",
    "events:ListTargetsByRule"
   ],
   "Resource": "arn:aws:events:*:*:rule/*ControlTower*"
  },
  // Add permission to publish the security notifications to SNS
  {
   "Sid": "AllowControlTowerToPublishSecurityNotifications",
   "Effect": "Allow",
   "Action": "sns:publish",
   "Resource": "arn:aws:sns:*:*:aws-controltower-AggregateSecurityNotifications",
   "Condition": {
    "StringEquals": {
     "aws:PrincipalAccount": "${aws:ResourceAccount}"
    }
   }
  },
  // For drift verification
  {
   "Sid": "AllowActionsForSecurityHubIntegration",
```

```
    "Effect": "Allow",
    "Action": [
     "securityhub:DescribeStandardsControls",
     "securityhub:GetEnabledStandards"
    ],
    "Resource": "arn:aws:securityhub:*:*:hub/default"
   }
  ]
}
```

Les mises à jour de cette politique gérée sont résumées dans le tableauPolitiques gérées pour AWS Control Tower.

Politiques gérées pour AWS Control Tower

AWS répond à de nombreux cas d'utilisation courants en fournissant des politiques IAM autonomes créées et administrées par. AWS Les politiques gérées octroient les autorisations requises dans les cas d'utilisation courants et vous évitent d'avoir à réfléchir aux autorisations qui sont requises. Pour plus d'informations, consultez Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

Modification	Description	Date
AWSControlTowerAccountServiceRolePolicy— Une nouvelle politique	AWS Control Tower a ajouté un nouveau rôle lié à un service qui permet à AWS Control Tower de créer et de gérer des règles relatives aux événements et, sur la base de ces règles, de gérer la détection des dérives pour les contrôles liés à Security Hub. Cette modification est nécessaire pour que les clients puissent visualiser les ressources dérivées dans la console, lorsque ces ressources sont liées aux contrôles Security Hub qui font	22 mai 2023

Modification	Description	Date
	partie de la norme gérée par le Security Hub Service : AWS Control Tower.	
AWS ControlTowerServiceRolePolicy – Mise à jour d'une politique existante	AWS Control Tower a ajouté de nouvelles autorisations qui permettent à AWS Control Tower de passer des appels vers `EnableRegion` `ListRegions` , et des `GetRegionOptStatus` API implémentées par le service de gestion des AWS comptes, afin de rendre l'opt-in Régions AWS disponible pour les comptes clients dans la zone de landing zone (compte de gestion, compte d'archive des journaux, compte d'audit, comptes membres de l'unité d'organisation). Ce changement est nécessaire pour que les clients puissent avoir la possibilité d'étendre la gouvernance des régions par AWS Control Tower aux régions optionnelles.	6 avril 2023

Modification	Description	Date
AWS ControlTowerServiceRolePolicy – Mise à jour d'une politique existante	AWS Control Tower a ajouté de nouvelles autorisations qui permettent à AWS Control Tower d'assumer le `AWSControlTowerBlueprintAccess` rôle dans le compte Blueprint (hub), qui est un compte dédié au sein d'une organisation, contenant des plans prédéfinis stockés dans un ou plusieurs produits Service Catalog. AWS Control Tower assume le `AWSControlTowerBlueprintAccess` rôle d'effectuer trois tâches : créer un portefeuille de services Catalog, ajouter le produit Blueprint demandé et partager le portefeuille sur le compte membre demandé au moment de la mise en service du compte. Cette modification est nécessaire pour que les clients puissent créer des comptes personnalisés via AWS Control Tower Account Factory.	28 octobre 2022

Modification	Description	Date
AWS ControlTowerServiceRolePolicy – Mise à jour d'une politique existante	AWS Control Tower a ajouté de nouvelles autorisations qui permettent aux clients de configurer des AWS CloudTrail parcours au niveau de l'organisation, à partir de la version 3.0 de la landing zone. La CloudTrail fonctionnalité basée sur l'organisation exige que les clients aient activé l'accès sécurisé pour le CloudTrail service, et que l'utilisateur ou le rôle IAM soit autorisé à créer un suivi au niveau de l'organisation dans le compte de gestion.	20 juin 2022

Modification	Description	Date
AWS ControlTowerServiceRolePolicy – Mise à jour d'une politique existante	AWS Control Tower a ajouté de nouvelles autorisations qui permettent aux clients d'utiliser le chiffrement par clé KMS. La fonctionnalité KMS permet aux clients de fournir leur propre clé KMS pour chiffrer leurs CloudTrail journaux. Les clients peuvent également modifier la clé KMS lors de la mise à jour ou de la réparation de la zone d'atterrissage. Lors de la mise à jour de la clé KMS, AWS CloudFormation nécessite des autorisations pour appeler l' AWS CloudTrail `PutEventSelector` API. La modification apportée à la politique consiste à autoriser le AWS ControlTowerAdminrôle à appeler l' AWS CloudTrail `PutEventSelector` API.	28 juillet 2021
AWS Control Tower a commencé à suivre les modifications	AWS Control Tower a commencé à suivre les modifications apportées AWS à ses politiques gérées.	27 mai 2021

Sécurité dans AWS Control Tower

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit ceci en tant que sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. L'efficacité de notre sécurité est régulièrement testée et vérifiée par des auditeurs tiers dans le cadre des programmes de conformitéAWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Control Tower, consultez la section AWS Services concernés par programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par les AWS services que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre organisation, et la législation et la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation d'AWS Control Tower. Les rubriques suivantes expliquent comment configurer AWS Control Tower pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser les ressources de votre AWS Control Tower.

Protection des données dans AWS Control Tower

Le modèle de responsabilité AWS partagée de s'applique à la protection des données dans AWS Control Tower. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec AWS Control Tower ou une autre entité à Services AWS l'aide de la console, de l'API ou AWS des kits SDK. AWS CLI Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

> **Note**
>
> La journalisation de l'activité des utilisateurs avec AWS CloudTrail est gérée automatiquement dans AWS Control Tower lorsque vous configurez votre zone de landing zone.

Pour en savoir plus sur la protection des données, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD sur le Blog sur la sécurité d'AWS . AWS Control Tower propose les options suivantes que vous pouvez utiliser pour sécuriser le contenu existant dans votre zone de landing zone :

Rubriques

Chiffrement au repos

AWS Control Tower utilise des compartiments Amazon S3 et des bases de données Amazon DynamoDB qui sont chiffrés au repos à l'aide de clés gérées par Amazon S3 (SSE-S3) pour prendre en charge votre zone de landing zone. Ce chiffrement est configuré par défaut lorsque vous configurez votre zone de landing zone. Vous pouvez éventuellement configurer votre zone de landing zone pour chiffrer les ressources à l'aide de clés de chiffrement KMS. Vous pouvez également établir un chiffrement au repos pour les services que vous utilisez dans votre zone de landing zone pour les services qui le prennent en charge. Pour plus d'informations, consultez le chapitre sur la sécurité de la documentation en ligne de ce service.

Chiffrement en transit

AWS Control Tower utilise le protocole TLS (Transport Layer Security) et le chiffrement côté client pour le chiffrement en transit afin de prendre en charge votre zone de landing zone. En outre, l'accès à AWS Control Tower nécessite l'utilisation de la console, accessible uniquement via un point de terminaison HTTPS. Ce chiffrement est configuré par défaut lorsque vous configurez votre zone de landing zone.

Restreindre l'accès au contenu

La bonne pratique consiste à limiter l'accès au sous-ensemble d'utilisateurs approprié. Avec AWS Control Tower, vous pouvez le faire en vous assurant que vos administrateurs cloud centraux et vos utilisateurs finaux disposent des autorisations IAM appropriées ou, dans le cas des utilisateurs d'IAM Identity Center, qu'ils appartiennent aux bons groupes.

- Pour plus d'informations sur les rôles et les politiques des entités IAM, consultez le Guide de l'utilisateur IAM.

- Pour plus d'informations sur les groupes IAM Identity Center créés lorsque vous configurez votre zone de landing zone, consultezGroupes de centres d'identité IAM pour AWS Control Tower.

Validation de conformité pour AWS Control Tower

AWS Control Tower est un service bien conçu qui peut aider votre organisation à répondre à vos besoins de conformité grâce à des contrôles et à de bonnes pratiques. En outre, des auditeurs tiers évaluent la sécurité et la conformité d'un certain nombre de services que vous pouvez utiliser dans votre zone d'atterrissage dans le cadre de plusieurs programmes de AWS conformité. Il s'agit notamment des certifications SOC, PCI, FedRAMP, HIPAA et d'autres.

Pour une liste des AWS services concernés par des programmes de conformité spécifiques, voir AWS Services concernés par programme de conformité. Pour obtenir des informations générales, consultez Programmes de conformitéAWS.

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, consultez la section Téléchargement de rapports dans AWS Artifact dans le guide de l'AWS Artifact utilisateur.

Lorsque vous utilisez AWS Control Tower, votre responsabilité en matière de conformité dépend de la sensibilité de vos données, des objectifs de conformité de votre entreprise et des lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur la sécurité et la conformité sur. AWS
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.
- AWS Ressources relatives à la conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Config— Ce AWS service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Ce AWS service fournit une vue complète de l'état de votre sécurité interne, AWS ce qui vous permet de vérifier votre conformité aux normes et aux meilleures pratiques du secteur de la sécurité.

Résilience dans AWS Control Tower

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité.

AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées au moyen d'un réseau à faible latence, à haut débit et hautement redondant. Les zones de disponibilité vous permettent de concevoir et d'exploiter des applications et des bases de données qui basculent automatiquement d'une zone de disponibilité à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour obtenir la liste des Régions AWS endroits où AWS Control Tower est disponible, consultezComment AWS les régions fonctionnent avec AWS Control Tower.

Votre région d'origine est définie comme la AWS région dans laquelle votre zone d'atterrissage a été configurée.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS mondiale.

Sécurité de l'infrastructure dans AWS Control Tower

AWS Control Tower est protégée par les procédures de sécurité du réseau AWS mondial décrites dans le livre blanc Amazon Web Services : Overview of Security Processes.

Vous utilisez des appels d'API AWS publiés pour accéder aux AWS services et aux ressources de votre zone de landing zone via le réseau. Nous avons besoin de Transport Layer Security (TLS) 1.2 et recommandons Transport Layer Security (TLS) 1.3 ou version ultérieure. Les clients doivent aussi prendre en charge les suites de chiffrement PFS (Perfect Forward Secrecy) comme Ephemeral Diffie-Hellman (DHE) ou Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Vous pouvez configurer des groupes de sécurité afin de renforcer la sécurité de l'infrastructure réseau pour vos charges de travail liées à la zone de landing zone AWS Control Tower. Pour plus

d'informations, voir Procédure pas à pas : configurer des groupes de sécurité dans AWS Control Tower avec AWS Firewall Manager.

Journalisation et surveillance dans AWS Control Tower

La surveillance vous permet de planifier et d'intervenir en cas d'incidents potentiels. Les résultats des activités de surveillance sont enregistrés dans des fichiers journaux. Par conséquent, la journalisation et la surveillance sont des concepts étroitement liés, et ils jouent un rôle important dans la bonne architecture d'AWS Control Tower.

Lorsque vous configurez votre zone de landing zone, l'un des comptes partagés créés est le compte d'archivage des journaux. Il est dédié à la collecte centralisée de tous les journaux, y compris les journaux de tous vos comptes partagés et membres. Les fichiers journaux sont stockés dans un compartiment Amazon S3. Ces fichiers journaux permettent aux administrateurs et aux auditeurs d'examiner les actions et les événements qui se sont produits.

La meilleure pratique consiste à collecter les données de surveillance de toutes les parties de votre AWS configuration dans vos journaux, afin de pouvoir corriger plus facilement une panne multipoint le cas échéant. AWS fournit plusieurs outils pour surveiller vos ressources et votre activité dans votre zone d'atterrissage.

Par exemple, l'état de vos commandes est surveillé en permanence. Vous pouvez voir leur statut en un coup d'œil dans la console AWS Control Tower ou par programmation au moyen des API AWS Control Tower. L'état et l'état des comptes que vous avez provisionnés dans Account Factory sont également surveillés en permanence.

Afficher les actions enregistrées depuis la page Activités

Dans la console AWS Control Tower, la page Activités fournit une vue d'ensemble des actions du compte de gestion AWS Control Tower. Pour accéder à la page des activités d'AWS Control Tower, sélectionnez Activities dans le menu de navigation de gauche.

Les activités affichées sur la page Activités sont les mêmes que celles signalées dans le journal AWS CloudTrail des événements d'AWS Control Tower, mais elles sont présentées sous forme de tableau. Pour plus d'informations sur une activité spécifique, sélectionnez l'activité dans le tableau, puis choisissez View details (Afficher les détails).

Vous pouvez consulter les actions et les événements liés aux comptes des membres dans les fichiers d'archives du journal.

Les sections suivantes décrivent plus en détail la surveillance et la journalisation dans AWS Control Tower :

Rubriques

- Outils intégrés pour la surveillance
- Journalisation des actions d'AWS Control Tower avec AWS CloudTrail
- Événements liés au cycle de vie dans AWS Control Tower
- Utilisation des notifications AWS utilisateur avec AWS Control Tower

À propos de la connexion à AWS Control Tower

AWS Control Tower enregistre automatiquement les actions et les événements, grâce à son intégration avec AWS CloudTrail et AWS Config, et les CloudWatch enregistre. Toutes les actions sont enregistrées, y compris les actions depuis le compte de gestion AWS Control Tower et depuis les comptes des membres de votre organisation. Les actions et les événements du compte de gestion sont consultables sur la page Activités de la console. Vous pouvez consulter les actions et les événements liés aux comptes des membres dans les fichiers d'archives du journal.

Sentiers au niveau de l'organisation

AWS Control Tower définit un nouveau CloudTrail parcours lorsque vous configurez une zone d'atterrissage. Il s'agit d'un suivi au niveau de l'organisation, ce qui signifie qu'il enregistre tous les événements relatifs au compte de gestion et à tous les comptes des membres de l'organisation. Cette fonctionnalité repose sur un accès fiable pour autoriser le compte de gestion à créer une trace sur chaque compte membre.

Pour plus d'informations sur AWS Control Tower et les parcours d' CloudTrail organisation, consultez la section Création d'un parcours pour une organisation.

> **Note**
>
> Dans les versions d'AWS Control Tower antérieures à la version 3.0 de landing zone, AWS Control Tower créait un historique de compte de membre dans chaque compte. Lorsque vous effectuez une mise à jour vers la version 3.0, votre CloudTrail parcours devient un parcours d'organisation. Pour connaître les meilleures pratiques en matière de déplacement entre les sentiers, consultez la section Meilleures pratiques pour changer de sentier dans le guide de CloudTrail l'utilisateur.

Lorsque vous créez un compte dans AWS Control Tower, celui-ci est régi par le AWS CloudTrail parcours de l'organisation AWS Control Tower. Si vous avez déjà déployé un CloudTrail essai sur ce compte, des frais supplémentaires peuvent être facturés, sauf si vous supprimez le journal existant pour le compte avant de l'inscrire dans AWS Control Tower.

> **Note**
>
> Lorsque vous passez à la version 3.0 de landing zone, AWS Control Tower supprime les traces au niveau du compte (créées par AWS Control Tower) dans vos comptes inscrits en votre nom. Vos fichiers journaux existants au niveau du compte sont conservés dans leur compartiment Amazon S3.

Politique relative au compartiment Amazon S3 dans le compte d'audit

Dans AWS Control Tower, les AWS services ont accès à vos ressources uniquement lorsque la demande provient de votre organisation ou unité organisationnelle (UO). Une `aws:SourceOrgID` condition doit être remplie pour toute autorisation d'écriture.

Vous pouvez utiliser la clé de `aws:SourceOrgID` condition et définir la valeur en fonction de l'ID de votre organisation dans l'élément condition de votre politique de compartiment Amazon S3. Cette condition garantit que CloudTrail seuls les journaux peuvent être écrits pour le compte de comptes au sein de votre organisation dans votre compartiment S3 ; elle empêche CloudTrail les journaux extérieurs à votre organisation d'écrire dans votre compartiment AWS Control Tower S3.

Cette politique n'affecte pas la fonctionnalité de vos charges de travail existantes. La politique est illustrée dans l'exemple suivant.

```
S3AuditBucketPolicy:
    Type: AWS::S3::BucketPolicy
    Properties:
      Bucket: !Ref S3AuditBucket
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Sid: AllowSSLRequestsOnly
            Effect: Deny
            Principal: '*'
```

```
      Action: s3:*
      Resource:
       - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
       - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/*"
      Condition:
        Bool:
          aws:SecureTransport: false
    - Sid: AWSBucketPermissionsCheck
      Effect: Allow
      Principal:
        Service:
          - cloudtrail.amazonaws.com
          - config.amazonaws.com
      Action: s3:GetBucketAcl
      Resource:
        - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
    - Sid: AWSConfigBucketExistenceCheck
      Effect: Allow
      Principal:
        Service:
          - cloudtrail.amazonaws.com
          - config.amazonaws.com
      Action: s3:ListBucket
      Resource:
        - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
    - Sid: AWSBucketDeliveryForConfig
      Effect: Allow
      Principal:
        Service:
          - config.amazonaws.com
      Action: s3:PutObject
      Resource:
        - Fn::Join:
            - ""
            -
              - !Sub "arn:${AWS::Partition}:s3:::"
              - !Ref "S3AuditBucket"
              - !Sub "/${AWSLogsS3KeyPrefix}/AWSLogs/*/*"
      Condition:
        StringEquals:
          aws:SourceOrgID: !Ref OrganizationId
    - Sid: AWSBucketDeliveryForOrganizationTrail
      Effect: Allow
      Principal:
```

```
              Service:
                - cloudtrail.amazonaws.com
            Action: s3:PutObject
            Resource: !If [IsAccountLevelBucketPermissionRequiredForCloudTrail,
                [!Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
${AWSLogsS3KeyPrefix}/AWSLogs/${Namespace}/*", !Sub "arn:${AWS::Partition}:s3:::
${S3AuditBucket}/${AWSLogsS3KeyPrefix}/AWSLogs/${OrganizationId}/*"],
                !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
${AWSLogsS3KeyPrefix}/AWSLogs/*/*"]
            Condition:
              StringEquals:
            aws:SourceOrgID: !Ref OrganizationId
```

Pour plus d'informations sur cette clé de condition, consultez la documentation IAM et le billet de blog IAM intitulé « Utiliser des contrôles évolutifs pour les AWS services accédant à vos ressources ».

Outils intégrés pour la surveillance

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'AWS Control Tower et de vos autres AWS solutions. AWS fournit les outils de surveillance suivants pour surveiller AWS Control Tower, signaler un problème et prendre des mesures automatiques le cas échéant :

- Amazon CloudWatch surveille vos AWS ressources et les applications que vous utilisez AWS en temps réel. Vous pouvez collecter et suivre les métriques, créer des tableaux de bord personnalisés, et définir des alarmes qui vous informent ou prennent des mesures lorsqu'une métrique spécifique atteint un seuil que vous spécifiez. Par exemple, vous pouvez CloudWatch suivre l'utilisation du processeur ou d'autres indicateurs de vos instances Amazon EC2 et lancer automatiquement de nouvelles instances en cas de besoin. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.
- Amazon CloudWatch Events fournit un flux en temps quasi réel d'événements système décrivant les modifications apportées aux AWS ressources. CloudWatch Les événements permettent une informatique automatisée axée sur les événements, car vous pouvez rédiger des règles qui surveillent certains événements et déclenchent des actions automatisées dans d'autres AWS services lorsque ces événements se produisent. Pour plus d'informations, consultez le guide de l'utilisateur d'Amazon CloudWatch Events.
- Amazon CloudWatch Logs vous permet de surveiller, de stocker et d'accéder à vos fichiers journaux à partir d'instances Amazon EC2 et d'autres sources. CloudTrail CloudWatch Les journaux peuvent surveiller les informations contenues dans les fichiers journaux et vous avertir

lorsque certains seuils sont atteints. Vous pouvez également archiver vos données de journaux dans une solution de stockage hautement durable. Pour plus d'informations, consultez le guide de l'utilisateur d'Amazon CloudWatch Logs.

- AWS CloudTrailcapture les appels d'API et les événements associés effectués par ou pour le compte de votre AWS compte et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels.

Conseil : Vous pouvez consulter et interroger CloudTrail l'activité d'un compte via CloudWatch Logs and CloudWatch Logs Insights. Cette activité inclut les événements relatifs au cycle de vie d'AWS Control Tower. CloudWatchLes fonctionnalités des journaux vous permettent d'effectuer des requêtes plus granulaires et précises que ce que vous pourriez normalement faire avec. CloudTrail

Pour plus d'informations, voir Journalisation des actions d'AWS Control Tower avec AWS CloudTrail.

Journalisation des actions d'AWS Control Tower avec AWS CloudTrail

AWS Control Tower est intégré à AWS CloudTrailun service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans AWS Control Tower. CloudTrail capture les actions pour AWS Control Tower sous forme d'événements. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour AWS Control Tower.

Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande envoyée à AWS Control Tower, l'adresse IP à partir de laquelle la demande a été faite, l'auteur de la demande, la date à laquelle elle a été faite, ainsi que des informations supplémentaires.

Pour en savoir plus CloudTrail, notamment comment le configurer et l'activer, consultez le guide deAWS CloudTrail l'utilisateur.

Informations sur AWS Control Tower dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité événementielle prise en charge se produit dans AWS Control Tower, cette activité est enregistrée dans un CloudTrail

événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre AWS compte. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

> **Note**
>
> Dans les versions d'AWS Control Tower antérieures à la version 3.0 de landing zone, AWS Control Tower a créé un historique des comptes de membres. Lorsque vous passez à la version 3.0, votre journal CloudTrail est mis à jour pour devenir un journal d'organisation. Pour connaître les meilleures pratiques en matière de déplacement entre les sentiers, voir Création d'un parcours organisationnel dans le guide de CloudTrail l'utilisateur.

Recommandé : créer un parcours

Pour un enregistrement continu des événements de votre AWS compte, y compris les événements relatifs à AWS Control Tower, créez un historique. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions AWS . Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Présentation de la création d'un journal d'activité
- Préparez-vous à créer un sentier
- Gérer CloudTrail les coûts
- CloudTrail Services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

AWS Control Tower enregistre les actions suivantes sous forme d'événements dans des fichiers CloudTrail journaux :

API publiques

- DisableControl
- EnableControl
- GetControlOperation
- ListEnabledControls

Autres API

- SetupLandingZone
- UpdateAccountFactoryConfig
- ManageOrganizationalUnit
- CreateManagedAccount
- EnableGuardrail
- GetLandingZoneStatus
- GetHomeRegion
- ListManagedAccounts
- DescribeManagedAccount
- DescribeAccountFactoryConfig
- DescribeGuardrailForTarget
- DescribeManagedOrganizationalUnit
- ListEnabledGuardrails
- ListGuardrailViolations
- ListGuardrails
- ListGuardrailsForTarget
- ListManagedAccountsForGuardrail
- ListManagedAccountsForParent
- ListManagedOrganizationalUnits
- ListManagedOrganizationalUnitsForGuardrail
- GetGuardrailComplianceStatus
- DescribeGuardrail
- ListDirectoryGroups

- `DescribeSingleSignOn`
- `DescribeCoreService`
- `GetAvailableUpdates`

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.
- Si la demande a été rejetée parce que l'accès a été refusé ou si elle a été traitée avec succès.

Pour plus d'informations, consultez la section Élément userIdentity CloudTrail .

Exemple : entrées dans le fichier journal d'AWS Control Tower

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les événements n'apparaissent pas dans un ordre spécifique dans les fichiers journaux.

L'exemple suivant montre une entrée de CloudTrail journal qui montre la structure d'une entrée de fichier journal typique pour un événement `SetupLandingZone` AWS Control Tower, y compris un enregistrement de l'identité de l'utilisateur qui a initié l'action.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:backend-test-assume-role-session",
    "arn": "arn:aws:sts::76543EXAMPLE;:assumed-role/AWSControlTowerTestAdmin/backend-
test-assume-role-session",
    "accountId": "76543EXAMPLE",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-11-20T19:36:11Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::AKIAIOSFODNN7EXAMPLE:role/AWSControlTowerTestAdmin",
        "accountId": "AIDACKCEVSQ6C2EXAMPLE",
        "userName": "AWSControlTowerTestAdmin"
      }
    }
  },
  "eventTime": "2018-11-20T19:36:15Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "SetupLandingZone",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "Coral/Netty4",
  "errorCode": "InvalidParametersException",
  "errorMessage": "Home region EU_CENTRAL_1 is unsupported",
  "requestParameters": {
    "homeRegion": "EU_CENTRAL_1",
    "logAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "sharedServiceAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "securityAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "securityNotificationEmail": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "responseElements": null,
  "requestID": "96f47b68-ed5f-4268-931c-807cd1f89a96",
  "eventID": "4ef5cf08-39e5-4fdf-9ea2-b07ced506851",
  "eventType": "AwsApiCall",
  "recipientAccountId": "76543EXAMPLE"
}
```


Surveillez l'évolution des ressources avec AWS Config

AWS Control Tower active tous AWS Config les comptes inscrits, afin de pouvoir surveiller la conformité par le biais de contrôles de détection, d'enregistrer les modifications des ressources et de fournir les journaux des modifications des ressources au compte d'archivage des journaux.

Si la version de votre zone de landing zone est antérieure à la version 3.0 : pour vos comptes inscrits, AWS Config enregistre toutes les modifications apportées aux ressources, pour toutes les régions dans lesquelles le compte fonctionne. Chaque modification est modélisée sous la forme d'un élément de configuration (CI), qui contient des informations telles que l'identifiant de la ressource, la région, la date à laquelle chaque modification a été enregistrée et si la modification concerne une ressource connue ou une ressource récemment découverte.

Si la version de votre zone de landing zone est 3.0 ou ultérieure : AWS Control Tower limite l'enregistrement des ressources globales, telles que les utilisateurs, les groupes, les rôles et les politiques gérées par le client IAM, à votre région d'origine uniquement. Les copies des modifications des ressources globales ne sont pas stockées dans toutes les régions. Cette limitation de l'enregistrement des ressources est conforme aux AWS Config meilleures pratiques. Une liste complète des ressources mondiales est disponible dans AWS Config la documentation.

- Pour en savoir plus AWS Config, consultez la section AWS Config Fonctionnement.
- Pour obtenir la liste des ressources AWS Config pouvant être prises en charge, consultez la section Types de ressources pris en charge.
- Pour savoir comment personnaliser le suivi des ressources dans l'environnement AWS Control Tower, consultez le billet de blog intitulé Personnaliser le suivi AWS Config des ressources dans AWS Control Tower.

AWS Control Tower met en place un canal AWS Config de diffusion pour tous les comptes inscrits. Ce canal de diffusion enregistre toutes les modifications enregistrées par AWS Config le compte d'archivage des journaux, où elles sont stockées dans un dossier d'un bucket Amazon Simple Storage Service.

Gérez AWS Config les coûts dans AWS Control Tower

Cette section décrit comment AWS Config enregistrer et facturer les modifications apportées aux ressources de vos comptes AWS Control Tower. Ces informations peuvent vous aider à comprendre comment gérer les coûts associés AWS Configà l'utilisation d'AWS Control Tower lorsque vous utilisez AWS Control Tower. AWS Control Tower n'entraîne aucun coût supplémentaire.

> **Note**
>
> Si la version de votre zone de landing zone est 3.0 ou ultérieure : AWS Control Tower limite AWS Config l'enregistrement des ressources globales, telles que les utilisateurs, les groupes,

les rôles et les politiques gérées par le client IAM, à votre région d'origine uniquement. Par conséquent, certaines informations de cette section peuvent ne pas s'appliquer à votre zone d'atterrissage.

AWS Config est conçu pour enregistrer chaque modification apportée à chaque ressource, dans chaque région où un compte fonctionne, en tant qu'élément de configuration (CI). AWS Config vous facture chaque élément de configuration généré.

Comment AWS Config fonctionne

AWS Config enregistre les ressources dans chaque région, séparément. Certaines ressources mondiales, telles que les rôles IAM, sont enregistrées une fois par région. Par exemple, si vous créez un nouveau rôle IAM dans un compte inscrit qui fonctionne dans cinq régions, cela AWS Config génère cinq CI, un pour chaque région. Les autres ressources mondiales, telles que les zones hébergées par Route 53, ne sont enregistrées qu'une seule fois dans toutes les régions. Par exemple, si vous créez une nouvelle zone hébergée Route 53 dans un compte inscrit, cela AWS Config génère un CI, quel que soit le nombre de régions sélectionnées pour ce compte. Pour obtenir une liste qui vous aide à distinguer ces types de ressources, consultezLa même ressource est enregistrée plusieurs fois.

Note

Lorsqu'AWS Control Tower fonctionne avec AWS Config, une région peut être gouvernée par AWS Control Tower, ou non gouvernée, et enregistre AWS Config toujours les modifications si le compte fonctionne dans cette région.

AWS Config détecte deux types de relations dans les ressources

AWS Config fait une distinction entre les relations directes et indirectes entre les ressources. Si une ressource est renvoyée lors de l'appel d'API Describe d'une autre ressource, ces ressources sont enregistrées en tant que relation directe. Lorsque vous modifiez une ressource dans une relation directe avec une autre ressource, AWS Config cela ne crée pas de CI pour les deux ressources.

Par exemple, si vous créez une instance Amazon EC2 et que l'API vous oblige à créer une interface réseau, AWS Config considérez que l'instance Amazon EC2 a une relation directe avec l'interface réseau. Par conséquent, ne AWS Config génère qu'un seul CI.

AWS Config enregistre les modifications distinctes pour les relations de ressources qui sont des relations indirectes. Par exemple, AWS Config génère deux CI si vous créez un groupe de sécurité et ajoutez une instance Amazon EC2 associée faisant partie du groupe de sécurité.

Pour plus d'informations sur les relations directes et indirectes, voir Qu'est-ce qu'une relation directe et indirecte par rapport à une ressource ?

Vous trouverez une liste des relations entre les ressources dans la AWS Config documentation.

Afficher les données de l' AWS Config enregistreur sur les comptes inscrits

AWS Config est intégré CloudWatch afin que vous puissiez afficher les AWS Config CI dans un tableau de bord. Pour plus d'informations, consultez le billet de blog intitulé AWS Config Supports Amazon CloudWatch metrics.

Par programmation, pour afficher les AWS Config données, vous pouvez utiliser la AWS CLI ou utiliser d'autres AWS outils.

Interrogez les données de l' AWS Config enregistreur sur une ressource spécifique

Vous pouvez utiliser la AWS CLI pour récupérer la liste des modifications les plus récentes apportées à une ressource.

Commande d'historique des ressources :

- `aws configservice get-resource-config-history --resource-type RESOURCE-TYPE --resource-id RESOURCE-ID --region REGION`

Pour en savoir plus, consultez la documentation de l'API pour `get-config-history`.

Visualisez AWS Config les données avec Amazon QuickSight

Vous pouvez visualiser et interroger les ressources enregistrées par AWS Config l'ensemble de votre organisation. Pour plus d'informations, consultez Visualisation des AWS Config données à l'aide d'Amazon Athena et Amazon. QuickSight

Résolution des problèmes AWS Config dans AWS Control Tower

Cette section fournit des informations sur certains problèmes que vous pouvez rencontrer lors de l'utilisation AWS Config d'AWS Control Tower.

AWS Config Coûts élevés

Si votre flux de travail inclut des processus qui créent, mettent à jour ou suppriment fréquemment des ressources, ou s'il gère un grand nombre de ressources, ce flux de travail peut générer un grand nombre de CI. Si vous exécutez ces processus dans un compte hors production, pensez à désinscrire le compte. Vous devrez peut-être désactiver manuellement l' AWS Config enregistreur de ce compte.

> **Note**
>
> Une fois le compte désinscrit, AWS Control Tower ne peut pas appliquer de contrôles de détection ni enregistrer les événements du compte, tels que les AWS Config activités, pour les ressources de ce compte.

Pour plus d'informations, voir Annuler la gestion d'un compte inscrit. Pour savoir comment désactiver l' AWS Config enregistreur, voir Gestion de l'enregistreur de configuration.

La même ressource est enregistrée plusieurs fois

Vérifiez si la ressource est une ressource globale. Pour les zones d'atterrissage d'AWS Control Tower antérieures à la version 3.0, certaines ressources globales AWS Config peuvent être enregistrées une fois pour chaque région dans laquelle AWS Config elle opère. Par exemple, s'il AWS Config est activé dans huit régions, chaque rôle est enregistré huit fois.

Les ressources suivantes sont enregistrées une fois pour chaque région dans laquelle AWS Config elle opère :

- `AWS::IAM::Group`
- `AWS::IAM::Policy`
- `AWS::IAM::Role`
- `AWS::IAM::User`

Les autres ressources globales ne sont enregistrées qu'une seule fois. Voici quelques exemples de ressources enregistrées une seule fois :

- `AWS::Route53::HostedZone`

- `AWS::Route53::HealthCheck`
- `AWS::ECR::PublicRepository`
- `AWS::GlobalAccelerator::Listener`
- `AWS::GlobalAccelerator::EndpointGroup`
- `AWS::GlobalAccelerator::Accelerator`

AWS Config n'a pas enregistré de ressource

Certaines ressources ont des relations de dépendance avec d'autres ressources. Ces relations peuvent être directes ou indirectes. Vous trouverez une liste des relations indirectes déconseillées dans la AWS Config FAQ.

Événements liés au cycle de vie dans AWS Control Tower

Certains événements enregistrés par AWS Control Tower sont des événements du cycle de vie. L'objectif d'un événement du cycle de vie est de marquer l'achèvement de certaines actions AWS Control Tower qui modifient l'état des ressources. Les événements du cycle de vie s'appliquent aux ressources créées ou gérées par AWS Control Tower, telles que les unités organisationnelles (UO), les comptes et les contrôles.

Caractéristiques des événements liés au cycle de vie d'AWS Control Tower

- Pour chaque événement du cycle de vie, le journal des événements indique si l'action Control Tower d'origine s'est terminée avec succès ou a échoué.
- AWS CloudTrail enregistre automatiquement chaque événement du cycle de vie en tant qu'événement de AWS service non lié à l'API. Pour plus d'informations, consultez le guide de AWS CloudTrail l'utilisateur.
- Chaque événement du cycle de vie est également transmis aux services Amazon EventBridge et Amazon CloudWatch Events.

Les événements du cycle de vie dans AWS Control Tower offrent deux avantages principaux :

- Étant donné qu'un événement du cycle de vie enregistre la fin d'une action AWS Control Tower, vous pouvez créer une EventBridge règle Amazon ou une règle Amazon CloudWatch Events qui peut déclencher les étapes suivantes de votre flux de travail d'automatisation, en fonction de l'état de l'événement du cycle de vie.

- Les journaux fournissent des détails supplémentaires pour aider les administrateurs et les auditeurs à examiner certains types d'activités dans vos organisations.

Fonctionnement des événements de cycle de vie

AWS Control Tower s'appuie sur plusieurs services pour mettre en œuvre ses actions. Par conséquent, chaque événement de cycle de vie est enregistré une fois qu'une série d'actions est terminée. Par exemple, lorsque vous activez un contrôle sur une unité d'organisation, AWS Control Tower lance une série de sous-étapes qui mettent en œuvre la demande. Le résultat final de l'ensemble de la série de sous-étapes est enregistré dans le journal comme état de l'événement de cycle de vie.

- Si chaque sous-étape sous-jacente a abouti, l'état de l'événement de cycle de vie est enregistré comme Succeeded (Réussite).
- Si l'une des sous-étapes sous-jacentes n'a pas abouti, l'état de l'événement de cycle de vie est enregistré comme Failed (Échec).

Chaque événement du cycle de vie inclut un horodatage enregistré qui indique le moment où l'action AWS Control Tower a été lancée, et un autre horodatage indiquant la fin de l'événement du cycle de vie, marquant le succès ou l'échec.

Afficher les événements du cycle de vie dans Control Tower

Vous pouvez consulter les événements du cycle de vie sur la page Activités de votre tableau de bord AWS Control Tower.

- Pour accéder à la page Activities (Activités), choisissez Activities (Activités) dans le panneau de navigation de gauche.
- Pour obtenir de plus amples informations sur un événement spécifique, sélectionnez l'événement, puis cliquez sur le bouton View details (Afficher les détails) en haut à droite.

Pour plus d'informations sur la manière d'intégrer les événements du cycle de vie d'AWS Control Tower dans vos flux de travail, consultez ce billet de blog intitulé Utiliser les événements du cycle de vie pour suivre les actions d'AWS Control Tower et déclencher des flux de travail automatisés.

Comportement attendu CreateManagedAccount et événements UpdateManagedAccount du cycle de vie

Lorsque vous créez un compte ou que vous inscrivez un compte dans AWS Control Tower, ces deux actions appellent la même API interne. Si une erreur se produit au cours du processus, elle se produit généralement après la création du compte, mais il n'est pas entièrement provisionné. Lorsque vous essayez à nouveau de créer le compte après l'erreur, ou lorsque vous essayez de mettre à jour le produit mis en service, AWS Control Tower constate que le compte existe déjà.

Comme le compte existe, AWS Control Tower enregistre l'événement du `UpdateManagedAccount` cycle de vie plutôt que l'événement du `CreateManagedAccount` cycle de vie à la fin de la demande de nouvelle tentative. Vous vous attendiez peut-être à un autre `CreateManagedAccount` événement à cause de cette erreur. Cependant, l'événement `UpdateManagedAccount` du cycle de vie correspond au comportement attendu et souhaité.

Si vous envisagez de créer ou d'inscrire des comptes dans AWS Control Tower à l'aide de méthodes automatisées, programmez la fonction Lambda UpdateManagedAccountpour rechercher les événements du cycle de vie CreateManagedAccountainsi que les événements du cycle de vie.

Noms de l'événement de cycle de vie

Chaque événement du cycle de vie est nommé de manière à correspondre à l'action AWS Control Tower d'origine, qui est également enregistrée par AWS CloudTrail. Ainsi, par exemple, un événement du cycle de vie créé par l'`CreateManagedAccount` CloudTrail événement AWS Control Tower est nomm`CreateManagedAccount`é.

Chaque nom de la liste qui suit constitue un lien vers un exemple de détail consigné au format `JSON`. Les informations supplémentaires présentées dans ces exemples sont extraites des journaux d' CloudWatch événements Amazon.

Bien que `JSON` ne prenne pas en charge les commentaires, certains commentaires ont été ajoutés dans les exemples à des fins explicatives. Les commentaires sont précédés de « // » et apparaissent à droite des exemples.

Dans ces exemples, certains noms de comptes et d'organisations sont masqués. Un `accountId` est toujours une séquence de 12 chiffres, qui a été remplacée par « xxxxxxxxxxxx » dans les exemples. Un `organizationalUnitID` est une chaîne unique de lettres et de chiffres. Sa forme est préservée dans les exemples.

- `CreateManagedAccount`: Le journal indique si AWS Control Tower a effectué avec succès toutes les actions nécessaires pour créer et approvisionner un nouveau compte à l'aide de Account Factory.

- `UpdateManagedAccount`: Le journal indique si AWS Control Tower a effectué avec succès toutes les actions de mise à jour d'un produit provisionné associé à un compte que vous aviez créé précédemment à l'aide de Account Factory.
- `EnableGuardrail`: Le journal indique si AWS Control Tower a effectué avec succès toutes les actions nécessaires pour activer un contrôle sur une unité d'organisation créée par AWS Control Tower.
- `DisableGuardrail`: Le journal indique si AWS Control Tower a effectué avec succès toutes les actions visant à désactiver un contrôle sur une unité d'organisation créée par AWS Control Tower.
- `SetupLandingZone`: Le journal indique si AWS Control Tower a effectué avec succès toutes les actions nécessaires pour configurer une zone de landing zone.
- `UpdateLandingZone`: Le journal indique si AWS Control Tower a effectué avec succès toutes les actions nécessaires pour mettre à jour votre zone de landing zone existante.
- `RegisterOrganizationalUnit`: Le journal indique si AWS Control Tower a effectué avec succès toutes les actions nécessaires pour activer ses fonctionnalités de gouvernance sur une unité d'organisation.
- `DeregisterOrganizationalUnit`: Le journal indique si AWS Control Tower a effectué avec succès toutes les actions visant à désactiver ses fonctionnalités de gouvernance sur une unité d'organisation.
- `PrecheckOrganizationalUnit`: Le journal indique si AWS Control Tower a détecté une ressource susceptible d'empêcher le bon déroulement de l'opération de gouvernance Extend.

Les sections suivantes fournissent une liste des événements du cycle de vie d'AWS Control Tower, avec des exemples des détails enregistrés pour chaque type d'événement du cycle de vie.

`CreateManagedAccount`

Cet événement du cycle de vie indique si AWS Control Tower a correctement créé et provisionné un nouveau compte à l'aide de Account Factory. Cet événement correspond à l'`CreateManagedAccount` CloudTrail événement AWS Control Tower. Le journal des événements de cycle de vie inclut les éléments `accountName` et `accountId` du compte nouvellement créé, ainsi que les éléments `organizationalUnitName` et `organizationalUnitId` de l'unité d'organisation dans laquelle le compte a été placé.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
```

```
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                    // Management account
 ID.
    "time": "2018-08-30T21:42:18Z",                               // Format: yyyy-MM-
dd'T'hh:mm:ssZ
    "region": "us-east-1",                                        // AWS Control Tower
 home region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                      // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "CreateManagedAccount",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "createManagedAccountStatus": {
                "organizationalUnit":{
                    "organizationalUnitName":"Custom",
                    "organizationalUnitId":"ou-XXXX-l3zc8b3h"

                    },
                "account":{
                    "accountName":"LifeCycle1",
                    "accountId":"XXXXXXXXXXXX"
                    },
                "state":"SUCCEEDED",
                "message":"AWS Control Tower successfully created a managed account.",
                "requestedTimestamp":"2019-11-15T11:45:18+0000",
                "completedTimestamp":"2019-11-16T12:09:32+0000"}
        }
    }
}
```

UpdateManagedAccount

Cet événement du cycle de vie enregistre si AWS Control Tower a correctement mis à jour le produit provisionné associé à un compte créé précédemment à l'aide de Account Factory. Cet événement correspond à l'`UpdateManagedAccount` CloudTrailévénement AWS Control Tower. Le journal des événements de cycle de vie inclut les éléments `accountName` et `accountId` du compte associé, ainsi que les éléments `organizationalUnitName` et `organizationalUnitId` de l'unité d'organisation dans laquelle le compte mis à jour est placé.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                    // AWS Control Tower
 organization management account.
    "time": "2018-08-30T21:42:18Z",                               // Format: yyyy-MM-
dd'T'hh:mm:ssZ
    "region": "us-east-1",                                        // AWS Control Tower
 home region.
    "resources": [],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                      // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "UpdateManagedAccount",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "updateManagedAccountStatus": {
                "organizationalUnit":{
                    "organizationalUnitName":"Custom",
                    "organizationalUnitId":"ou-XXXX-l3zc8b3h"
```

```
                    },
                "account":{
                    "accountName":"LifeCycle1",
                    "accountId":"624281831893"
                    },
                "state":"SUCCEEDED",
                "message":"AWS Control Tower successfully updated a managed account.",
                "requestedTimestamp":"2019-11-15T11:45:18+0000",
                "completedTimestamp":"2019-11-16T12:09:32+0000"}
        }
    }
}
```

EnableGuardrail

Cet événement du cycle de vie enregistre si AWS Control Tower a activé avec succès un contrôle sur une unité d'organisation gérée par AWS Control Tower. Cet événement correspond à l'`EnableGuardrail` CloudTrail événement AWS Control Tower. Le journal des événements du cycle de vie inclut le `guardrailId` et `guardrailBehavior` du contrôle, ainsi que le `organizationalUnitName` et `organizationalUnitId` de l'unité d'organisation sur laquelle le contrôle est activé.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",                                  // End-time of action.
 Format: yyyy-MM-dd'T'hh:mm:ssZ
    "region": "us-east-1",                                           // AWS Control Tower
 home region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "EnableGuardrail",
```

```
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "enableGuardrailStatus": {
                "organizationalUnits": [
                    {
                      "organizationalUnitName": "Custom",
                      "organizationalUnitId": "ou-vwxy-18vy4yro"
                    }
                  ],
                  "guardrails": [
                    {
                      "guardrailId": "AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK",
                      "guardrailBehavior": "DETECTIVE"
                    }
                  ],
                  "state": "SUCCEEDED",
                  "message": "AWS Control Tower successfully enabled a guardrail on an
 organizational unit.",
                  "requestTimestamp": "2019-11-12T09:01:07+0000",
                  "completedTimestamp": "2019-11-12T09:01:54+0000"
                }
        }
    }
}
```

DisableGuardrail

Cet événement du cycle de vie enregistre si AWS Control Tower a correctement désactivé un contrôle sur une unité d'organisation gérée par AWS Control Tower. Cet événement correspond à l'`DisableGuardrail` CloudTrail événement AWS Control Tower. Le journal des événements du cycle `guardrailBehavior` de vie inclut le `guardrailId` et du contrôle et le `organizationalUnitName` et `organizationalUnitId` de l'unité d'organisation sur laquelle le contrôle est désactivé.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
```

```
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "DisableGuardrail",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "disableGuardrailStatus": {
                   "organizationalUnits": [
                    {
                      "organizationalUnitName": "Custom",
                      "organizationalUnitId": "ou-vwxy-18vy4yro"
                    }
                  ],
                  "guardrails": [
                    {
                      "guardrailId": "AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK",
                      "guardrailBehavior": "DETECTIVE"
                    }
                  ],
                  "state": "SUCCEEDED",
                  "message": "AWS Control Tower successfully disabled a guardrail on an
 organizational unit.",
                  "requestTimestamp": "2019-11-12T09:01:07+0000",
                  "completedTimestamp": "2019-11-12T09:01:54+0000"
                }
            }
        }
```

```
    }
```

SetupLandingZone

Cet événement du cycle de vie enregistre si AWS Control Tower a correctement configuré une zone de landing zone. Cet événement correspond à l'`SetupLandingZone` CloudTrail événement AWS Control Tower. Le journal des événements du cycle de vie inclut le`rootOrganizationalId`, qui est l'ID de l'organisation créée par AWS Control Tower à partir du compte de gestion. L'entrée du journal inclut également le `organizationalUnitName` et `organizationalUnitId` pour chacune des UO, ainsi que le `accountName` et `accountId` pour chaque compte, créés lorsque AWS Control Tower configure la zone de landing zone.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",                // Request ID.
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                  // Management account
 ID.
    "time": "2018-08-30T21:42:18Z",                             // Event time from
 CloudTrail.
    "region": "us-east-1",                                      // Management account
 CloudTrail region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",                        // Management-account
 ID.
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                    // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "SetupLandingZone",
        "awsRegion": "us-east-1",                               // AWS Control Tower
 home region.
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "CloudTrail_event_ID",                       // This value is
 generated by CloudTrail.
        "readOnly": false,
```

```
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "setupLandingZoneStatus": {
                "state": "SUCCEEDED",                                // Status of entire
 lifecycle operation.
                "message": "AWS Control Tower successfully set up a new landing zone.",

                "rootOrganizationalId" : "r-1234",
                "organizationalUnits" : [                            // Use a list.
                  {
                    "organizationalUnitName": "Security",             // Security OU
 name.
                    "organizationalUnitId": "ou-adpf-302pk332"    // Security OU ID.
                  },
                  {
                    "organizationalUnitName": "Custom",           // Custom OU name.
                    "organizationalUnitId": "ou-adpf-302pk332"    // Custom OU ID.
                  },
                ],
               "accounts": [                                         // All created
 accounts are here. Use a list of "account" objects.

                  {
                    "accountName": "Audit",
                    "accountId": "XXXXXXXXXXXX"
                  },
                  {
                    "accountName": "Log archive",
                    "accountId": "XXXXXXXXXXXX"
                  }
              ],
              "requestedTimestamp": "2018-08-30T21:42:18Z",
              "completedTimestamp": "2018-08-30T21:42:18Z"
            }
        }
    }
}
```

UpdateLandingZone

Cet événement du cycle de vie enregistre si AWS Control Tower a correctement mis à jour votre zone de landing zone existante. Cet événement correspond à l'`UpdateLandingZone` CloudTrail événement AWS Control Tower. Le journal des événements du cycle de vie inclut

le`rootOrganizationalId`, qui est l'ID de l'organisation (mise à jour) régie par AWS Control Tower. L'entrée du journal inclut également le `organizationalUnitName` et `organizationalUnitId` pour chacune des UO, ainsi que le `accountName` et `accountId` pour chaque compte, créé précédemment, lorsque AWS Control Tower a initialement configuré la zone de landing zone.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",                // Request ID.
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                   // Management account
 ID.
    "time": "2018-08-30T21:42:18Z",                              // Event time from
 CloudTrail.
    "region": "us-east-1",                                       // Management account
 CloudTrail region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",                         // Management account
 ID.
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                     // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "UpdateLandingZone",
        "awsRegion": "us-east-1",                                // AWS Control Tower
 home region.
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "CloudTrail_event_ID",                        // This value is
 generated by CloudTrail.

        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "updateLandingZoneStatus": {
                "state": "SUCCEEDED",                            // Status of entire
 operation.
                "message": "AWS Control Tower successfully updated a landing zone.",
```

```
                "rootOrganizationalId" : "r-1234",
                "organizationalUnits" : [                          // Use a list.
                  {
                    "organizationalUnitName": "Security",             // Security OU
 name.
                    "organizationalUnitId": "ou-adpf-302pk332"    // Security OU ID.
                  },
                  {
                    "organizationalUnitName": "Custom",            // Custom OU name.
                    "organizationalUnitId": "ou-adpf-302pk332"     // Custom OU ID.
                  },
                ],
               "accounts": [                                        // All created
 accounts are here. Use a list of "account" objects.

                  {
                    "accountName": "Audit",
                    "accountId": "XXXXXXXXXXXX"
                  },
                  {
                    "accountName": "Log archive",
                    "accountId": "XXXXXXXXXX"
                  }
              ],
              "requestedTimestamp": "2018-08-30T21:42:18Z",
              "completedTimestamp": "2018-08-30T21:42:18Z"
            }
        }
    }
}
```

RegisterOrganizationalUnit

Cet événement du cycle de vie indique si AWS Control Tower a activé avec succès ses fonctionnalités de gouvernance sur une unité d'organisation. Cet événement correspond à l'`RegisterOrganizationalUnit` CloudTrail événement AWS Control Tower. Le journal des événements du cycle de vie inclut le `organizationalUnitName` et `organizationalUnitId` de l'unité d'organisation qu'AWS Control Tower a placée sous sa gouvernance.

```
{
    "version": "0",
```

```
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "123456789012",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "RegisterOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "registerOrganizationalUnitStatus": {
                "state": "SUCCEEDED",

                "message": "AWS Control Tower successfully registered an organizational
 unit.",

                "organizationalUnit" :
                  {
                    "organizationalUnitName": "Test",
                    "organizationalUnitId": "ou-adpf-302pk332"
                  }
                "requestedTimestamp": "2018-08-30T21:42:18Z",
                "completedTimestamp": "2018-08-30T21:42:18Z"
            }
        }
    }
}
```

DeregisterOrganizationalUnit

Cet événement du cycle de vie indique si AWS Control Tower a correctement désactivé ses fonctionnalités de gouvernance sur une unité d'organisation. Cet événement correspond à l'`DeregisterOrganizationalUnit` CloudTrail événement AWS Control Tower. Le journal des événements du cycle de vie inclut le `organizationalUnitName` et `organizationalUnitId` de l'unité d'organisation sur laquelle AWS Control Tower a désactivé ses fonctionnalités de gouvernance.


```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "DeregisterOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "deregisterOrganizationalUnitStatus": {
                "state": "SUCCEEDED",
                "message": "AWS Control Tower successfully deregistered an
 organizational unit, and enabled mandatory guardrails on the new organizational
 unit.",
                "organizationalUnit" :
                  {
```

```
                    "organizationalUnitName": "Test",                   // Foundational
 OU name.
                    "organizationalUnitId": "ou-adpf-302pk332"          // Foundational
 OU ID.
                  },
                "requestedTimestamp": "2018-08-30T21:42:18Z",
                "completedTimestamp": "2018-08-30T21:42:18Z"
            }
            }
        }
    }
```

PrecheckOrganizationalUnit

Cet événement du cycle de vie enregistre si AWS Control Tower a correctement effectué les prévérifications sur une unité d'organisation. Cet événement correspond à l'`PrecheckOrganizationalUnit` CloudTrail événement AWS Control Tower. Le journal des événements du cycle de vie contient un champ pour les `IdName`, et `failedPrechecks` les valeurs pour chaque ressource sur laquelle AWS Control Tower a effectué des prévérifications lors du processus d'enregistrement de l'unité d'organisation.

Le journal des événements contient également des informations sur les comptes imbriqués sur lesquels les prévérifications ont été effectuées, notamment les `accountName` champs`accountId`, et`failedPrechecks`.

Si la `failedPrechecks` valeur est vide, cela signifie que tous les précontrôles pour cette ressource ont été effectués avec succès.

- Cet événement n'est émis qu'en cas d'échec de la prévérification.
- Cet événement n'est pas émis si vous enregistrez une unité d'organisation vide.

Exemple d'événement :

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "XXXXXXXXXXXX",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2021-09-20T22:45:43Z",
  "eventSource": "controltower.amazonaws.com",
```

```
  "eventName": "PrecheckOrganizationalUnit",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "eventID": "b41a9d67-0da4-4dc5-a87a-25fa19dc5305",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "XXXXXXXXXXXX",
  "serviceEventDetails": {
    "precheckOrganizationalUnitStatus": {
      "organizationalUnit": {
        "organizationalUnitName": "Ou-123",
        "organizationalUnitId": "ou-abcd-123456",
        "failedPrechecks": [
            "SCP_CONFLICT"
          ]
      },
      "accounts": [
        {
          "accountName": "Child Account 1",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": [
            "FAILED_TO_ASSUME_ROLE"
          ]
        },
        {
          "accountName": "Child Account 2",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": [
            "FAILED_TO_ASSUME_ROLE"
          ]
        },
        {
          "accountName": "Management Account",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": [
            "MISSING_PERMISSIONS_AF_PRODUCT"
          ]
        },
        {
          "accountName": "Child Account 3",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": []
```

```
        },
        ...
      ],
      "state": "FAILED",
      "message": "AWS Control Tower failed to register an organizational unit due to
 pre-check failures. Go to the OU details page to download a list of failed pre-checks
 for the OU and accounts within.",
      "requestedTimestamp": "2021-09-20T22:44:02+0000",
      "completedTimestamp": "2021-09-20T22:45:43+0000"
    }
  },
  "eventCategory": "Management"
}
```

Utilisation des notifications AWS utilisateur avec AWS Control Tower

Vous pouvez utiliser les notifications auxAWS utilisateurs pour configurer les canaux de diffusion afin d'être informé AWS Control Tower des événements. Vous recevez une notification lorsqu'un événement correspond à une règle que vous avez spécifiée. Vous pouvez recevoir des notifications relatives à des événements par le biais de plusieurs canaux, notamment par e-mail, par AWS Chatbotchat ou par notification push via l'application mobile pourAWS console. Vous pouvez également consulter les notifications dans le Centre de notifications de la console.

AWS Les notifications utilisateur prennent en charge l'agrégation, ce qui peut réduire le nombre de notifications que vous recevez lors d'événements spécifiques. Les notifications sont également visibles dans le centre de notifications de la console.

Les avantages de l'abonnement aux notifications par le biais des notifications AWS utilisateur EventBridge sont les suivants :

- Une interface utilisateur (UI) plus conviviale.
- Intégration à la AWS console, dans la zone cloche/notifications de la barre de navigation globale.
- Support natif pour les notifications par e-mail, il n'est pas nécessaire de configurer Amazon SNS.
- Plus particulièrement, la prise en charge des notifications push mobiles, exclusive aux notifications AWS utilisateur.

Par exemple, vous souhaiterez peut-être recevoir un type de notification en cas de résultats critiques et très graves pour Security Hub. Un extrait de code au format JSON pour configurer cet abonnement aux notifications peut ressembler à ceci :

```
{
  "detail": {
    "findings": {
      "Compliance": {
        "Status": ["FAILED", "WARNING", "NOT_AVAILABLE"]
      },
      "RecordState": ["ACTIVE"],
      "Severity": {
        "Label": ["CRITICAL", "HIGH"]
      },
      "Workflow": {
        "Status": ["NEW", "NOTIFIED"]
      }
    }
  }
}
```

Filtrage des événements

- Vous pouvez filtrer les événements par service et par nom à l'aide des filtres disponibles sur la console des notifications AWS utilisateur.
- Vous pouvez filtrer les événements en fonction de propriétés spécifiques si vous créez votre propre EventBridge filtre à partir du code JSON.

Exemple d' AWS Control Tower événement

Voici un exemple d'événement généralisé pour AWS Control Tower.

- C'est un EventBridge événement.
- Vous pouvez vous abonner à EventBridge des événements (tels que celui-ci) à l'aide des notifications AWS utilisateur.

```
{
    "version": "0",
    "id": "<id>", // alphanumeric string
```

```
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "<account ID>", // Management account ID.
    "time": "<date>", // Format: yyyy-MM-dd'T'hh:mm:ssZ
    "region": "<region>", // AWS Control Tower home region.
    "resources": [],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "121212121212",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z", // Timestamp when call was made. Format:
 yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "<event name>", // one of the 9 event names in https://
docs.aws.amazon.com/controltower/latest/userguide/lifecycle-events.html
        "awsRegion": "<region>",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "<id>",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            // the contents of this object vary depending on the event subtype and
 event state
        }
    }
}
```

Procédures

Ce chapitre contient des procédures pas à pas qui peuvent vous aider à utiliser AWS Control Tower.

Rubriques

Procédure pas à pas : passer d'ALZ à AWS Control Tower

De nombreux AWS clients ont adopté la solution AWS Landing Zone (ALZ) pour mettre en place un environnement multi-comptes AWS sécurisé et conforme. Pour réduire la charge de travail liée à la gestion d'une zone d'atterrissage, nous avons AWS créé le service géré appelé AWS Control Tower.

Aucune fonctionnalité supplémentaire n'est prévue pour ALZ ; le support à long terme est uniquement disponible. Par conséquent, nous vous recommandons de passer au service AWS Control Tower depuis ALZ. Le blog dont le lien figure dans ce chapitre vous présente les différentes considérations relatives à cette migration et explique comment planifier une migration réussie d'ALZ vers AWS Control Tower.

Blog : Migrer la solution AWS Landing Zone vers AWS Control Tower

AWS Prescriptive Guidance propose une documentation plus complète, y compris les étapes de transition d'ALZ vers AWS Control Tower. Essentiellement, vous allez activer la gouvernance d'AWS Control Tower dans votre organisation existante qui exécute ALZ, en fonction d'un certain nombre de prérequis. Pour plus d'informations, consultez Transitioning from AWS Landing Zone vers AWS Control Tower.

Procédure pas à pas : Automatisez le provisionnement des comptes dans AWS Control Tower par les API Service Catalog

AWS Control Tower est intégré à plusieurs autres AWS services, tels que AWS Service Catalog. Vous pouvez utiliser les API pour créer et approvisionner vos comptes membres dans AWS Control Tower.

La vidéo vous montre comment approvisionner des comptes de manière automatisée et par lots, en appelant les AWS Service Catalog API. Pour le provisionnement, vous appellerez l'`ProvisionProduct`API depuis l'interface de ligne de AWS commande (CLI) et vous spécifierez un fichier JSON contenant les paramètres de chaque compte que vous souhaitez configurer. La vidéo illustre l'installation et l'utilisation de l'environnement de développement AWS Cloud9 pour effectuer ce travail. Les commandes CLI seront les mêmes si vous utilisez AWS Cloudshell au lieu de AWS Cloud9.

> **Note**
>
> Vous pouvez également adapter cette approche pour automatiser les mises à jour des comptes, en appelant l'`UpdateProvisionedProduct`API de AWS Service Catalog pour chaque compte. Vous pouvez écrire un script pour mettre à jour les comptes, un par un.

En tant que méthode d'automatisation complètement différente, si vous connaissez Terraform, vous pouvez provisionner des comptes avec AWS Control Tower Account Factory for Terraform (AFT).

Exemple de rôle d'administration de l'automatisation

Voici un exemple de modèle que vous pouvez utiliser pour configurer votre rôle d'administration d'automatisation dans le compte de gestion. Vous devez configurer ce rôle dans votre compte de gestion afin qu'il puisse effectuer l'automatisation avec un accès administrateur sur les comptes cibles.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure the SampleAutoAdminRole

Resources:
  AdministrationRole:
    Type: AWS::IAM::Role
```

```
    Properties:
      RoleName: SampleAutoAdminRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: cloudformation.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
      Policies:
        - PolicyName: AssumeSampleAutoAdminRole
          PolicyDocument:
            Version: 2012-10-17
            Statement:
              - Effect: Allow
                Action:
                  - sts:AssumeRole
                Resource:
                  - "arn:aws:iam::*:role/SampleAutomationExecutionRole"
```

Exemple de rôle d'exécution de l'automatisation

Voici un exemple de modèle que vous pouvez utiliser pour configurer votre rôle d'exécution d'automatisation. Vous devez configurer ce rôle dans les comptes cibles.

```
AWSTemplateFormatVersion: "2010-09-09"
Description: "Create automation execution role for creating Sample Additional Role."

Parameters:
  AdminAccountId:
    Type: "String"
    Description: "Account ID for the administrator account (typically management,
 security or shared services)."
  AdminRoleName:
    Type: "String"
    Description: "Role name for automation administrator access."
    Default: "SampleAutomationAdministrationRole"
  ExecutionRoleName:
    Type: "String"
    Description: "Role name for automation execution."
    Default: "SampleAutomationExecutionRole"
```

```
  SessionDurationInSecs:
    Type: "Number"
    Description: "Maximum session duration in seconds."
    Default: 14400

Resources:
  # This needs to run after AdminRoleName exists.
  ExecutionRole:
    Type: "AWS::IAM::Role"
    Properties:
      RoleName: !Ref ExecutionRoleName
      MaxSessionDuration: !Ref SessionDurationInSecs
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: "Allow"
            Principal:
              AWS:
                - !Sub "arn:aws:iam::${AdminAccountId}:role/${AdminRoleName}"
            Action:
              - "sts:AssumeRole"
      Path: "/"
      ManagedPolicyArns:
        - "arn:aws:iam::aws:policy/AdministratorAccess"
```

Après avoir configuré ces rôles, vous appelez les AWS Service Catalog API pour effectuer les tâches automatisées. Les commandes CLI sont données dans la vidéo.

Exemple d'entrée de provisionnement pour l'API Service Catalog

Voici un exemple des informations que vous pouvez fournir à l'`ProvisionProduct`API Service Catalog si vous utilisez l'API pour approvisionner des comptes AWS Control Tower :

```
{
  pathId: "lpv2-7n2o3nudljh4e",
  productId: "prod-y422ydgjge2rs",
  provisionedProductName: "Example product 1",
  provisioningArtifactId: "pa-2mmz36cfpj2p4",
  provisioningParameters: [
    {
      key: "AccountEmail",
      value: "abc@amazon.com"
    },
```

```
    {
      key: "AccountName",
      value: "ABC"
    },
    {
      key: "ManagedOrganizationalUnit",
      value: "Custom (ou-xfe5-a8hb8ml8)"
    },
    {
      key: "SSOUserEmail",
      value: "abc@amazon.com"
    },
    {
      key: "SSOUserFirstName",
      value: "John"
    },
    {
      key: "SSOUserLastName",
      value: "Smith"
    }
  ],
  provisionToken: "c3c795a1-9824-4fb2-a4c2-4b1841be4068"
}
```

Pour plus d'informations, consultez la référence d'API pour Service Catalog.

> **Note**
>
> Notez que le format de la chaîne d'entrée pour la valeur de `ManagedOrganizationalUnit` est passé de `OU_NAME` à`OU_NAME (OU_ID)`. La vidéo qui suit ne mentionne pas ce changement.

Vidéo de procédure

Cette vidéo (6:58) explique comment automatiser les déploiements de comptes dans AWS Control Tower. Pour un visionnage de meilleure qualité, sélectionnez l'icône dans le coin inférieur droit de la vidéo pour l'afficher en plein écran. Le sous-titrage est disponible.

Présentation vidéo du provisionnement automatique des comptes dans AWS Control Tower.

Procédure pas à pas : configurer AWS Control Tower sans VPC

Cette rubrique explique comment configurer vos comptes AWS Control Tower sans VPC.

Si votre charge de travail ne nécessite pas de VPC, vous pouvez effectuer les opérations suivantes :

- Vous pouvez supprimer le cloud privé virtuel (VPC) d'AWS Control Tower. Ce VPC a été créé lorsque vous avez configuré votre zone d'accueil.
- Vous pouvez modifier les paramètres de votre Account Factory afin que de nouveaux comptes AWS Control Tower soient créés sans VPC associé.

> **Important**
>
> Si vous configurez des comptes Account Factory avec les paramètres d'accès Internet VPC activés, ce paramètre annule le contrôle Interdire l'accès à Internet pour une instance Amazon VPC gérée par un client. Pour éviter d'activer l'accès à Internet pour les comptes nouvellement provisionnés, vous devez modifier le paramètre dans Account Factory.

Supprimer le VPC AWS Control Tower

En dehors d'AWS Control Tower, chaque AWS client dispose d'un VPC par défaut, que vous pouvez consulter sur la console Amazon Virtual Private Cloud (Amazon VPC) à l'adresse https://console.aws.amazon.com/vpc/. Vous reconnaîtrez le VPC par défaut, car son nom inclut toujours le mot (default) à la fin du nom.

Lorsque vous configurez une zone de landing zone AWS Control Tower, AWS Control Tower supprime votre VPC AWS par défaut et crée un nouveau VPC par défaut AWS Control Tower. Le nouveau VPC est associé à votre compte de gestion AWS Control Tower. Cette rubrique désigne ce nouveau VPC sous le nom de VPC Control Tower.

Lorsque vous consultez votre VPC AWS Control Tower dans la console Amazon VPC, le mot (par défaut) ne s'affiche pas à la fin du nom. Si vous possédez plusieurs VPC, vous devez utiliser la plage d'adresses CIDR attribuée pour identifier le VPC AWS Control Tower approprié.

Vous pouvez supprimer le VPC AWS Control Tower, mais si vous avez besoin ultérieurement d'un VPC dans AWS Control Tower, vous devez le créer vous-même.

Pour supprimer le VPC AWS Control Tower

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Recherchez **VPC** ou sélectionnez VPC dans les options du Service Catalog. Vous voyez ensuite le tableau de bord VPC.
3. Dans le menu de gauche, choisissez Your VPCs (Vos VPC). Vous voyez ensuite une liste de tous vos VPC.
4. Identifiez le VPC AWS Control Tower en fonction de sa plage de CIDR.
5. Sélectionnez le VPC, choisissez Actions, puis Delete VPC (Supprimer le VPC).

Un VPC AWS (par défaut) existe déjà dans chaque région pour le compte de gestion AWS Control Tower. Conformément aux meilleures pratiques en matière de sécurité, si vous choisissez de supprimer le VPC AWS Control Tower, il est également préférable de supprimer le AWS VPC par défaut associé au compte de gestion dans toutes les régions. AWS Par conséquent, pour sécuriser le compte de gestion, supprimez le VPC par défaut de chaque région, ainsi que le VPC créé par Control Tower dans votre région d'origine AWS Control Tower.

Créez un compte dans AWS Control Tower sans VPC

Si les charges de travail de vos utilisateurs finaux ne nécessitent pas de VPC, vous pouvez utiliser cette méthode pour configurer des comptes d'utilisateurs finaux pour lesquels aucun VPC n'a été créé automatiquement.

Depuis le tableau de bord d'AWS Control Tower, vous pouvez consulter et modifier les paramètres de configuration de votre réseau. Une fois que vous avez modifié les paramètres afin que les comptes AWS Control Tower soient créés sans VPC associé, tous les nouveaux comptes sont créés sans VPC jusqu'à ce que vous modifiiez à nouveau les paramètres.

Pour configurer Account Factory afin de créer des comptes sans VPC

1. Ouvrez un navigateur Web et accédez à la console AWS Control Tower à l'adresse https://console.aws.amazon.com/controltower.
2. Choisissez Account Factory dans le menu de gauche.
3. Vous voyez ensuite la page Account Factory avec la section Configuration réseau.
4. Notez les paramètres actuels si vous avez l'intention de les restaurer ultérieurement.

5. Choisissez le bouton Edit (Modifier) dans la section Network Configuration (Configuration du réseau).
6. Sur la page Edit account factory network configuration (Modifier la configuration du réseau Account Factory), accédez à la section VPC Configuration options for new accounts (Options de configuration des VPC pour les nouveaux comptes) .

   Vous pouvez suivre l'option 1 ou l'option 2, ou les deux, pour vous assurer qu'AWS Control Tower ne crée pas de VPC lors du provisionnement d'un compte.

   a. Option 1 — Supprimer des sous-réseaux

      - Désactivez le commutateur bascule du sous-réseau accessible sur Internet .
      - Définissez la valeur Maximum number of private subnets (Nombre maximal de sous-réseaux privés) sur 0.

   b. Option 2 — Supprimer des AWS régions

      - Désactivez chaque case à cocher de la colonne Regions for VPC creation (Régions pour la création de VPC).
7. Choisissez Enregistrer.

Erreurs possibles

Soyez conscient de ces erreurs possibles qui peuvent se produire lorsque vous supprimez votre VPC AWS Control Tower ou que vous reconfigurez Account Factory pour créer des comptes sans VPC.

- Votre compte de gestion existant peut comporter des dépendances ou des ressources dans le VPC AWS Control Tower, ce qui peut provoquer une erreur de suppression.
- Si vous conservez le CIDR par défaut en place lorsque vous configurez pour lancer de nouveaux comptes sans VPC, votre demande échoue avec une erreur indiquant que le CIDR n'est pas valide.

Procédure pas à pas : configurer des groupes de sécurité dans AWS Control Tower avec AWS Firewall Manager

La vidéo explique comment utiliser le service AWS Firewall Manager pour améliorer la sécurité de votre réseau pour AWS Control Tower. Vous pouvez désigner un compte d'administrateur de sécurité

qui est activé pour configurer des groupes de sécurité. Vous découvrirez comment configurer des politiques de sécurité et appliquer des règles de sécurité pour vos organisations AWS Control Tower, et comment remédier aux ressources non conformes en appliquant des politiques automatiquement. Vous pouvez consulter les groupes de sécurité en vigueur pour chaque compte et ressource (par exemple, une instance Amazon EC2) de votre organisation.

Vous pouvez créer vos propres stratégies de pare-feu ou vous abonner aux règles des fournisseurs approuvés.

Configuration de groupes de sécurité avec AWS Firewall Manager

Cette vidéo (8:02) explique comment configurer une meilleure sécurité de l'infrastructure réseau pour vos ressources et vos charges de travail dans AWS Control Tower. Pour un visionnage de meilleure qualité, sélectionnez l'icône dans le coin inférieur droit de la vidéo pour l'afficher en plein écran. Le sous-titrage est disponible.

Présentation vidéo de la configuration du pare-feu dans AWS Control Tower.

Pour plus d'informations, consultez la documentation sur la configuration du AWS WAF.

Procédure pas à pas : mise hors service d'une zone d'atterrissage d'une AWS Control Tower

AWS Control Tower vous permet de configurer et de gérer des AWS environnements multi-comptes sécurisés, appelés zones d'atterrissage. Le processus de nettoyage de toutes les ressources allouées par AWS Control Tower est appelé mise hors service d'une zone d'atterrissage.

Si vous ne souhaitez plus utiliser AWS Control Tower, l'outil de mise hors service automatique nettoie les ressources allouées par AWS Control Tower. Pour démarrer le processus de mise hors service automatique, accédez à la page Paramètres de la zone d'atterrissage, sélectionnez l'onglet de mise hors service, puis choisissez Zone d'atterrissage de mise hors service.

Pour obtenir la liste des actions effectuées lors de la mise hors service, voir. Vue d'ensemble du processus de mise hors service

> **Warning**
>
> La suppression manuelle de toutes vos ressources AWS Control Tower n'est pas la même chose que la mise hors service. Cela ne vous permettra pas de configurer une nouvelle zone d'atterrissage.

Vos données et vos données existantes ne AWS Organizations sont pas modifiées par le processus de mise hors service, de la manière suivante.

- AWS Control Tower ne supprime pas vos données. Il supprime uniquement les parties de la zone de destination qu'il a créée.
- Une fois le processus de mise hors service terminé, il reste quelques artefacts de ressources, tels que les compartiments Amazon S3 et les groupes de CloudWatch journaux Amazon Logs. Ces ressources doivent être supprimées manuellement avant de configurer une autre zone de destination et pour éviter les coûts éventuels associés à la gestion de certaines ressources.
- Vous ne pouvez pas utiliser la désaffectation automatique pour supprimer une zone de destination partiellement configurée. Si le processus de configuration de votre zone de destination échoue, vous devez résoudre l'état d'échec et le configurer jusqu'au bout pour rendre possible la désaffectation automatique, ou vous devez supprimer manuellement les ressources individuellement.

La désaffectation d'une zone de destination entraîne des modifications significatives et ne peut pas être annulé. Les mesures de mise hors service prises par AWS Control Tower et les artefacts qui restent après la mise hors service sont décrits dans les sections suivantes.

> **Important**
>
> Nous vous recommandons fortement de n'effectuer ce processus de désaffectation que si vous avez l'intention de cesser d'utiliser la zone de destination concernée. Il n'est pas possible de recréer la zone de destination après la désaffectation.

Vue d'ensemble du processus de mise hors service

Lorsque vous demandez la mise hors service de votre zone d'atterrissage, AWS Control Tower effectue les actions suivantes.

- Désactive chaque commande de détection activée dans la zone d'atterrissage. AWS Control Tower supprime les AWS CloudFormation ressources prenant en charge le contrôle.
- Désactive chaque contrôle préventif en supprimant les politiques de contrôle des services (SCP) de. AWS Organizations Si une politique est vide (ce qui devrait être le cas après avoir supprimé tous les SCP gérés par AWS Control Tower), AWS Control Tower détache et supprime entièrement la politique.
- Supprime tous les plans déployés en tant que. AWS CloudFormation StackSets
- Supprime tous les plans déployés sous forme de CloudFormation piles dans toutes les régions.
- Pour chaque compte provisionné, AWS Control Tower effectue les actions suivantes pendant le processus de mise hors service.
  - Supprime les enregistrements de chaque compte de l'usine de comptes.
  - Révoque les autorisations AWS Control Tower sur le compte en supprimant le rôle IAM créé par AWS Control Tower (sauf si des politiques supplémentaires y ont été ajoutées) et en recréant le rôle IAM standard`OrganizationsFullAccessRole`.
  - Supprime les enregistrements du compte de AWS Service Catalog.
  - Supprime le produit et le portefeuille de l'usine de comptes d' AWS Service Catalog.
- Supprime les plans des comptes partagés (audit et archivage des journaux).
- Révoque les autorisations AWS Control Tower associées aux comptes partagés en supprimant le rôle IAM créé par AWS Control Tower (sauf si des politiques supplémentaires y ont été ajoutées) et en recréant le `OrganizationsFullAccessRole` rôle IAM.
- Supprime les enregistrements relatifs aux comptes partagés.
- Supprime les enregistrements liés aux unités d'organisation créées par le client.
- Supprime les enregistrements internes qui identifient la région d'origine.

> **Note**
>
> Après la mise hors service, vous pouvez supprimer le plan VPC Account Factory (`BP_ACCOUNT_FACTORY_VPC`) pour nettoyer les routes et les passerelles NAT, si votre VPC n'était pas vide.

Ressources non supprimées lors de la mise hors service

La mise hors service d'une zone d'atterrissage n'inverse pas complètement le processus de configuration d'AWS Control Tower. Certaines ressources sont préservées, mais peuvent être supprimées manuellement.

AWS Organizations

Pour les clients n'ayant pas d' AWS Organizations organisation existante, AWS Control Tower met en place une organisation composée de deux unités organisationnelles (UO), nommées Security et Sandbox. Lorsque vous désaffectez une zone de destination, la hiérarchie de l'organisation est préservée, comme suit :

- Les unités organisationnelles (UO) que vous avez créées à partir de la console AWS Control Tower ne sont pas supprimées.
- Les unités d'organisation de sécurité et de sandbox ne sont pas supprimées.
- L'organisation n'est pas supprimée de AWS Organizations.
- Aucun compte AWS Organizations (partagé, provisionné ou géré) n'est déplacé ou supprimé.

AWS IAM Identity Center (SSO)

Pour les clients ne disposant pas d'un annuaire IAM Identity Center existant, AWS Control Tower met en place IAM Identity Center et configure un répertoire initial. Lorsque vous mettez hors service votre zone de landing zone, AWS Control Tower n'apporte aucune modification à IAM Identity Center. Si nécessaire, vous pouvez supprimer manuellement les informations de l'IAM Identity Center stockées dans votre compte de gestion. Plus spécifiquement, ces éléments ne sont pas concernés par la désaffectation :

- Les utilisateurs créés avec l'usine de comptes ne sont pas supprimés.
- Les groupes créés lors de la configuration d'AWS Control Tower ne sont pas supprimés.
- Les ensembles d'autorisations créés par AWS Control Tower ne sont pas supprimés.
- Les associations entre les comptes AWS et les ensembles d'autorisations IAM Identity Center ne sont pas supprimées.
- Les annuaires de l'IAM Identity Center ne sont pas modifiés.

Rôles

Lors de la configuration, AWS Control Tower crée certains rôles pour vous si vous utilisez la console, ou vous demande de créer ces rôles si vous configurez votre zone de landing zone via les API. Lorsque vous désactivez votre zone d'atterrissage, les rôles suivants ne sont pas supprimés :

- `AWSControlTowerAdmin`
- `AWSControlTowerCloudTrailRole`
- `AWSControlTowerStackSetRole`
- `AWSControlTowerConfigAggregatorRoleForOrganizations`

Compartiments Simple Storage Service (Amazon S3)

Lors de la configuration, AWS Control Tower crée des compartiments dans le compte de journalisation pour la journalisation et pour l'accès à la journalisation. Lorsque vous désaffectez la zone de destination, les ressources suivantes ne sont pas supprimées :

- Les compartiments S3 de journalisation et d'accès à la journalisation du compte de journalisation ne sont pas supprimés.
- Le contenu des compartiments de journalisation et d'accès à la journalisation ne sont pas supprimés.

Comptes partagés

Deux comptes partagés (Audit et Log Archive) sont créés dans l'unité d'organisation de sécurité lors de la configuration d'AWS Control Tower. Lorsque vous désaffectez la zone de destination :

- Les comptes partagés créés lors de la configuration d'AWS Control Tower ne sont pas fermés.
- Le rôle `OrganizationAccountAccessRole` IAM est recréé pour s'aligner sur la configuration standard AWS Organizations .
- Le rôle `AWSControlTowerExecution` est supprimé.

Comptes provisionnés

Les clients d'AWS Control Tower peuvent utiliser Account Factory pour créer de nouveaux comptes AWS. Lorsque vous désaffectez la zone de destination :

- Les comptes provisionnés que vous avez créés avec Account Factory ne sont pas fermés.
- Les produits approvisionnés ne AWS Service Catalog sont pas supprimés. Si vous les nettoyez en les résiliant, leurs comptes sont transférés vers l'unité d'organisation racine.
- Le VPC créé par AWS Control Tower n'est pas supprimé, et le AWS CloudFormation stack set (`BP_ACCOUNT_FACTORY_VPC`) associé n'est pas supprimé.
- Le rôle `OrganizationAccountAccessRole` IAM est recréé pour s'aligner sur la configuration standard AWS Organizations .
- Le rôle `AWSControlTowerExecution` est supprimé.

CloudWatch Logs Log Group

Un groupe de CloudWatch journaux Logs est créé dans le cadre du plan nomméAWSControlTowerBP-BASELINE-CLOUDTRAIL-MANAGEMENT. `aws-controltower/CloudTrailLogs` Ce groupe de journaux n'est pas supprimé. Le plan est supprimé, tandis que les ressources sont conservées.

- Ce groupe de journaux doit être supprimé manuellement avant de configurer une autre zone de destination.

> **Note**
>
> Les clients utilisant la landing zone 3.0 et les versions ultérieures n'ont pas besoin de supprimer les CloudTrail CloudTrail journaux et les rôles de journal de leur compte inscrit individuel, car ceux-ci sont créés uniquement dans le compte de gestion, pour le suivi au niveau de l'organisation.
> À partir de la version 3.2 de landing zone, AWS Control Tower crée une EventBridge règle Amazon, appeléeAWSControlTowerManagedRule. Cette règle est créée dans chaque compte membre, pour toutes les régions gouvernées. La règle n'est pas supprimée automatiquement lors de la mise hors service. Vous devez donc la supprimer manuellement des comptes partagés et membres de toutes les régions gouvernées avant de pouvoir configurer une zone d'atterrissage dans une nouvelle région.

Les procédures de suppression des ressources AWS Control Tower sont indiquées dansGérer les ressources d'AWS Control Tower.

Gérer les ressources d'AWS Control Tower

Ce document fournit des instructions sur la manière de supprimer les ressources AWS Control Tower individuellement, dans le cadre des tâches de maintenance et d'administration régulières. Les procédures décrites dans ce chapitre sont uniquement destinées à supprimer des ressources individuelles, ou quelques ressources, en cas de besoin. Ce n'est pas la même chose que de mettre hors service votre zone d'atterrissage.

Deux types de tâches peuvent vous obliger à supprimer des ressources :

- Pour supprimer des ressources lorsque vous gérez votre zone de destination dans des situations ordinaires.
- Pour nettoyer les ressources restantes après la mise hors service automatisée.

> **Warning**
>
> La suppression manuelle des ressources ne vous permettra pas de configurer une nouvelle zone de landing zone. Ce n'est pas la même chose que le déclassement. Si vous avez l'intention de mettre hors service votre zone d'atterrissage AWS Control Tower, suivez les instructions Procédure pas à pas : mise hors service d'une zone d'atterrissage d'une AWS Control Tower avant de prendre les mesures décrites dans ce chapitre. Les instructions de ce chapitre peuvent vous aider à nettoyer les ressources qui restent une fois la mise hors service automatique terminée. Même si vous supprimez manuellement toutes les ressources de votre zone d'atterrissage, cela n'équivaut pas à la mise hors service de la zone d'atterrissage et vous risquez de devoir payer des frais imprévus.

Si vous devez supprimer un compte d'AWS Control Tower, consultez les sections suivantes pour le fermer :

- Annuler la gestion d'un compte
- Fermer un compte créé dans Account Factory

Dois-je le mettre hors service au lieu de le supprimer ?

Si vous n'avez plus l'intention d'utiliser AWS Control Tower pour votre entreprise, ou si vous avez besoin d'un redéploiement majeur de vos ressources organisationnelles, vous souhaiterez peut-être

mettre hors service les ressources créées lors de la configuration initiale de votre zone de landing zone.

- Une fois le processus de mise hors service terminé, il reste quelques artefacts de ressources, tels que les compartiments Amazon S3 et les groupes de CloudWatch journaux Amazon Logs.
- Vous devez nettoyer manuellement les ressources restantes de vos comptes avant de configurer une autre zone d'atterrissage, afin d'éviter tout risque de frais imprévus. Pour de plus amples informations, veuillez consulter Ressources non supprimées lors de la mise hors service.

> **Warning**
>
> Nous vous recommandons vivement d'effectuer un processus de mise hors service uniquement si vous avez l'intention de ne plus utiliser votre zone d'atterrissage. Ce processus ne peut pas être annulé.

À propos de la suppression des ressources AWS Control Tower

Les procédures individuelles décrites dans ce chapitre vous guident à travers les méthodes manuelles de suppression des ressources AWS Control Tower. Ces procédures peuvent être suivies lorsque vous devez supprimer une ressource spécifique de votre zone de landing zone.

Avant d'exécuter ces procédures, sauf indication contraire, vous devez être connecté à la AWS Management Console région d'origine de votre zone d'atterrissage, et vous devez être connecté en tant qu'utilisateur IAM ou utilisateur dans IAM Identity Center avec des autorisations administratives pour le compte de gestion contenant votre zone d'atterrissage.

> **Warning**
>
> Il s'agit d'actions destructrices qui peuvent entraîner une dérive de la gouvernance dans la configuration de votre AWS Control Tower. Elles ne peuvent pas être annulées.

Rubriques

- Supprimer des stratégies de contrôle de service
- Supprimer StackSets et empiler
- Supprimer les compartiments Amazon S3 dans le compte Log Archive

- Supprimer un portefeuille et un produit Account Factory
- Supprimer les rôles et politiques d'AWS Control Tower
- Aide relative aux ressources AWS Control Tower

Supprimer des stratégies de contrôle de service

AWS Control Tower utilise des politiques de contrôle des services (SCP) pour ses contrôles. Cette procédure explique comment supprimer les SCP spécifiquement liés à AWS Control Tower.

Pour supprimer des AWS Organizations SCP

1. Ouvrez la console Organizations à l'adresse https://console.aws.amazon.com/organizations/.
2. Ouvrez l'onglet Stratégies et recherchez les stratégies de contrôle de service (SCP) ayant le préfixe aws-guardrails-, puis effectuez ce qui suit pour chaque SCP :
   a. Détachez la stratégie de contrôle de service de l'unité d'organisation.
   b. Supprimez la stratégie de contrôle de service.

Supprimer StackSets et empiler

AWS Control Tower utilise StackSets et cumule les commandes AWS Config Rules associées à votre zone de landing zone pour les déployer. Les procédures suivantes expliquent comment supprimer ces ressources spécifiques.

Pour supprimer AWS CloudFormation StackSets

1. Ouvrez la AWS CloudFormation console à l'adresse https://console.aws.amazon.com/cloudformation.
2. Dans le menu de navigation de gauche, choisissez StackSets.
3. Pour chacune StackSet d'entre elles comportant le préfixe AWSControlTower, procédez comme suit. Si vous avez plusieurs comptes dans un StackSet, cela peut prendre un certain temps.
   a. Choisissez le spécifique dans le tableau StackSet du tableau de bord. Cela ouvre la page des propriétés correspondante StackSet.
   b. Au bas de la page, dans le tableau Stacks, enregistrez les identifiants de AWS compte de tous les comptes du tableau. Copiez la liste de tous les comptes.
   c. Dans Actions, choisissez Supprimer les piles de StackSet.

d. Dans Définir les options de déploiement, dans Emplacements de déploiement, choisissez Déployer des piles dans les comptes.

e. Dans le champ de texte, entrez les identifiants de AWS compte que vous avez enregistrés à l'étape 3.b, séparés par des virgules. Par exemple : *123456789012*, *098765431098*, et ainsi de suite.

f. Dans Spécifier les régions, choisissez Ajouter tout, conservez les valeurs par défaut des autres paramètres de la page, puis choisissez Suivant.

g. Sur la page Vérification, vérifiez vos sélections, puis choisissez Supprimer les piles.

h. Sur la page StackSet des propriétés, vous pouvez recommencer cette procédure pour votre partenaire StackSets.

4. Le processus est terminé lorsque les enregistrements de la table Stacks des différentes pages de StackSets propriétés sont vides.
5. Lorsque les enregistrements de la table Stacks sont vides, choisissez Supprimer StackSet.

Pour supprimer des AWS CloudFormation piles

1. Ouvrez la AWS CloudFormation console à l'adresse https://console.aws.amazon.com/cloudformation.
2. Dans le tableau de bord Stacks, recherchez toutes les piles avec le préfixe. AWSControlTower
3. Pour chaque pile du tableau, procédez comme suit :

   a. Activez la case à cocher en regard du nom de la pile.

   b. Dans le menu Actions, sélectionnez Supprimer la pile.

   c. Dans la boîte de dialogue qui s'ouvre, consultez les informations, puis choisissez Oui, supprimer.

Supprimer les compartiments Amazon S3 dans le compte Log Archive

Les procédures suivantes vous indiquent comment vous connecter au compte d'archivage de journaux en tant qu'utilisateur d'IAM Identity Center dans le AWSControlTowerExecutiongroupe, puis comment supprimer les compartiments Amazon S3 de votre compte d'archivage de journaux.

Pour vous connecter à votre compte d'archivage de journaux avec les autorisations appropriées

1. Ouvrez la console Organizations à l'adresse https://console.aws.amazon.com/organizations/.

2. Dans l'onglet Comptes, recherchez le compte Archivage des journaux.
3. Dans le volet droit, qui s'ouvre, notez le numéro du compte d'archivage des journaux.
4. Dans la barre de navigation, choisissez le nom de votre compte pour ouvrir votre menu de compte.
5. Choisissez Changer de rôle.
6. Sur la page qui s'ouvre, fournissez le numéro de compte pour le compte d'archivage des journaux dans Compte.
7. Pour Rôle, entrez AWSControlTowerExecution.
8. Le champ Nom d'affichage est rempli de texte.
9. Choisissez votre Couleur.
10. Choisissez Changer de rôle.

Pour supprimer des compartiments Amazon S3

1. Ouvrez la console Amazon S3 sur https://console.aws.amazon.com/s3/.
2. Recherchez des noms de compartiments qui contiennent des aws controltower.
3. Pour chaque compartiment dans le tableau, procédez comme suit :

    a. Cochez la case pour le compartiment du tableau.
    b. Sélectionnez Delete (Supprimer).
    c. Dans la boîte de dialogue qui s'ouvre, vérifiez les informations pour vous assurer qu'elles sont exactes, entrez le nom du compartiment à confirmer, puis choisissez Confirmer.

Supprimer un portefeuille et un produit Account Factory

La procédure suivante vous explique comment vous connecter en tant qu'utilisateur d'IAM Identity Center dans le AWSServiceCatalogAdminsgroupe, puis nettoyer votre portefeuille et vos produits Account Factory.

Pour vous connecter à votre compte de gestion avec les autorisations appropriées

1. Accédez à l'URL du portail utilisateur à *directory-id*.awsapps.com/start
2. Dans AWS Compte, recherchez le compte de gestion.
3. Dans AWSServiceCatalogAdminFullAccess, choisissez Console de gestion pour vous connecter en AWS Management Console tant que tel.

Pour nettoyer Account Factory

1. Ouvrez la console Service Catalog à l'adresse https://console.aws.amazon.com/servicecatalog/.
2. Dans le menu de navigation de gauche, choisissez Liste de portefeuilles.
3. Dans le tableau Local Portfolios, recherchez un portefeuille nommé AWS Control Tower Account Factory Portfolio.
4. Choisissez le nom de ce portefeuille pour accéder à la page des détails.
5. Développez la section Contraintes de la page, puis cliquez sur le bouton radio correspondant à la contrainte portant le nom de produit AWS Control Tower Account Factory.
6. Choisissez SUPPRIMER LES CONTRAINTES.
7. Dans la boîte de dialogue qui s'ouvre, consultez les informations, puis choisissez CONTINUER.
8. Dans la section Produits de la page, cliquez sur le bouton radio correspondant au produit nommé AWS Control Tower Account Factory.
9. Choisissez SUPPRIMER LE PRODUIT.
10. Dans la boîte de dialogue qui s'ouvre, consultez les informations, puis choisissez CONTINUER.
11. Développez la section Utilisateurs, groupes et rôles de la page, puis activez les cases à cocher de tous les enregistrements de cette table.
12. Choisissez SUPPRIMER LES UTILISATEURS, GROUPES OU RÔLES.
13. Dans la boîte de dialogue qui s'ouvre, consultez les informations, puis choisissez CONTINUER.
14. Dans le menu de navigation de gauche, choisissez Liste de portefeuilles.
15. Dans le tableau Local Portfolios, recherchez un portefeuille nommé AWS Control Tower Account Factory Portfolio.
16. Sélectionnez la case d'option de ce portefeuille, puis choisissez SUPPRIMER LE PORTEFEUILLE.
17. Dans la boîte de dialogue qui s'ouvre, consultez les informations, puis choisissez CONTINUER.
18. Dans le menu de navigation de gauche, choisissez Liste de produits.
19. Sur la page des produits d'administration, recherchez le produit nommé AWS Control Tower Account Factory.
20. Choisissez le produit pour ouvrir la page Détails des produits admin
21. Dans Actions, choisissez Supprimer un produit.
22. Dans la boîte de dialogue qui s'ouvre, consultez les informations, puis choisissez CONTINUER.

Supprimer les rôles et politiques d'AWS Control Tower

Ces procédures vous expliquent comment nettoyer les rôles et les politiques créés par AWS Control Tower lors de la configuration de votre zone de landing zone, ou ultérieurement.

Pour supprimer le rôle IAM Identity Center AWSServiceCatalogEndUserAccess

1. Ouvrez la AWS IAM Identity Center console à l'adresse https://console.aws.amazon.com/singlesignon/.
2. Changez votre AWS région par votre région d'origine, qui est la région dans laquelle vous avez initialement configuré AWS Control Tower.
3. Dans le menu de navigation de gauche, sélectionnez AWS Comptes.
4. Choisissez le lien de votre compte de gestion.
5. Choisissez le menu déroulant pour les ensembles d'autorisations, sélectionnez AWSServiceCatalogEndUserAccess, puis choisissez Supprimer.
6. Choisissez AWS des comptes dans le panneau de gauche.
7. Choisissez l'onglet Jeux d'autorisations.
8. Sélectionnez-le AWSServiceCatalogEndUserAccesset supprimez-le.

Pour supprimer des rôles IAM

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le menu de navigation de gauche, choisissez Rôles.
3. Dans le tableau, recherchez les rôles portant le nom AWSControlTower.
4. Pour chaque rôle du tableau, procédez comme suit :
    a. Cochez la case correspondant au rôle.
    b. Choisissez Delete role (Supprimer le rôle).
    c. Dans la boîte de dialogue qui s'ouvre, consultez les informations, puis choisissez Oui, supprimer.

Pour supprimer les politiques IAM

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le menu de navigation de gauche, choisissez Stratégies.

3. Dans le tableau, recherchez les politiques portant le nom AWSControlTower.
4. Pour chaque stratégie du tableau, procédez comme suit :

    a. Cochez la case correspondant à la stratégie.

    b. Choisissez Actions de stratégie, puis Supprimer dans le menu déroulant.

    c. Dans la boîte de dialogue qui s'ouvre, consultez les informations, puis choisissez Supprimer.

Aide relative aux ressources AWS Control Tower

Si vous rencontrez des problèmes que vous ne parvenez pas à résoudre lorsque vous supprimez des ressources AWS Control Tower, contactez le AWS Support.

Comment mettre hors service une zone d'atterrissage

Pour mettre hors service votre zone d'atterrissage AWS Control Tower, suivez la procédure indiquée ici.

> **Note**
>
> Nous vous recommandons de dégérer vos comptes inscrits avant de les mettre hors service.

1. Accédez à la page des paramètres de la zone d'atterrissage dans la console AWS Control Tower.
2. Choisissez Decommission your landing zone (Désaffecter la zone de destination) dans la section du même nom.
3. Une boîte de dialogue s'affiche, expliquant l'action que vous êtes sur le point d'effectuer. Votre confirmation est requise. Pour confirmer l'intention de désaffectation, vous devez sélectionner toutes les cases et valider la procédure conformément aux instructions.

    > **Important**
    >
    > Le processus de désaffectation ne peut pas être annulé.

4. Si vous confirmez votre intention de mettre hors service votre zone d'atterrissage, vous êtes redirigé vers la page d'accueil d'AWS Control Tower pendant que la mise hors service est en cours. Ce processus peut nécessiter jusqu'à deux heures.

5. Lorsque la mise hors service est réussie, vous devez supprimer les ressources restantes manuellement avant de configurer une nouvelle zone de landing zone depuis la console AWS Control Tower. Ces ressources restantes incluent des compartiments, des organisations et des groupes de CloudWatch journaux Amazon S3 spécifiques.

   > **Note**
   >
   > Ces actions peuvent avoir des conséquences importantes sur vos activités de facturation et de conformité. Par exemple, le fait de ne pas supprimer ces ressources peut entraîner des frais imprévus.

   Pour plus d'informations sur la suppression manuelle des ressources, consultez À propos de la suppression des ressources AWS Control Tower.

6. Si vous avez l'intention de configurer une nouvelle zone de landing zone dans une nouvelle AWS région, suivez cette étape supplémentaire. Entrez la commande suivante via la CLI :

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

Tâches de nettoyage manuelles requises après la mise hors service

- Vous devez spécifier des adresses e-mail différentes pour les comptes d'archive du journal et d'audit si vous créez une nouvelle zone d'atterrissage après en avoir mis hors service, ou suivez la procédure pour importer vos propres comptes d'archive de journal ou d'audit existants.
- Le groupe de CloudWatch journaux Logs doit être supprimé manuellement avant de configurer une autre zone de landing zone. `aws-controltower/CloudTrailLogs`
- Les deux compartiments Amazon S3 avec des noms réservés pour les journaux doivent être supprimés ou renommés manuellement.
- Vous devez supprimer ou renommer manuellement les unités organisationnelles Security et Sandbox existantes.

> **Note**
>
> Avant de pouvoir supprimer l'organisation OU AWS Control Tower Security, vous devez d'abord supprimer les comptes de journalisation et d'audit, mais pas le compte de gestion. Pour supprimer ces comptes, vous devez Quand se connecter en tant qu'utilisateur root au compte d'audit et au compte de journalisation, puis les supprimer manuellement.

- Vous souhaiterez peut-être supprimer manuellement la configuration AWS IAM Identity Center (IAM Identity Center) d'AWS Control Tower, mais vous pouvez continuer avec la configuration IAM Identity Center existante.
- Vous souhaiterez peut-être supprimer le VPC créé par AWS Control Tower et supprimer le CloudFormation stack set AWS associé.
- Avant de configurer une nouvelle zone de landing zone dans une nouvelle AWS région, vous devez suivre ces étapes supplémentaires.
  - Entrez la commande suivante via la CLI :

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

  - Supprimez la règle gérée restante, appeléeAWSControlTowerManagedRule, des comptes partagés et membres de toutes les régions gouvernées. AWSControlTowerManagedRuleest une EventBridge règle d'Amazon.

Configuration après la mise hors service d'une zone d'atterrissage

Une fois que vous avez désaffecté une zone de destination, vous ne pouvez pas réexécuter de configuration tant que le nettoyage manuel n'est pas terminé. En outre, sans nettoyage manuel de ces ressources restantes, vous risquez de devoir payer des frais de facturation imprévus. Gardez bien à l'esprit les points suivants :

- Le compte de gestion AWS Control Tower fait partie de l'unité d'organisation racine d'AWS Control Tower. Assurez-vous que les rôles IAM et les politiques IAM suivants sont supprimés du compte de gestion :
  - Rôles :

    - AWSControlTowerAdmin

    - `AWSControlTowerCloudTrailRole`

    - `AWSControlTowerStackSetRole`

  - Stratégies :

    - `AWSControlTowerAdminPolicy`

    - `AWSControlTowerCloudTrailRolePolicy`

    - `AWSControlTowerStackSetRolePolicy`

- Vous souhaiterez peut-être supprimer ou mettre à jour la configuration existante de l'IAM Identity Center pour AWS Control Tower avant de créer à nouveau une zone de landing zone, mais il n'est pas obligatoire de la supprimer.
- Vous souhaiterez peut-être supprimer le VPC créé par AWS Control Tower.
- L'installation échoue si les adresses e-mail spécifiées pour les comptes de journalisation ou d'audit sont associées à un AWS compte existant. Vous pouvez fermer les AWS comptes ou utiliser des adresses e-mail différentes pour configurer à nouveau une zone de landing zone. Vous pouvez également réutiliser ces comptes partagés existants, avec la fonctionnalité qui vous permet d'apporter vos propres comptes de journalisation et d'audit. Pour plus d'informations, consultez Considérations relatives à l'ajout de comptes de sécurité ou de journalisation existants.
- L'installation échoue si des compartiments Amazon S3 portant les noms réservés suivants existent déjà dans le compte de journalisation :
  - `aws-controltower-logs-{accountId}-{region}` (utilisé pour le compartiment de journalisation).
  - `aws-controltower-s3-access-logs-{accountId}-{region}` (utilisé pour le compartiment d'accès à la journalisation).

  Vous devez renommer ou supprimer ces compartiments, ou utiliser un autre compte de journalisation.
- L'installation échoue si le compte de gestion possède le groupe de journaux existant dans CloudWatch Logs. `aws-controltower/CloudTrailLogs` Vous devez renommer ou supprimer le groupe de journaux.

Avant de procéder à la configuration d'un nouveau Région AWS

Si vous avez l'intention de configurer une nouvelle zone de landing zone dans une nouvelle AWS région, suivez ces étapes supplémentaires.

- Entrez la commande suivante via la CLI :

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

- Supprimez la règle gérée restante, appeléeAWSControlTowerManagedRule, des comptes partagés et des comptes membres pour toutes les régions gouvernées.

> **Note**
>
> Vous ne pouvez pas configurer de nouvelle zone de landing zone dans une organisation dotée d'unités d'organisation de haut niveau nommées Security ou Sandbox. Vous devez renommer ou supprimer ces UO pour reconfigurer une zone de destination.

Résolution des problèmes

Si vous rencontrez des problèmes lors de l'utilisation d'AWS Control Tower, vous pouvez utiliser les informations suivantes pour les résoudre conformément à nos meilleures pratiques. Si les problèmes que vous rencontrez ne sont pas couverts par les informations suivantes, ou s'ils persistent après avoir essayé de les résoudre, contactez le AWS Support.

Échec de lancement de la zone de destination

Causes courantes d'échec du lancement de la zone de destination :

- Absence de réponse à un message électronique de confirmation.
- AWS CloudFormation StackSet échec.

Messages électroniques de confirmation : si votre compte de gestion date de moins d'une heure, il est possible que vous rencontriez des problèmes lors de la création des comptes supplémentaires.

Action à exécuter

Si vous rencontrez ce problème, vérifiez votre e-mail. Vous avez peut-être reçu un e-mail de confirmation qui est en attente de réponse. Sinon, nous vous recommandons d'attendre une heure, puis de réessayer. Si le problème persiste, contactez le AWS Support.

Échec StackSets : L'échec du lancement dans la zone d'atterrissage est une autre cause possible AWS CloudFormation StackSet d'échec. AWS Les régions Security Token Service (STS) doivent être activées dans le compte de gestion pour toutes les AWS régions gouvernées par AWS Control Tower, afin que le provisionnement puisse réussir ; sinon, les stack sets ne pourront pas être lancés.

Action à exécuter

Assurez-vous d'activer toutes les régions de point de terminaison STS (AWS Security Token Service) requises avant de lancer AWS Control Tower.

Pour consulter la liste des produits Régions AWS pris en charge par AWS Control Tower, consultezComment AWS les régions fonctionnent avec AWS Control Tower.

Erreur indiquant que la zone d'atterrissage n'est pas à jour

Si vous n'avez pas récemment mis à jour votre zone de landing zone, il se peut que vous receviez un message d'erreur lorsque vous tenterez de regagner l'accès à AWS Control Tower. Un message d'erreur similaire à celui-ci peut s'afficher :

```
Unable to access Control Tower
```

Votre compte est inactif depuis trop longtemps. En raison de votre inactivité, vous devez mettre à jour votre zone de landing zone pour accéder à AWS Control Tower.

Cependant, la mise à jour de votre zone d'atterrissage peut échouer.

Étapes à suivre

Connectez-vous au compte de gestion de votre organisation et connectez-vous en tant qu'utilisateur root. Votre utilisateur IAM ou utilisateur dans IAM Identity Center doit disposer des autorisations d'administrateur AWS Control Tower et faire partie du AWSControlTowerAdminsgroupe. Réessayez ensuite la mise à jour.

Échec du provisionnement du nouveau compte

Si vous rencontrez ce problème, recherchez parmi les causes les plus courantes.

Lorsque vous avez rempli le formulaire de provisionnement du compte, vous pouvez avoir :

- tagOptions spécifié,
- notifications SNS activées,
- notifications de produits provisionnés activées.

Réessayez de provisionner votre compte, sans spécifier aucune de ces options. Pour plus d'informations, consultez Provisionner des comptes avec AWS Service Catalog Account Factory .

Autres causes communes d'échec :

- Si vous avez créé un plan produit provisionné (pour afficher les modifications des ressources), le provisionnement de votre compte peut rester indéfiniment dans l'état In progress (En cours).
- La création d'un nouveau compte dans Account Factory échouera alors que d'autres modifications de configuration d'AWS Control Tower sont en cours. Par exemple, alors qu'un processus est en

cours d'exécution pour ajouter un contrôle à une unité d'organisation, Account Factory affiche un message d'erreur si vous essayez de configurer un compte.

Pour vérifier le statut d'une action précédente dans AWS Control Tower

- Naviguez vers AWS CloudFormation > StackSets
- Vérifiez chaque ensemble de piles associé à AWS Control Tower (préfixe : "AWSControlTower«)
- Recherchez les AWS CloudFormation StackSets opérations toujours en cours.

Si le provisionnement de votre compte prend plus d'une heure, il est préférable de mettre fin au processus de provisionnement et de réessayer.

Échec de l'inscription d'un compte existant

Si vous essayez une fois d'inscrire un AWS compte existant et que cette inscription échoue, le message d'erreur peut vous indiquer que le stack set existe lors de la deuxième tentative. Pour continuer, vous devez supprimer le produit provisionné dans Account Factory.

Si la raison du premier échec d'inscription était que vous aviez oublié de créer le rôle `AWSControlTowerExecution` dans le compte à l'avance, le message d'erreur que vous recevrez vous demandera à juste titre de créer le rôle. Toutefois, lorsque vous essayez de créer le rôle, vous êtes susceptible de recevoir un autre message d'erreur indiquant qu'AWS Control Tower n'a pas pu le créer. Cette erreur se produit car le processus a été partiellement terminé.

Dans ce cas, vous devez effectuer deux étapes de récupération avant de pouvoir procéder à l'inscription de votre compte existant. Tout d'abord, vous devez résilier le produit approvisionné par Account Factory via la AWS Service Catalog console. Ensuite, vous devez utiliser la AWS Organizations console pour déplacer manuellement le compte hors de l'unité d'organisation et le ramener à la racine. Après cela, créez le rôle `AWSControlTowerExecution` dans le compte, puis remplissez à nouveau le formulaire Inscrire un compte.

Une autre cause possible d'échec d'inscription est que le compte dispose de ressources AWS Config existantes. Dans ce cas, consultez la section Inscrire des comptes disposant de AWS Config ressources existantes pour savoir comment modifier vos ressources existantes.

Impossible de mettre à jour un compte Account Factory

Lorsqu'un compte est dans un état incohérent, il ne peut pas être mis à jour correctement depuis Account Factory ou AWS Service Catalog.

Cas 1 : Vous pouvez rencontrer un message d'erreur similaire à celui-ci :

```
AWS Control Tower could not baseline VPC in the managed account because of existing resource dependencies.
```

Cause courante : AWS Control Tower supprime toujours le VPC AWS par défaut lors du provisionnement initial. Pour avoir un VPC AWS par défaut dans un compte, vous devez l'ajouter après la création du compte. AWS Control Tower possède son propre VPC par défaut qui remplace le AWS VPC par défaut, sauf si vous configurez Account Factory comme indiqué dans la procédure pas à pas, afin qu'AWS Control Tower ne fournisse aucun VPC. Ensuite, le compte n'a pas de VPC. Vous devrez ajouter à nouveau le VPC AWS par défaut si vous souhaitez utiliser celui-ci.

Cependant, AWS Control Tower ne prend pas en charge le AWS VPC par défaut. Si vous en déployez un, le compte entre dans l'état `Tainted`. Lorsqu'il est dans cet état, vous ne pouvez pas mettre à jour le compte via AWS Service Catalog.

Action à mettre en œuvre : vous devez supprimer le VPC par défaut que vous avez ajouté, puis vous pourrez mettre à jour le compte.

> **Note**
>
> Cet `Tainted` état entraîne un problème complémentaire : un compte qui n'est pas mis à jour peut empêcher l'activation des contrôles sur l'unité organisationnelle dont il fait partie.

Cas 2 : un message d'erreur similaire à celui-ci peut s'afficher :

```
AWS Control Tower detects that your enrolled account has been moved to a new organizational unit.
```

Cause fréquente : vous avez tenté de déplacer un compte d'une unité d'organisation enregistrée vers une autre, mais les anciennes règles de AWS configuration sont conservées. Le compte est dans un état incohérent.

Mesures à prendre :

Si le transfert de compte était prévu :

- Résiliez le compte dans Service Catalog.
- Inscrivez-le à nouveau.
- Contexte/impact : les règles de AWS configuration déployées ne correspondent pas à la configuration dictée par l'unité d'organisation de destination.
- AWS Les règles de configuration peuvent être conservées par rapport à l'unité d'organisation précédente, ce qui entraîne des dépenses imprévues.
- Les tentatives de réinscription ou de mise à jour du compte échoueront en raison de conflits de dénomination des ressources.

Si le transfert de compte n'était pas intentionnel :

- Rétablissez le compte dans son unité d'organisation d'origine.
- Mettez à jour le compte depuis Service Catalog.
- Dans les paramètres de lancement, entrez l'unité d'organisation dans laquelle le compte se trouvait à l'origine.
- Contexte/impact : Si le compte n'est pas renvoyé dans son unité d'organisation d'origine, son état ne sera pas conforme aux contrôles dictés par la nouvelle unité d'organisation dans laquelle il se trouve.
- La mise à jour d'un compte n'est pas une correction valide, car elle ne supprime pas les AWS Config règles associées à son unité d'organisation précédente.

Impossible de mettre à jour la zone d'atterrissage

AWS Control Tower ne revient pas à une version précédente de la zone d'atterrissage en cas d'échec d'une mise à jour. Il se peut que votre zone d'atterrissage soit dans un état indéterminé. Si tel est le cas, contactez AWS le support.

Les mises à jour de la zone d'atterrissage peuvent échouer pour plusieurs raisons.

- Conditions préalables non remplies
- AWS Config des ressources existent dans certains comptes
- Des comptes fermés existent

Conditions préalables non remplies

Une mise à jour de zone d'atterrissage doit répondre aux mêmes exigences que la configuration d'une zone d'atterrissage. Avant de procéder à la mise à jour, passez en revue les vérifications préalables au lancement.

AWS Config des ressources existent dans les comptes de l'unité d'organisation de sécurité

N'ajoutez pas de AWS Config ressources dans vos comptes d'archivage d'audit et de journal. Le processus de mise à jour de la zone d'atterrissage ne peut pas être terminé en présence de ces ressources. Ces restrictions sont similaires à celles applicables à l'ouverture d'un compte ou à la création d'une zone de landing zone pour la première fois. Pour plus d'informations, voir Inscrire des comptes disposant de AWS Config ressources existantes.

Des comptes fermés existent

Lorsqu'un compte est fermé ou suspendu, vous pouvez rencontrer un problème lorsque vous essayez de mettre à jour votre zone de landing zone. Vous devez supprimer le produit approvisionné sur chaque compte fermé avant d'effectuer une mise à jour de la zone de landing zone.

Sur la page du produit AWS Service Catalog approvisionné, vous pouvez voir un message d'erreur similaire à celui-ci :

```
AWSControlTowerExecution role can't be assumed on the account.
```

Cause fréquente : vous avez suspendu un compte sans supprimer le produit approvisionné.

Action à effectuer : Si cette erreur s'affiche, deux options s'offrent à vous :

1. Contactez le AWS Support et rouvrez le compte, supprimez le produit approvisionné, puis fermez-le à nouveau.
2. Supprimez les ressources du StackSets qui sont devenues orphelines en raison de la fermeture du compte. (Cette option n'est disponible que s' StackSets ils contiennent des instances à l'état actuel que vous ne supprimez pas.)

Pour supprimer les ressources du StackSets, procédez comme suit pour chaque compte fermé :

- Accédez à chacune des AWS Control Tower StackSets et supprimez-les StackInstances de chaque région, pour le compte qui a été fermé.

- IMPORTANT : Choisissez l'option Retain Stack afin de StackSet supprimer uniquement les instances de pile. StackSet ne peut pas assumer un rôle depuis le compte fermé. Il échouera donc s'il essaie d'assumer le `AWSControlTowerExecution` rôle, ce qui entraîne le message d'erreur que vous avez reçu.

Erreur de défaillance mentionnant AWS Config

S'il AWS Config est activé dans n'importe quelle AWS région prise en charge par AWS Control Tower, vous pouvez recevoir un message d'erreur en raison de l'échec d'une pré-vérification. Le message peut ne pas expliquer correctement le problème, en raison d'un comportement sous-jacent de AWS Config.

Vous pouvez recevoir un message d'erreur similaire à l'un des suivants :

- `AWS Control Tower cannot create an AWS Config delivery channel because one already exists. To continue, delete the existing delivery channel and try again .`
- `AWS Control Tower cannot create an AWS Config configuration recorder because one already exists. To continue, delete the existing delivery channel and try again .`

Cause courante : lorsque le AWS Config service est activé sur un AWS compte, il crée un enregistreur de configuration et un canal de diffusion avec un nom par défaut. Si vous désactivez le AWS Config service via la console, il ne supprime pas l'enregistreur de configuration ni le canal de diffusion. Vous devez les supprimer via la CLI ou les modifier pour les utiliser dans AWS Control Tower. Si le AWS Config service est activé dans l'une des régions prises en charge par AWS Control Tower, cela peut entraîner cet échec.

Si le compte possède des ressources AWS Config existantes, voir Inscrire des comptes dotés de AWS Config ressources existantes pour savoir comment modifier vos ressources existantes.

Action à entreprendre : supprimez l'enregistreur de configuration et le canal de livraison dans toutes les régions prises en charge. La désactivation de AWS Config ne suffit pas, l'enregistreur de configuration et le canal de livraison doivent être supprimés au moyen de la CLI. Après avoir

supprimé l'enregistreur de configuration et le canal de diffusion de la CLI, vous pouvez réessayer de lancer AWS Control Tower et d'enregistrer le compte.

Si vous êtes en train de déployer un produit provisionné, vous devez le supprimer avant de réessayer. Dans le cas contraire, un message d'erreur similaire à celui-ci peut s'afficher :

- `An error occurred (InvalidParametersException) when calling the ProvisionProduct operation: A stack named Stackname already exists.`

Dans le message, *Stackname*indique le nom de la pile.

Voici quelques exemples de commandes AWS Config CLI que vous pouvez utiliser pour déterminer l'état de votre enregistreur de configuration et de votre canal de diffusion.

Commandes d'affichage :

- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-recorders`
- `The normal response is something like "name": "default"`

Commandes de suppression :

- `aws configservice stop-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-delivery-channel --delivery-channel-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`

Pour plus d'informations, consultez la AWS Config documentation

- Gestion de l'enregistreur de configuration (AWS CLI)
- Gestion du canal de distribution

Erreur Aucun chemin de lancement trouvé

Lorsque vous essayez de créer un nouveau compte, un message d'erreur similaire à celui-ci peut s'afficher :

```
No launch paths found for resource: prod-dpqqfywxxxx
```

Ce message d'erreur est généré par AWS Service Catalog, qui est le service intégré qui permet de provisionner des comptes dans AWS Control Tower.

Causes courantes :

- Vous êtes peut-être connecté en tant que root. AWS Control Tower ne prend pas en charge la création de comptes lorsque vous êtes connecté en tant qu'utilisateur root.
- L'utilisateur de votre IAM Identity Center n'a pas été ajouté au groupe d'autorisations approprié. Vous devrez peut-être ajouter votre utilisateur IAM Identity Center à l'un des groupes d'autorisations suivants : AWSAccountFactory(pour l'accès utilisateur final) ou AWSServiceCatalogAdmins(pour l'accès administrateur).
- Si vous êtes authentifié en tant qu'utilisateur IAM, vous devez l'ajouter au AWS Service Catalog portefeuille afin qu'il dispose des autorisations appropriées.
- Ce problème se produit également si vous disposez des autorisations appropriées, mais qu'une dérive d'AWS Control Tower est détectée et qu'une réparation de la dérive est nécessaire. Pour réparer la plupart des types de dérive, choisissez Réinitialiser sur la page des paramètres de la zone d'atterrissage.

Réception d'une erreur Autorisations insuffisantes

Il est possible que votre compte ne dispose pas des autorisations nécessaires pour effectuer certaines tâches dans certains cas AWS Organizations. Si vous rencontrez le type d'erreur suivant, vérifiez tous les domaines d'autorisation, tels que les autorisations IAM ou IAM Identity Center, pour vous assurer que votre autorisation n'est pas refusée à partir de ces endroits :

```
You have insufficient permissions to perform AWS Organizations API actions.
```

Si vous pensez que votre travail nécessite l'action que vous tentez d'effectuer et que vous ne trouvez aucune restriction pertinente, contactez votre administrateur système ou le AWS Support.

Les contrôles Detective n'ont aucun effet sur les comptes

Si vous avez récemment étendu le déploiement de votre AWS Control Tower à une nouvelle AWS région, les contrôles de détection nouvellement appliqués ne prennent effet sur les nouveaux comptes que vous créez dans aucune région tant que les comptes individuels au sein des unités d'organisation régies par AWS Control Tower ne sont pas mis à jour. Les contrôles de détection existants sur les comptes existants sont toujours en vigueur.

Si vous essayez d'activer un contrôle de détection avant de mettre à jour vos comptes, un message d'erreur similaire à celui-ci peut s'afficher :

```
AWS Control Tower can't enable the selected control on this OU. AWS Control Tower cannot apply the control on the OU ou-xxx-xxxxxxxx, because child accounts have dependencies that are missing. Update all child accounts under the OU, then try again.
```

Action à exécuter : mettre à jour les comptes.

Pour mettre à jour vos comptes depuis la console AWS Control Tower, consultezQuand mettre à jour les unités d'organisation et les comptes AWS Control Tower.

Pour mettre à jour plusieurs comptes individuels par programmation, vous pouvez utiliser les API de AWS Service Catalog et la AWS CLI pour automatiser les mises à jour. Pour plus d'informations sur l'approche à adopter en matière de mise à jour, consultez cette Vidéo de procédure. Vous pouvez remplacer l'UpdateProvisionedProductProvisionProductAPI présentée dans la vidéo par l'API.

Si vous rencontrez d'autres difficultés pour activer les contrôles de détection sur vos comptes, contactez le AWS Support.

Erreur de dépassement du taux renvoyée par l' AWS Organizations API

Cause possible

Votre charge de travail s'exécutait pendant qu'AWS Control Tower effectuait un scan quotidien pour vérifier si vos SCP étaient à la dérive.

Étapes à suivre

Si vous rencontrez une limitation ou une `rate exceeded` erreur d'API, procédez comme suit :

- Exécutez vos charges de travail à un autre moment. (Reportez-vous au calendrier des analyses d'invariance SCP d'AWS Control Tower par région pour savoir quand AWS Control Tower exécute ses analyses d'audit.)
- Si vous appelez les API directement via HTTP : utilisez le AWS SDK, qui réessaie automatiquement les actions ayant échoué
- Demandez une augmentation de limite par le biais du Service Quotas et du AWS Support

Voici un exemple d'instructions de résolution des problèmes liés à la limitation des API dans Elastic Beanstalk : `https://aws.amazon.com/premiumsupport/knowledge-center/elastic-beanstalk-api-throttling-errors/`

Impossible de déplacer un compte Account Factory directement d'une zone d'atterrissage d'AWS Control Tower vers une autre zone d'atterrissage d'AWS Control Tower

> **Warning**
>
> Cette pratique ne répond pas aux conditions requises pour l'inscription à un compte éligible, car les comptes éligibles doivent appartenir à la même organisation AWS globale, et chaque organisation ne peut disposer que d'une seule zone de landing zone. Si vous avez essayé d'effectuer cette action et que vous recevez plusieurs messages d'erreur, voici quelques informations qui pourraient vous être utiles.

Pour déplacer un compte que vous avez provisionné via Account Factory vers une autre zone de landing zone gérée par AWS Control Tower, sous un autre compte de gestion, vous devez supprimer tous les rôles IAM et les stacks associés à ce compte de l'unité d'organisation d'origine. Supprimez ces ressources de chaque région dans laquelle le compte est déployé.

> **Note**
>
> Le meilleur moyen de supprimer les ressources est de déprovisionner le compte dans son unité d'organisation d'origine avant d'essayer de le déplacer.

Si vous ne supprimez pas les ressources, l'inscription à la nouvelle unité d'organisation échouera, de façon assez spectaculaire. Vous pouvez rencontrer un ou plusieurs messages d'erreur, et vous continuerez à recevoir des messages d'erreur similaires jusqu'à ce que les rôles et les piles restants soient supprimés de chaque région dans laquelle le compte a été déployé.

Chaque fois que vous recevez un message d'erreur, vous devez supprimer le compte de la nouvelle unité d'organisation, supprimer l'ancienne ressource visée par le message d'erreur, puis tenter de déplacer le compte à nouveau dans la nouvelle unité d'organisation. Ce processus removing-and-deleting doit être répété pour chaque ressource restante, pour chaque région dans laquelle le compte a été déployé, éventuellement 10 ou 20 fois. Ces erreurs répétées se produisent parce que le compte a été configuré dans une unité d'organisation avec un SCP qui empêche la suppression du rôle IAM. Vous pouvez raccourcir le processus de restauration en supprimant toutes les ressources du compte avant de réessayer.

Les exemples ci-dessous représentent les types de messages d'échec que vous pouvez recevoir si des rôles et des piles non supprimés sont conservés. Vous verrez probablement l'un de ces messages à la fois, à chaque fois que vous tenterez d'enregistrer le compte, tant que les anciennes ressources restent.

Les valeurs des chaînes d'ID de ressource ont été modifiées pour les exemples. Leurs valeurs ne seront pas identiques dans un message d'erreur que vous pourriez recevoir. Un message similaire aux exemples suivants peut s'afficher :

- `AWS Control Tower cannot create the IAM role aws-controltower-AdministratorExecutionRole because the role already exists. To continue, delete the existing IAM role and try again.`
- `AWS Control Tower cannot create the IAM role aws-controltower-ConfigRecorderRole because the role already exists. To continue, delete the existing IAM role and try again.`
- `AWS Control Tower cannot create the IAM role aws-controltower-ForwardSnsNotificationRole because the role already exists. To continue, delete the existing IAM role and try again.`

Il se peut également qu'un message d'erreur similaire à celui-ci s'affiche à propos d'une défaillance d'un stack set :

```
"Error\":\"StackSetFailState\",
```

```
\"Cause\":\"StackSetOperation on AWSControlTowerBP-BASELINE-CLOUDWATCH
with id 8aXXXXf5-e0XX-4XXa-bc4XX-dXXXXXee31
has reached SUCCEEDED state but has 1 NON-CURRENT stack instances;
here is the summary :{ StackSet Id:
AWSControlTowerBP-BASELINE-CLOUDWATCH:40XXXbf2-Xead-46a1-XXXa-eXXXXecb2ee2,
Stack instance Id:
arn:aws:cloudformation:eu-west-1:1X23456789XX:
            stack/StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-4feXXXXXX-ecXX-XXc6-
bXXX-4ae678/4feXXXXXX-ecX-4ae123458,
Status: OUTDATED,
Status Reason: ResourceLogicalId:ForwardSnsNotification,
ResourceType:AWS::Lambda::Function,
ResourceStatusReason:aws-controltower-NotificationForwarder already exists in stack
arn:aws:cloudformation:eu-west-1:1X23456789XX:
            stack/StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-4feXXXXXX-ecXX-XXc6-
bXXX-4ae678/4feXXXXXX-ecX-4ae123458.
```

Une fois que toutes les ressources restantes auront été supprimées de la première UO, vous pourrez inviter, approvisionner ou inscrire le compte dans la nouvelle UO avec succès.

AWS Support

Si vous souhaitez déplacer vos comptes de membres existants vers un autre plan de support, vous pouvez vous connecter à chaque compte avec les informations d'identification du compte racine, comparer les plans et définir le niveau de support que vous préférez.

Nous vous recommandons de mettre à jour les contacts MFA et de sécurité des comptes lorsque vous apportez des modifications à votre plan de support.

Types de lignes de base

Dans AWS Control Tower, une référence est un groupe de ressources et de configurations spécifiques que vous pouvez appliquer à une cible. L'objectif de référence le plus courant peut être une unité organisationnelle (UO). Par exemple, vous pouvez activer une ligne de base avec une unité d'organisation sélectionnée comme cible, afin d'enregistrer cette unité d'organisation dans AWS Control Tower.

Lors de la configuration de la zone d'atterrissage, la cible de référence peut être un compte partagé ou la zone d'atterrissage dans son ensemble. Certaines lignes de base peuvent être activées et mises à jour en fonction des paramètres et des configurations de votre zone d'atterrissage. AWS Control Tower crée et déploie les ressources vers la cible conformément à la ligne de base spécifiée.

Lorsque vous activez une ligne de base pour une cible, celle-ci est représentée sous la forme d'une AWS CloudFormation ressource, appelée `EnabledBaseline` ressource.

AWS Control Tower inclut quatre types essentiels de lignes de base :

- Un type peut s'appliquer à une unité d'organisation enregistrée auprès d'AWS Control Tower ou à une unité d'organisation que vous avez l'intention d'enregistrer en appliquant la ligne de base.
- Trois types de référence peuvent s'appliquer à une zone d'atterrissage ou à un compte partagé, lors de la configuration initiale ou lors d'une mise à jour de la zone d'atterrissage.

Type de référence qui s'applique au niveau de l'unité d'organisation, pour l'enregistrement et la mise à jour des unités d'organisation

- Nom: `AWSControlTowerBaseline`

  Description : configure les ressources et les contrôles obligatoires pour les comptes membres au sein de l'unité d'organisation cible, nécessaires à la gouvernance d'AWS Control Tower.

  Remarque : Cette ligne de base conserve les paramètres de la zone d'atterrissage. La région refuse le contrôle. En d'autres termes, si une région n'est pas autorisée au niveau de la zone d'atterrissage, elle n'est pas autorisée pour cette unité d'organisation lorsque vous appelez l'`EnableBaseline`API pour enregistrer une unité d'organisation.

> **Note**
>
> Le refus de contrôle de la région au niveau de l'OU n'a aucun moyen d'autoriser les régions que la région de refus de contrôle de la zone d'atterrissage n'autorise pas.

Pour plus d'informations, consultez la section Comment les SCP fonctionnent avec le déni dans la AWS Organizations documentation.

Recommandation : Nous vous recommandons de vérifier les régions dans lesquelles votre unité d'organisation cible peut exécuter des charges de travail, et de comparer les résultats par rapport à la zone de destination Refus de contrôle, avant d'appeler l'`EnableBaseline`API de l'unité d'organisation, sous peine de perdre l'accès aux ressources dans certaines régions.

> **Note**
>
> Les lignes de base des zones d'atterrissage se comportent différemment des lignes de base au niveau de l'OU.

AWS Control Tower active automatiquement les lignes de base qui s'appliquent au niveau de la zone d'atterrissage, dans le cadre du processus de configuration et de mise à jour de la zone d'atterrissage. Les valeurs de référence de votre zone d'atterrissage peuvent changer au fur et à mesure que vous modifiez les paramètres de votre zone d'atterrissage. Par exemple, si vous optez pour IAM Identity Center, AWS Control Tower peut activer la dernière version de la `IdentityCenterBaseline` ligne de base sur votre zone de landing zone.

Vous pouvez consulter les lignes de base activées pour votre zone de landing grâce à l'appel `ListEnabledBaselines` d'API.

Types de référence pouvant s'appliquer à votre zone d'atterrissage ou à vos comptes partagés

- Nom: `AuditBaseline`

  Description : configure les ressources pour surveiller la sécurité et la conformité des comptes de votre organisation. Vous ne pouvez pas modifier cette ligne de base, elle est déployée par AWS Control Tower.

- Nom: `LogArchiveBaseline`

  Description : met en place un référentiel central pour les journaux des activités des API et des configurations de ressources provenant des comptes de votre organisation. Vous ne pouvez pas modifier cette ligne de base, elle est déployée par AWS Control Tower.

- Nom: `IdentityCenterBaseline`

  Description : configure des ressources partagées pour IAM Identity Center, qui prépare la configuration de l'accès `AWSControlTowerBaseline` à Identity Center pour les comptes.

  Remarque : Cette base de référence ne fonctionne que lorsque vous avez sélectionné IAM Identity Center comme fournisseur d'identité au moment de configurer votre zone d'atterrissage pour la première fois, ou si vous modifiez ultérieurement les paramètres de votre zone d'atterrissage pour activer IAM Identity Center pour votre zone d'atterrissage. Si vous utilisez un autre fournisseur d'identité, vous n'aurez pas accès à cette base de référence.

Inscription partielle de comptes

Lorsque vous travaillez avec des bases de référence, un compte peut être placé dans un état appelé Partiellement inscrit.

Cet état peut se produire si vous réenregistrez une unité d'organisation en appelant l'`ResetEnabledBaseline`API, car AWS Control Tower applique uniquement les ressources obligatoires aux comptes de l'unité d'organisation cible. Un compte qui ne dispose pas des ressources facultatives (contrôles) de son unité d'organisation parent est marqué comme étant partiellement inscrit.

Si vous déplacez un compte non inscrit vers une unité d'organisation enregistrée, puis que vous appelez l'`ResetEnabledBaseline`API de l'unité d'organisation pour inscrire ce compte, AWS Control Tower applique les ressources associées `AWSControlTowerBaseline` au compte nouvellement inscrit. Toutefois, les contrôles facultatifs activés pour cette unité d'organisation ne sont pas appliqués au compte. Le compte reste dans un état partiellement inscrit.

Pour inscrire complètement le compte, choisissez Réenregistrer ou Mettre à jour le compte dans la console. Lorsque vous sélectionnez ces opérations depuis la console, AWS Control Tower applique toutes les ressources de cette unité d'organisation au compte nouvellement inscrit, y compris les contrôles facultatifs activés pour cette unité d'organisation.

Variation des opérations entre la console AWS Control Tower et les API pour les lignes de base

Lorsque vous modifiez le statut de gouvernance d'une unité d'organisation, la console AWS Control Tower effectue automatiquement un plus grand nombre d'opérations pour vous, par rapport à une modification de la gouvernance au moyen des API pour les lignes de base.

Différences

- Enregistrement et approvisionnement de produits

  Lorsque vous enregistrez une UO via la console, AWS Control Tower crée des produits Service Catalog pour les comptes membres de l'UO, dans le cadre de l'inscription de chaque compte. Lorsque vous enregistrez une unité d'organisation par le biais de l'`EnableBaseline`API et qu'AWS Control Tower ne crée pas de produits provisionnés pour les comptes membres de l'unité d'organisation. `AWSControlTowerBaseline`
- Désenregistrer une UO

  Chaque fois que vous annulez l'enregistrement d'une unité d'organisation, vous devez d'abord supprimer tous les comptes membres et les unités d'organisation imbriquées. AWS Control Tower supprime ensuite tous les contrôles appliqués à l'unité d'organisation.
  - Si vous sélectionnez Supprimer l'UO de la console, AWS Control Tower procède au désenregistrement puis supprime l'UO de votre organisation.
  - Toutefois, si vous annulez l'enregistrement de l'UO en appelant l'`DisableBaseline`API pour la supprimer `AWSControlTowerBaseline` de l'UO, AWS Control Tower ne supprime pas l'UO de votre organisation, l'UO est toujours présente dans l'organisation, non enregistrée.

Valeurs de référence et paramètres de version par défaut

Si votre zone d'atterrissage AWS Control Tower est déjà configurée et que vous choisissez d'activer une ligne de base de zone d'atterrissage, AWS Control Tower active la dernière version de la ligne de base compatible avec votre version de zone d'atterrissage. Si vous choisissez d'activer une ligne de base pour une unité d'organisation qui n'est pas encore enregistrée auprès d'AWS Control Tower, AWS Control Tower fournit automatiquement la dernière version compatible de la ligne de base pour cette unité d'organisation.

Compatibilité des versions de base de l'UO et de la zone d'atterrissage

Les lignes de base d'AWS Control Tower vous permettent de définir une norme de gouvernance au niveau de l'unité organisationnelle, plutôt qu'au niveau de la zone de landing zone, si votre entreprise l'exige. La ligne de base appelée `AWSControlTowerBaseline` est disponible pour vous aider à enregistrer vos unités d'organisation auprès d'AWS Control Tower.

> **Note**
>
> Une base de référence est un ensemble de contrôles et de ressources qui fonctionnent ensemble pour établir un environnement de gouvernance stable au sein de votre zone d'atterrissage.

Lorsque vous activez une ligne de base sur une unité d'organisation, en appelant l'`EnableBaseline`API dans AWS Control Tower, vous devez spécifier une version de référence compatible avec votre version actuelle de la zone de landing zone d'AWS Control Tower. Une fois que vous avez spécifié une ligne de base, tous les comptes membres d'une unité d'organisation suivent la ligne de référence définie pour l'unité d'organisation. En d'autres termes, les nouveaux comptes sont approvisionnés avec la base de référence mise à jour, et les comptes des membres existants sont régis conformément à la nouvelle base de référence.

Si vous ne sélectionnez pas de référence pour vos unités d'organisation et comptes existants, la version de la zone d'atterrissage détermine par défaut l'ensemble de la posture de gouvernance. Cependant, chaque unité d'organisation enregistrée dans votre zone d'atterrissage se voit attribuer une version de référence, qui est la dernière version de référence compatible avec votre version de zone d'atterrissage actuelle. Par conséquent, chaque unité organisationnelle et chaque compte de membre inscrit sont associés à une référence, même si vous n'attribuez jamais de référence spécifique.

Pour la ligne de base au niveau de l'unité d'organisation`AWSControlTowerBaseline`, le tableau ci-dessous indique la compatibilité des lignes de base avec les versions de la zone de landing zone d'AWS Control Tower.

Version de référence	Versions de zone d'atterrissage	Plans inclus	Commandes incluses	Variation par rapport au niveau de référence précédent	
1.0	2,0 à 2,7	BP_BASELINE_CLOUDTRAIL, BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_ROLES, ressources IAM	Toutes les commandes obligatoires	Aucun	
2.0	2,8 à 2,9	BP_BASELINE_CLOUDTRAIL, BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_ROLES, Config SLR,	Toutes les commandes obligatoires	Ajout d'un rôle AWS Config lié au service (SLR) et d'un nouveau plan de configuration pour utiliser le SLR	

Version de référence	Versions de zone d'atterrissage	Plans inclus	Commandes incluses	Variation par rapport au niveau de référence précédent	
		ressources IAM			
3.0	3,0 à 3,1	BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_ROLES, Config SLR, ressources IAM	Toutes les commandes obligatoires	Nouveau AWS Config plan. Modifiez pour enregistrer les ressources mondiales uniquement dans la région d'origine. CloudTrail Plan supprimé	

Version de référence	Versions de zone d'atterrissage	Plans inclus	Commandes incluses	Variation par rapport au niveau de référence précédent	
4.0	3.2 à 3.3	BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_LINKED_ROLE, BP_BASELINE_SERVICE_ROLES, Config SLR, ressources IAM	Toutes les commandes obligatoires	Nouveau modèle SLR	

Pour plus d'informations sur les ressources spécifiques créées dans les comptes lorsque vous configurez votre zone de landing zone, consultez la section Ressources créées dans les comptes partagés.

Si vous mettez à jour votre zone d'atterrissage vers une version compatible avec une version de `AWSControlTowerBaseline` référence plus récente et que la nouvelle version de zone d'atterrissage est compatible avec votre version de référence existante, l'état de votre unité d'organisation passe à Mise à jour disponible.

- Vous pouvez continuer à utiliser Account Factory et les autres fonctionnalités sans mettre à jour immédiatement la ligne de base de l'unité d'organisation, sauf dans le cas d'une mise à jour de la zone d'atterrissage de la version 2.x à la version 3.x.

- Les nouveaux comptes inscrits à cette unité d'organisation reçoivent des ressources basées sur la version de base existante jusqu'à ce que la version de base soit mise à jour (avec la fonctionnalité de gouvernance étendue dans la console ou `UpdateEnabledBaseline` via l'API).
- Après avoir mis à jour la version de référence, tous les comptes de cette unité d'organisation reçoivent des ressources basées sur la nouvelle version de référence.

> **Note**
>
> Si vous mettez à jour votre zone de landing zone AWS Control Tower d'une version 2.X à une version 3.X, vous devez également mettre à jour la version de référence sur vos unités d'organisation, en raison du passage des pistes au niveau du compte à celles de l'organisation. AWS CloudTrail Dans la console, votre unité d'organisation affichera le statut « Mise à jour requise ».

Considérations relatives aux niveaux de référence

- Si votre unité d'organisation nécessite une mise à jour de base, vous ne pouvez pas créer de nouveaux comptes ni inscrire des comptes existants dans cette unité d'organisation.
- Après une mise à jour de la zone d'atterrissage, si vous prévoyez également de mettre à jour une ligne de base d'unité d'organisation, vous devez réenregistrer l'unité d'organisation ou mettre à jour la version de référence de votre unité d'organisation par programmation.
- Nous vous recommandons de passer à la ligne de base compatible la plus élevée pour la version de zone d'atterrissage que vous utilisez, afin de bénéficier de tous les avantages de la combinaison de la zone d'atterrissage et de la ligne de base. Par exemple, si vous passez à la version 3.3 de la zone d'atterrissage, vous pouvez continuer à utiliser la version de base 3.0, mais vous ne bénéficierez pas de tous les avantages de la version 3.3 de la zone d'atterrissage, sauf si vous passez également à la version de base 4.0.
- Les mises à jour de référence ne peuvent pas être annulées.
- L'activation de base cible une unité organisationnelle à la fois. Par conséquent, les unités d'organisation imbriquées ne sont pas mises à jour automatiquement lorsque l'unité d'organisation parent est mise à jour. Nous vous recommandons de mettre à jour l'unité d'organisation parent avant de mettre à jour les unités d'organisation imbriquées.

- Lorsque vous appelez l'`UpdateEnabledBaseline`API ou que vous réenregistrez une unité d'organisation depuis la console, l'unité d'organisation conserve tous les contrôles qui étaient activés avant la mise à jour de référence.
- Lorsque plusieurs versions de référence sont compatibles avec votre version de zone d'atterrissage, vous devez utiliser la dernière version de référence si vous activez une ligne de base sur une unité d'organisation non gérée.

Exemples : enregistrer une unité d'organisation AWS Control Tower avec des API uniquement

Cette présentation d'exemples est un document d'accompagnement. Pour des explications, des mises en garde et de plus amples informations, voir. Types de lignes de base

Prérequis

Vous devez disposer d'une unité d'organisation existante qui n'est pas enregistrée auprès d'AWS Control Tower et que vous souhaitez enregistrer. Vous devez également disposer d'une unité d'organisation enregistrée que vous souhaitez réenregistrer à des fins de mise à jour.

Enregistrer une UO

1. Vérifiez si le `IdentityCenterBaseline` est activé pour la zone d'atterrissage. Si tel est le cas, obtenez l'identifiant Identity Center Enabled Baseline.

```
aws controltower list-baselines --query 'baselines[?name==`IdentityCenterBaseline`].
[arn]'
```

```
aws controltower list-enabled-baselines --query 'enabledBaselines[?
baselineIdentifier==`<Identity Center Baseline Arn>`].[arn]'
```

2. Obtenez l'ARN de l'unité d'organisation cible.

```
aws organizations describe-organizational-unit --organizational-unit-id
 <Organizational Unit ID> --query 'OrganizationalUnit.[Arn]'
```

3. Obtenez l'ARN de la `AWSControlTowerBaseline` ligne de base.

```
aws controltower list-baselines --query 'baselines[?name==`AWSControlTowerBaseline`].
[arn]'
```

4. Créez la `AWSControlTowerBaseline` ligne de base sur l'unité d'organisation cible.

   Si l'Identity Center Baseline est activée :

```
aws controltower enable-baseline --baseline-identifier <AWSControlTowerBaseline ARN>
 --baseline-version <BASELINE VERSION> --target-identifier <OU ARN> --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"<Identity Center Enabled
 Baseline ARN>"}]'
```

   Si la ligne de base de référence du centre d'identité n'est pas activée, omettez l'*`parameters`*indicateur, comme suit :

```
aws controltower enable-baseline --baseline-identifier <AWSControlTowerBaseline ARN>
 --baseline-version <BASELINE VERSION> --target-identifier <OU ARN>
```

Réenregistrer une UO

Après avoir mis à jour les paramètres de la zone d'atterrissage ou mis à jour la version de votre zone d'atterrissage, vous devez réenregistrer les unités d'organisation pour leur apporter les dernières modifications. Procédez comme suit pour réenregistrer une unité d'organisation par programmation, en réinitialisant la ressource associée. `EnabledBaseline`

1. Obtenez l'ARN de l'unité d'organisation cible pour vous réenregistrer.

```
aws organizations describe-organizational-unit --organizational-unit-id <OU ID> --
query 'OrganizationalUnit.[Arn]'
```

2. Obtenez l'ARN de la `EnabledBaseline` ressource pour l'unité d'organisation cible.

```
aws controltower list-enabled-baselines --query 'enabledBaselines[?
targetIdentifier==`<OUARN>`].[arn]'
```

3. Réinitialisez la ligne de base activée.

```
aws controltower reset-enabled-baseline --enabled-baseline-
identifier <EnabledBaselineArn>
```

Exemples d'utilisation de l'API de base

Cette section contient des exemples de paramètres d'entrée et de sortie pour les API de base d'AWS Control Tower.

`DisableBaseline`

Pour plus d'informations sur cette opération d'API, consultez DisableBaseline.

`DisableBaseline`entrée :

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789"
}
```

`DisableBaseline`sortie :

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
}
```

`DisableBaseline`Exemple de CLI :

```
aws controltower disable-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789 \
    --region us-west-2
```

`EnableBaseline`

Pour plus d'informations sur cette opération d'API, consultez EnableBaseline.

`EnableBaseline`entrée :

```
{
```

```
    "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline:17BSJV3IGJ2QSGA2",
    "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/ou-
r9mj-4j3mzjql",
    "baselineVersion": "3.0",
    "parameters": [
        {
            "key": "IdentityCenterEnabledBaselineArn",
            "value": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
        }
    ]
}
```

`EnableBaseline`sortie :

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f",
    "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
}
```

`EnableBaseline`Exemple de CLI :

Cet exemple montre l'activation d'une base de référence pour une AWS Organizations organisation dont la zone de landing zone a opté pour l'accès à l' AWS IAM Identity Center, géré par AWS Control Tower. Pour récupérer votre `EnabledBaseline` identifiant Identity Center, vous pouvez appeler l'`ListEnabledBaselines`API en filtrant sur la base de référence Identity Center : `(arn:aws:controltower:`*`Region`*`::baseline/LN25R72TTG6IGPTQ)`

```
aws controltower list-enabled-baselines \
    --filter baselineIdentifiers=arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ \
    --region us-west-2
```

La réponse affichera le `EnabledBaseline` détail, qui indique son identifiant.

```
{
    "enabledBaselines": [
        {
            "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHXS7P6C4I453EZC",
```

```
            "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ",
            "targetIdentifier": "arn:aws:organizations::123456789012:account/o-
aq21sw43de5/123456789012",
            "statusSummary": {
                "status": "SUCCEEDED"
            }
        }
    ]
}
```

> **Note**
>
> Notez la valeur ARN de la réponse et transmettez-la en paramètre pour activer la ligne de base par défaut.

```
aws controltower enable-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --baseline-version 3.0 \
    --target-identifier arn:aws:organizations::123456789012:ou/o-aq21sw43de5/ou-po90-
lk87jh65 \
    --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC"}]' \
    --region us-west-2
```

Pour une organisation dont la zone d'atterrissage est exclue de la gestion d'IAM Identity Center par AWS Control Tower, activez la ligne de base sans le paramètre.

```
aws controltower enable-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --baseline-version 3.0 \
    --target-identifier arn:aws:organizations::123456789012:ou/o-aq21sw43de5/ou-po90-
lk87jh65 \
    --region us-west-2
```

`GetBaseline`

Pour plus d'informations sur cette opération d'API, consultez GetBaseline.

`GetBaseline`entrée :

```
{
    "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2"
}
```

`GetBaseline`sortie :

```
{
    "arn": "arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2",
    "name": "AWSControlTowerBaseline",
    "description": "Sets up resources and mandatory controls for member accounts within
 the target OU, required for AWS Control Tower governance.",
}
```

`GetBaseline`Exemple de CLI :

```
aws controltower get-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --region us-west-2
```

`GetBaselineOperation`

Pour plus d'informations sur cette opération d'API, consultez GetBaselineOperation.

`GetBaselineOperation`entrée :

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
}
```

`GetBaselineOperation`sortie :

```
{
    "baselineOperation": {
        "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f",
        "operationType": "DISABLE_BASELINE",
        "status": "FAILED",
        "startTime": "2023-01-12T19:05:00Z",
        "endTime": "2023-01-12T19:45:00Z",
```

```
        "statusMessage": "Can't perform DisableBaseline on a parent target with
 governed child OUs"
    }
}
```

`GetBaselineOperation`Exemple de CLI :

```
aws controltower get-baseline-operation \
    --operation-identifier 58f12232-26be-4735-a3e9-dd30d90f021f \
    --region us-west-2
```

`GetEnabledBaseline`

Pour plus d'informations sur cette opération d'API, consultez GetEnabledBaseline.

`GetEnabledBaseline`entrée :

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHCR4CJTSI4W07MZ"
}
```

`GetEnabledBaseline`sortie :

```
{
    "enabledBaselineDetails": {
        "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ",
        "baselineIdentifier": "arn:aws:controltower:us-
west-2::baseline:17BSJV3IGJ2QSGA2",
        "baselineVersion": "3.0",
        "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/ou-
r9mj-4j3mzjql",
        "statusSummary": {
            "status": "SUCCEEDED",
            "lastOperationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
        },
        "parameters": [
            {
                "key": "IdentityCenterEnabledBaselineArn",
                "value": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
```

```
            }
        ]
    }
}
```

`GetEnabledBaseline`Exemple de CLI :

```
aws controltower get-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
    --region us-west-2
```

`ListBaselines`

Pour plus d'informations sur cette opération d'API, consultez ListBaselines.

`ListBaselines`entrée (en utilisant des entrées optionnelles) :

```
{
    "nextToken": "AbCd1234",
    "maxResults": "4"
}
```

`ListBaselines`sortie :

```
{
    "baselines": [
        {
            "arn": "arn:aws:controltower:us-west-1::baseline/4T4HA1KMO10S6311",
            "name": "AuditBaseline",
            "description": "Sets up resources to monitor security and compliance of
 accounts in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-west-1::baseline/J8HX46AHS5MIKQPD",
            "name": "LogArchiveBaseline",
            "description": "Sets up a central repository for logs of API activities and
 resource configurations from accounts in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-west-1::baseline/LN25R72TTG6IGPTQ",
            "name": "IdentityCenterBaseline",
```

```
            "description": "Sets up shared resources for AWS Identity Center, which
 prepares the AWSControlTowerBaseline to set up Identity Center access for accounts."
        },
        {
            "arn": "arn:aws:controltower:us-west-1::baseline/17BSJV3IGJ2QSGA2",
            "name": "AWSControlTowerBaseline",
            "description": "Sets up resources and mandatory controls for member
 accounts within the target OU, required for AWS Control Tower governance."
        }
    ]
}
```

`ListBaselines`Exemple de CLI :

```
aws controltower list-baselines \
    --region us-west-2
```

`ListEnabledBaselines`

Pour plus d'informations sur cette opération d'API, consultez ListEnabledBaselines.

`ListEnabledBaselines`entrée (aucun filtre) :

```
{
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

`ListEnabledBaselines`entrée (`baselineIdentifiers`filtre uniquement) :

```
{
    "filter": {
        "baselineIdentifiers": ['arn:aws:controltower:us-
east-1::baseline/17BSJV3IGJ2QSGA2', 'arn:aws:controltower:us-
east-1::baseline/12GZU8CKZKVMS2AW']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

`ListEnabledBaselines`entrée (`targetIdentifiers`filtre uniquement) :

```
{
    "filter": {
        "targetIdentifiers": ['arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-
xqj7-fex1u317', 'arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-xqj7-11q6n2cf']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 2
}
```

`ListEnabledBaselines`entrée (`baselineIdentifier`set `targetIdentifiers` filtres) :

```
{
    "filter": {
        "baselineIdentifiers": ['arn:aws:controltower:us-
east-1::baseline/17BSJV3IGJ2QSGA2']
        "targetIdentifiers": ['arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-
xqj7-fex1u317']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

`ListEnabledBaselines`sortie :

```
{
    "enabledBaselines": [
        {
            "arn": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ",
            "baselineIdentifier": "arn:aws:controltower:us-
east-1::baseline:17BSJV3IGJ2QSGA2",
            "baselineVersion": "3.0",
            "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/
ou-r9mj-4j3mzjql",
            "statusSummary": {
                "status": "SUCCEEDED",
                "lastOperationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
            }
        },
        {
            "arn": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAJ9NKW88AA4W9CLL",
```

```
            "baselineIdentifier": "arn:aws:controltower:us-
east-1::baseline:17BSJV3IGJ2QSGA2",
            "baselineVersion": "4.0",
            "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-s9511vn103/
ou-xqj7-fex1u317",
            "statusSummary": {
            "status": "FAILED",
                "lastOperationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
            }
        }
    ],
    "nextToken": "e2bXXXXX6cab"
}
```

Exemple de CLI avec un type de filtre (`baselineIdentifiers`filtre) :

```
aws controltower list-enabled-baselines \
    --filter baselineIdentifiers=arn:aws:controltower:us-
west-2::baseline/17BSJV3IGJ2QSGA2,arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ \
    --region us-west-2
```

Exemple de CLI utilisant plusieurs filtres (`baselineIdentifier`set `targetIdentifiers` filtres) :

```
aws controltower list-enabled-baselines \
    --filter targetIdentifiers=arn:aws:organizations::123456789012:ou/o-
aq21sw43de5/ou-po90-lk87jh65,baselineIdentifiers=arn:aws:controltower:us-
west-2::baseline/17BSJV3IGJ2QSGA2 \
    --region us-west-2
```

`ResetEnabledBaseline`

Pour plus d'informations sur cette opération d'API, consultez ResetEnabledBaseline.

`ResetEnabledbaselineentrée` :

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAJ9NKW88AA4W9CLL"
}
```

`ResetEnabledBaselinesortie` :

```
{
    "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

`ResetEnabledBaseline`Exemple de CLI :

```
aws controltower reset-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
    --region us-west-2
```

`UpdateEnabledBaseline`

Pour plus d'informations sur cette opération d'API, consultez UpdateEnabledBaseline.

`UpdateEnabledBaseline`entrée :

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
east-1:123456789012:enabledbaseline/XAJ9NKW88AA4W9CLL",
    "baselineVersion": "4.0",
    "parameters": [
        {
            "key": "IdentityCenterEnabledBaselineArn",
            "value": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
        }
    ]
}
```

`UpdateEnabledBaseline`sortie :

```
{
    "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

`UpdateEnabledBaseline`Exemple de CLI :

```
aws controltower update-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
```

```
    --baseline-version 4.0
    --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC"}]' \
    --region us-west-2
```

Informations connexes

Cette rubrique répertorie les cas d'utilisation courants et les meilleures pratiques concernant les fonctionnalités d'AWS Control Tower ainsi que les améliorations supplémentaires. Cette rubrique inclut également des liens vers des articles de blog pertinents, de la documentation technique et des ressources connexes qui peuvent vous aider dans votre travail avec AWS Control Tower.

Tutoriels et ateliers

- Laboratoire AWS Control Tower : ces ateliers fournissent une vue d'ensemble détaillée des tâches courantes liées à AWS Control Tower.
- Sur le tableau de bord d'AWS Control Tower, choisissez Get custom guidance si vous avez un cas d'utilisation en tête mais que vous ne savez pas par où commencer.
- Consultez une liste de YouTube vidéos qui expliquent en détail comment utiliser les fonctionnalités d'AWS Control Tower.

Réseaux

Configurez des modèles répétables et gérables pour les réseaux dans. AWS Apprenez-en davantage sur la conception, l'automatisation et les appareils couramment utilisés par les clients.

- AWS Architecture VPC de démarrage rapide : ce guide de démarrage rapide fournit une base réseau basée sur les AWS meilleures pratiques pour votre infrastructure AWS cloud. Il crée un AWS Virtual Private Network environnement avec des sous-réseaux publics et privés dans lequel vous pouvez lancer AWS des services et d'autres ressources.
- VPC en libre-service dans AWS Control Tower à l'aide d'AWS Service Catalog — Ce billet de blog décrit comment configurer Account Factory afin que vous puissiez approvisionner des comptes avec des VPC personnalisés.
- Implémentation du Serverless Transit Network Orchestrator (STNO) dans AWS Control Tower — Ce billet de blog explique comment automatiser l'accès à la connectivité réseau entre les comptes. Ce blog est destiné aux administrateurs d'AWS Control Tower ou aux personnes chargées de gérer les réseaux au sein de leur AWS environnement.

Sécurité, identité et journalisation

Élargissez votre niveau de sécurité, intégrez des fournisseurs d'identité externes ou existants et centralisez les systèmes de journalisation.

Sécurité

- Automatisation des AWS Security Hub alertes avec les événements du cycle de vie d'AWS Control Tower — Ce billet de blog explique comment automatiser l'activation et la configuration de Security Hub dans un environnement multi-comptes AWS Control Tower sur des comptes existants et nouveaux.
- Activation AWS Identity and Access Management : ce billet de blog explique comment améliorer la visibilité de votre organisation en matière de sécurité en activant et en centralisant les résultats d'IAM Access Analyzer.
- AWS Systems Manager Parameter Store fournit un stockage hiérarchique sécurisé pour la gestion des données de configuration et la gestion des secrets. Vous pouvez l'utiliser pour partager des informations de configuration dans un emplacement sécurisé, à l'usage d'AWS Systems Manager et d'AWS CloudFormation. Par exemple, vous pouvez stocker une liste des régions dans lesquelles vous souhaitez déployer des packs de conformité.

Identité

- Associez l'identité utilisateur d'Azure AD à AWS des comptes et à des applications pour l'authentification unique — Ce billet de blog explique comment utiliser Azure AD avec IAM Identity Center et AWS Control Tower.
- Gérez l'accès à AWS de manière centralisée pour les utilisateurs d'Okta avec AWS IAM Identity Center — Ce billet de blog explique comment utiliser Okta avec IAM Identity Center et AWS Control Tower.

Journalisation

- AWS Solution de journalisation centralisée — Cet article décrit la solution de journalisation centralisée qui permet aux entreprises de collecter, d'analyser et d'afficher les journaux sur AWS plusieurs comptes et AWS régions.

Déploiement des ressources et gestion des charges de travail

Déployez et gérez les ressources et les charges de travail.

- Intégration de la bibliothèque Getting Started — Ce billet de blog décrit les portefeuilles Getting Started que vous pouvez utiliser.
- Déploiement continu de Cloud Custodian sur AWS Control Tower

Travailler avec des organisations et des comptes existants

Travaillez avec des AWS organisations et des comptes existants.

- Création d'un compte : cette rubrique du guide de l'utilisateur explique comment inscrire un AWS compte existant dans AWS Control Tower.
- Créez un compte dans le cadre d'AWS Control Tower — Ce billet de blog explique comment déployer AWS Control Tower dans vos AWS organisations existantes.
- Étendez la gouvernance d'AWS Control Tower à l'aide des packs de conformité AWS Config — Ce billet de blog explique comment déployer des packs de AWS Config conformité pour aider à intégrer les comptes et les organisations existants à la gouvernance par AWS Control Tower.
- Comment détecter et atténuer les violations de garde-corps avec AWS Control Tower — Ce billet de blog explique comment ajouter des contrôles et comment s'abonner aux notifications SNS afin d'être averti par e-mail des violations de conformité aux contrôles.

Automatisation et intégration

Automatisez la création de comptes et intégrez les événements du cycle de vie à AWS Control Tower.

- Événements du cycle de vie — Ce billet de blog explique comment utiliser les événements du cycle de vie avec AWS Control Tower.
- Automatiser la création de comptes — Ce billet de blog explique comment configurer la création automatique de comptes dans AWS Control Tower.
- Automatisation des journaux de flux Amazon VPC — Ce billet de blog explique comment automatiser et centraliser les journaux de flux Amazon VPC dans un environnement multi-comptes.

- Automatisez le balisage des VPC avec les événements du cycle de vie d'AWS Control Tower — Ce billet de blog explique comment automatiser le balisage des ressources pour les VPC, au moyen d'événements du cycle de vie dans AWS Control Tower.
- Gestion automatisée des comptes : ce billet de blog explique comment automatiser les tâches de gestion des comptes une fois votre environnement AWS Control Tower configuré.

Migration des charges de travail

Utilisez d'autres AWS services avec AWS Control Tower pour faciliter la migration de la charge de travail.

- CloudEndure migration — Ce billet de blog explique comment combiner CloudEndure d'autres AWS services avec AWS Control Tower pour faciliter la migration de la charge de travail.

Services AWS connexes

AWS Control Tower agit comme une couche d'orchestration pour AWS Organizations. Par conséquent, grâce à la console AWS Organizations et aux API, vous avez accès à plus de 20 autres services AWS qui fonctionnent avec AWS Control Tower. Ces services supplémentaires ne sont pas accessibles directement via la console AWS Control Tower.

- Pour obtenir la liste complète des services mis à la disposition d'AWS Control Tower par le biais d'AWS Organizations, consultez les services AWS que vous pouvez utiliser avec AWS Organizations.
- Pour activer les fonctionnalités multi-comptes pour ces services AWS connexes, vous devez activer l'accès sécurisé. Pour plus d'informations, consultez la section Utilisation d'AWS Organizations avec d'autres services AWS.

> **Note**
>
> N'oubliez pas que AWS IAM Identity Center et IAM AWS CloudTrail sont configurés pour vous dans AWS Control Tower et qu'ils sont entièrement intégrés. AWS Config Il n'est pas nécessaire de modifier vos paramètres d'accès sécurisé ou d'administration déléguée pour ces services.

- Certains AWS services disponibles via AWS AWS Organizations peuvent utiliser l'administration déléguée, notamment AWS Systems Manager et AWS Firewall Manager. Pour plus d'informations, consultez Configuration d'un administrateur délégué et Activation d'un compte d'administrateur délégué pour Firewall Manager. Regardez également cette vidéo intitulée Configurer des groupes de sécurité avec AWS Firewall Manager.

AWS Marketplace solutions

Découvrez les solutions de AWS Marketplace.

- AWS Control Tower Marketplace : AWS Marketplace propose une large gamme de solutions pour AWS Control Tower afin de vous aider à intégrer des logiciels tiers. Ces solutions aident à résoudre les principaux cas d'utilisation de l'infrastructure et des opérations, notamment la gestion des identités, la sécurité d'un environnement multi-comptes, la mise en réseau centralisée, le renseignement opérationnel et la gestion des informations et des événements de sécurité (SIEM).

Notes de mise à jour d'AWS Control Tower

Les sections suivantes présentent des informations détaillées sur les versions d'AWS Control Tower qui nécessitent une mise à jour pour une zone d'atterrissage d'AWS Control Tower, ainsi que sur les versions qui sont automatiquement intégrées au service.

Les fonctionnalités et les versions sont répertoriées par ordre chronologique inverse (les plus récentes en premier) en fonction de la date à laquelle elles ont été officiellement annoncées au public. Comme il peut y avoir un décalage entre le moment où la fonctionnalité ou la version est documentée et le moment où elle est officiellement annoncée, la date indiquée pour une fonctionnalité ou une version ici peut légèrement différer de la date indiquée dans leHistorique du document.

Fonctionnalités publiées en 2024

Fonctionnalités publiées en 2023

Fonctionnalités publiées en 2022

Fonctionnalités publiées en 2021

Fonctionnalités publiées en 2020

Fonctionnalités publiées en 2019

Janvier 2024 - En cours

Depuis janvier 2024, AWS Control Tower a publié les mises à jour suivantes :

- AWS Control Tower prend en charge jusqu'à 100 opérations de contrôle simultanées
- AWS Control Tower est disponible dans l'ouest AWS du Canada (Calgary)
- AWS Control Tower prend en charge les ajustements de quotas en libre-service
- AWS Control Tower publie le guide de référence sur les contrôles
- AWS Control Tower met à jour et renomme deux contrôles proactifs
- Les contrôles obsolètes ne sont plus disponibles
- AWS Control Tower prend en charge le balisage des `EnabledControl` ressources dans AWS CloudFormation

- AWS Control Tower prend en charge les API pour l'enregistrement et la configuration des unités d'organisation avec des lignes de base

AWS Control Tower prend en charge jusqu'à 100 opérations de contrôle simultanées

20 mai 2024

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower prend désormais en charge plusieurs opérations de contrôle avec une plus grande simultanéité. Vous pouvez soumettre jusqu'à 100 opérations de contrôle AWS Control Tower, dans plusieurs unités organisationnelles (UO), en même temps, depuis la console ou via des API. Jusqu'à dix (10) opérations peuvent être exécutées simultanément, et les opérations supplémentaires sont mises en file d'attente. De cette façon, vous pouvez configurer une configuration plus standardisée sur plusieurs Comptes AWS, sans la charge opérationnelle liée aux opérations de contrôle répétitives.

Pour surveiller l'état de vos opérations de contrôle en cours et en file d'attente, vous pouvez accéder à la nouvelle page des opérations récentes dans la console AWS Control Tower, ou vous pouvez appeler la nouvelle `ListControlOperations`API.

La bibliothèque AWS Control Tower contient plus de 500 contrôles, qui correspondent à différents objectifs, frameworks et services de contrôle. Pour un objectif de contrôle spécifique, tel que le chiffrement des données au repos, vous pouvez activer plusieurs contrôles en une seule opération de contrôle, afin de vous aider à atteindre l'objectif. Cette fonctionnalité facilite le développement accéléré, permet une adoption plus rapide des meilleures pratiques de contrôle et atténue les complexités opérationnelles.

AWS Control Tower est disponible dans l'ouest AWS du Canada (Calgary)

3 mai 2024

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

À compter d'aujourd'hui, vous pouvez activer AWS Control Tower dans la région du Canada Ouest (Calgary). Si vous avez déjà déployé AWS Control Tower et que vous souhaitez étendre ses fonctionnalités de gouvernance à cette région, vous pouvez le faire avec les API de zone de landing

zone d'AWS Control Tower. Ou depuis la console, rendez-vous sur la page Paramètres de votre tableau de bord AWS Control Tower, sélectionnez vos régions, puis mettez à jour votre zone de landing zone.

La région du Canada Ouest (Calgary) ne soutient pas AWS Service Catalog. C'est pourquoi certaines fonctionnalités d'AWS Control Tower sont différentes. Le changement de fonctionnalité le plus notable est que Account Factory n'est pas disponible. Si vous choisissez Canada-Ouest (Calgary) comme région d'origine, les procédures de mise à jour des comptes, de configuration des automatisations des comptes et de tout autre processus impliquant Service Catalog sont différentes de celles des autres régions.

Comptes de provisionnement

Pour créer et approvisionner un nouveau compte dans la région du Canada Ouest (Calgary), nous vous recommandons de créer un compte en dehors d'AWS Control Tower, puis de l'inscrire dans une unité d'organisation enregistrée. Pour plus d'informations, consultez les sections Inscription d'un compte existant et Étapes pour créer un compte.

Les API Service Catalog ne sont pas disponibles dans la région du Canada Ouest (Calgary). L'exemple de script présenté dans Automatiser le provisionnement des comptes dans AWS Control Tower par les API Service Catalog n'est pas réalisable.

Account Factory Customizations (AFC), Account Factory for Terraform (AFT) et Customizations for AWS Control Tower (CfCT) ne sont pas disponibles dans l'ouest du Canada (Calgary), en raison de l'absence d'autres dépendances sous-jacentes pour AWS Control Tower. Si vous étendez la gouvernance à la région du Canada-Ouest (Calgary), vous pouvez continuer à gérer les plans AFC dans toutes les régions prises en charge par AWS Control Tower, à condition que Service Catalog soit disponible dans votre région d'origine.

Contrôles

Les contrôles proactifs et les contrôles conformes à la norme AWS Security Hub de gestion des services : AWS Control Tower ne sont pas disponibles dans la région du Canada-Ouest (Calgary). Le contrôle préventif n'`CT.CLOUDFORMATION.PR.1`est pas disponible dans le Canada-Ouest (Calgary) car il n'est nécessaire que pour activer les contrôles proactifs basés sur des crochets. Certaines commandes de détection basées sur ne AWS Config sont pas disponibles. Pour plus de détails, consultez Limites de contrôle.

Fournisseur d'identité

Le centre d'identité IAM n'est pas disponible dans l'ouest du Canada (Calgary). La meilleure pratique recommandée est de configurer votre zone de landing zone dans une région où le centre d'identité IAM est disponible. Vous avez également la possibilité de gérer vous-même la configuration de l'accès à votre compte si vous utilisez un fournisseur d'identité externe à Canada-Ouest (Calgary).

L'indisponibilité du Service Catalog dans la région du Canada Ouest (Calgary) n'a aucun effet sur les autres régions prises en charge par AWS Control Tower. Ces différences s'appliquent uniquement si votre région d'origine est le Canada-Ouest (Calgary).

Pour obtenir la liste complète des régions dans lesquelles AWS Control Tower est disponible, consultez le tableau des AWS régions.

AWS Control Tower prend en charge les ajustements de quotas en libre-service

25 avril 2024

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower prend désormais en charge les ajustements de quotas en libre-service via la console Service Quotas. Pour plus d'informations, consultez Demander une augmentation de quota.

AWS Control Tower publie le guide de référence sur les contrôles

21 avril 2024

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower a publié le Controls Reference Guide, un nouveau document dans lequel vous pouvez trouver des informations détaillées sur les contrôles spécifiques à l'environnement AWS Control Tower. Ce matériel figurait auparavant dans le guide de l'utilisateur d'AWS Control Tower. Le guide de référence sur les contrôles couvre les contrôles dans un format étendu. Pour plus d'informations, consultez le guide de référence d'AWS Control Tower Controls.

AWS Control Tower met à jour et renomme deux contrôles proactifs

26 mars 2024

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower a renommé deux contrôles proactifs afin de les aligner sur les mises à jour d'Amazon OpenSearch Service.

- [CT.OPENSEARCH.PR.8] Nécessite un domaine Elasticsearch Service pour utiliser TLSv1.2
- [CT.OPENSEARCH.PR.16] Exiger un domaine Amazon OpenSearch Service pour utiliser TLSv1.2

Nous avons mis à jour les noms de contrôle et les artefacts de ces deux contrôles afin de les aligner sur la récente version d'Amazon OpenSearch Service, qui prend désormais en charge la version 1.3 de Transport Layer Security (TLS) parmi ses options de sécurité du transport pour la sécurité des points de terminaison de domaine.

Pour ajouter la prise en charge de TLSv1.3 pour ces contrôles, nous avons mis à jour l'artefact et le nom des contrôles afin de refléter l'intention du contrôle. Ils évaluent désormais la version TLS minimale du domaine de service. Pour effectuer cette mise à jour dans votre environnement, vous devez désactiver et activer les commandes permettant de déployer le dernier artefact.

Aucun autre contrôle proactif n'est affecté par cette modification. Nous vous recommandons de passer en revue ces contrôles afin de vous assurer qu'ils répondent à vos objectifs de contrôle.

Pour toute question ou préoccupation, contactez AWS le Support.

Les contrôles obsolètes ne sont plus disponibles

12 mars 2024

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower a déconseillé certains contrôles. Ces commandes ne sont plus disponibles.

- CT.ATHENA.PR.1
- CT.CODEBUILD.PR.4
- CT.AUTOSCALING.PR.3
- SH.Athena.1
- SH.Codebuild.5
- SH.AutoScaling.4
- SH.SNS.1
- SH.SNS.2

AWS Control Tower prend en charge le balisage des **EnabledControl** ressources dans AWS CloudFormation

22 février 2024

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

Cette version d'AWS Control Tower met à jour le comportement de la `EnabledControl` ressource, afin de mieux l'aligner sur les contrôles configurables et d'améliorer la capacité à gérer votre environnement AWS Control Tower grâce à l'automatisation. Avec cette version, vous pouvez ajouter des balises aux `EnabledControl` ressources configurables au moyen de AWS CloudFormation modèles. Auparavant, vous pouviez ajouter des balises uniquement via la console AWS Control Tower et les API.

Les opérations AWS Control Tower `GetEnabledControl` et `ListTagsforResource` API sont mises à jour avec cette version, car elles reposent sur les fonctionnalités `EnabledControl` des ressources. `EnableControl`

Pour plus d'informations, consultez les `EnabledControl`ressources de balisage dans AWS Control Tower et `EnabledControl`dans le guide de l'AWS CloudFormation utilisateur.

AWS Control Tower prend en charge les API pour l'enregistrement et la configuration des unités d'organisation avec des lignes de base

14 février 2024

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

Ces API prennent en charge l'enregistrement programmatique de l'unité d'organisation lors de l'`EnableBaseline`appel. Lorsque vous activez une base de référence sur une unité d'organisation, les comptes des membres de l'unité d'organisation sont inscrits dans la gouvernance d'AWS Control Tower. Certaines mises en garde peuvent s'appliquer. Par exemple, l'enregistrement de l'unité d'organisation via la console AWS Control Tower permet des contrôles facultatifs ainsi que des contrôles obligatoires. Lorsque vous appelez des API, il se peut que vous deviez effectuer une étape supplémentaire afin que les commandes facultatives soient activées.

Une base de référence AWS Control Tower intègre les meilleures pratiques relatives à la gouvernance par AWS Control Tower d'une unité d'organisation et de comptes de membres. Par

exemple, lorsque vous activez une base de référence sur une unité d'organisation, les comptes membres de l'unité d'organisation reçoivent un groupe défini de ressources AWS CloudTrail AWS Config, notamment le centre d'identité IAM et les rôles AWS IAM requis.

Les lignes de base spécifiques sont compatibles avec les versions spécifiques de la zone d'atterrissage d'AWS Control Tower. AWS Control Tower peut appliquer la dernière ligne de base compatible à votre zone d'atterrissage lorsque vous modifiez les paramètres de cette dernière. Pour plus d'informations, consultez Compatibilité des versions de base de l'UO et de la zone d'atterrissage.

Cette version inclut quatre éléments essentiels Types de lignes de base

- `AWSControlTowerBaseline`
- `AuditBaseline`
- `LogArchiveBaseline`
- `IdentityCenterBaseline`

Grâce aux nouvelles API et aux lignes de base définies, vous pouvez enregistrer des unités d'organisation et automatiser votre flux de travail de provisionnement des unités d'organisation. Les API peuvent également gérer les unités d'organisation déjà soumises à la gouvernance d'AWS Control Tower. Vous pouvez donc réenregistrer les unités d'organisation après les mises à jour de la zone de landing zone. Les API incluent la prise en charge d'une AWS CloudFormation `EnabledBaseline` ressource, qui vous permet de gérer vos unités d'organisation à l'aide de l'infrastructure sous forme de code (IaC).

API de base

- EnableBaseline, UpdateEnabledBaseline, DisableBaseline: Agissez sur une ligne de base pour une unité d'organisation.
- GetEnabledBaseline, ListEnabledBaselines: Découvrez les configurations pour vos lignes de base activées.
- GetBaselineOperation: permet d'afficher le statut d'une opération de référence spécifique.
- ResetEnabledBaseline: Corrigez la dérive des ressources sur une unité d'organisation avec une ligne de base activée (y compris les unités d'organisation imbriquées et la dérive de contrôle obligatoire). Corrige également la dérive pour la landing-zone-level Région, refuse le contrôle
- GetBaseline, ListBaselines: Découvrez le contenu des lignes de base d'AWS Control Tower.

Pour en savoir plus sur ces API, consultez les lignes de base du guide de l'utilisateur d'AWS Control Tower et le guide de référence des API. Les nouvelles API sont disponibles Régions AWS là où AWS Control Tower est disponible, à l'exception des régions GovCloud (États-Unis). Pour une liste des Régions AWS endroits où AWS Control Tower est disponible, consultez le Région AWS tableau.

Janvier 2023 - En cours

Depuis janvier 2023, AWS Control Tower a publié les mises à jour suivantes :

- Transition vers un nouveau type de produit AWS Service Catalog externe (phase 3)
- Zone de landing zone d'AWS Control Tower, version 3.3
- Transition vers un nouveau type de produit AWS Service Catalog externe (phase 2)
- AWS Control Tower annonce des contrôles destinés à renforcer la souveraineté numérique
- AWS Control Tower prend en charge les API de zone d'atterrissage
- AWS Control Tower prend en charge le balisage pour les contrôles activés
- AWS Control Tower est disponible dans la région Asie-Pacifique (Melbourne)
- Transition vers un nouveau type de produit AWS Service Catalog externe (phase 1)
- Nouvelle API de contrôle disponible
- AWS Control Tower ajoute des contrôles supplémentaires
- Nouveau type de dérive signalé : accès sécurisé désactivé
- Quatre supplémentaires Régions AWS
- AWS Control Tower est disponible dans la région de Tel Aviv
- AWS Control Tower lance 28 nouveaux contrôles proactifs
- AWS Control Tower déconseille deux contrôles
- Zone de landing zone d'AWS Control Tower, version 3.2
- AWS Control Tower gère les comptes en fonction de leur identifiant
- Contrôles de détection supplémentaires du Security Hub disponibles dans la bibliothèque de contrôles AWS Control Tower
- AWS Control Tower publie des tables de métadonnées de contrôle
- Support de Terraform pour la personnalisation d'Account Factory
- AWS L'autogestion de l'IAM Identity Center est disponible pour la zone de landing zone
- AWS Control Tower résout le problème de la gouvernance mixte pour les unités d'organisation

- Contrôles proactifs supplémentaires disponibles
- Contrôles proactifs Amazon EC2 mis à jour
- Sept autres Régions AWS disponibles
- Suivi des demandes de personnalisation du compte Account Factory for Terraform (AFT)
- Zone de landing zone d'AWS Control Tower, version 3.1
- Contrôles proactifs généralement disponibles

Transition vers un nouveau type de produit AWS Service Catalog externe (phase 3)

14 décembre 2023

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower ne prend plus en charge Terraform Open Source en tant que type de produit (plan directeur) lors de la création de nouveaux produits. Comptes AWS Pour plus d'informations et pour obtenir des instructions sur la mise à jour des plans de votre compte, consultez la section Transition vers le type de produit AWS Service Catalog externe.

Si vous ne mettez pas à jour les plans de votre compte pour utiliser le type de produit externe, vous ne pouvez mettre à jour ou résilier que les comptes que vous avez provisionnés à l'aide des plans Open Source Terraform.

Zone de landing zone d'AWS Control Tower, version 3.3

14 décembre 2023

(Mise à jour requise pour la zone de landing zone d'AWS Control Tower vers la version 3.3. Pour plus d'informations, voirMettre à jour votre zone de destination).

Mises à jour de la politique relative aux compartiments S3 dans le compte AWS Control Tower Audit

Nous avons modifié la politique du bucket Amazon S3 Audit qu'AWS Control Tower déploie dans les comptes, de sorte qu'une `aws:SourceOrgID` condition doit être remplie pour toute autorisation d'écriture. Avec cette version, les AWS services ont accès à vos ressources uniquement lorsque la demande provient de votre organisation ou unité organisationnelle (UO).

Vous pouvez utiliser la clé de `aws:SourceOrgID` condition et définir la valeur en fonction de l'ID de votre organisation dans l'élément condition de votre politique de compartiment S3. Cette condition

garantit que CloudTrail seuls les journaux peuvent être écrits pour le compte de comptes au sein de votre organisation dans votre compartiment S3 ; elle empêche CloudTrail les journaux extérieurs à votre organisation d'écrire dans votre compartiment AWS Control Tower S3.

Nous avons apporté cette modification pour corriger une faille de sécurité potentielle, sans affecter le fonctionnement de vos charges de travail existantes. Pour consulter la politique mise à jour, voirPolitique relative au compartiment Amazon S3 dans le compte d'audit.

Pour plus d'informations sur la nouvelle clé de condition, consultez la documentation IAM et le billet de blog IAM intitulé « Utiliser des contrôles évolutifs pour les AWS services accédant à vos ressources ».

Mises à jour de la politique dans la AWS Config rubrique SNS

Nous avons ajouté la nouvelle clé de `aws:SourceOrgID` condition à la politique du sujet AWS Config SNS. Pour consulter la politique mise à jour, consultez la politique du AWS Config sujet SNS.

Mises à jour de la zone d'atterrissage : Region Deny control

- Supprimé`discovery-marketplace:`. Cette action est couverte par l'`aws-marketplace:*`exemption.
- Ajout de `quicksight:DescribeAccountSubscription`.

AWS CloudFormation Modèle mis à jour

Nous avons mis à jour le AWS CloudFormation modèle de la pile nommée `BASELINE-CLOUDTRAIL-MASTER` afin qu'elle ne montre pas de dérive lorsque AWS KMS le chiffrement n'est pas utilisé.

Transition vers un nouveau type de produit AWS Service Catalog externe (phase 2)

7 décembre 2023

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

HashiCorp a mis à jour leur licence Terraform. En conséquence, le support des produits Open Source de Terraform AWS Service Catalog a été modifié et les produits ont été approvisionnés en un nouveau type de produit, appelé External.

Pour éviter toute interruption des charges de travail et AWS des ressources existantes dans vos comptes, suivez les étapes de transition d'AWS Control Tower dans Transition vers le type de produit AWS Service Catalog externe d'ici le 14 décembre 2023.

AWS Control Tower annonce des contrôles destinés à renforcer la souveraineté numérique

27 novembre 2023

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower annonce 65 nouveaux contrôles AWS gérés, pour vous aider à répondre à vos exigences en matière de souveraineté numérique. Dans cette version, vous pouvez découvrir ces contrôles dans le cadre d'un nouveau groupe de souveraineté numérique dans la console AWS Control Tower. Vous pouvez utiliser ces contrôles pour empêcher les actions et détecter les modifications des ressources concernant la résidence des données, la restriction d'accès granulaire, le chiffrement et les capacités de résilience. Ces contrôles sont conçus pour vous permettre de répondre plus facilement aux exigences à grande échelle. Pour plus d'informations sur les contrôles de souveraineté numérique, voir Contrôles qui améliorent la protection de la souveraineté numérique.

Par exemple, vous pouvez choisir d'activer des contrôles qui vous aident à appliquer vos stratégies de chiffrement et de résilience, par exemple Exiger un cache d' AWS AppSync API pour activer le chiffrement en transit ou Exiger le déploiement d'un AWS Network Firewall dans plusieurs zones de disponibilité. Vous pouvez également personnaliser le contrôle des refus de la région AWS Control Tower afin d'appliquer les restrictions régionales les mieux adaptées aux besoins spécifiques de votre entreprise.

Cette version apporte des fonctionnalités de refus bien améliorées dans la région d'AWS Control Tower. Vous pouvez appliquer un nouveau contrôle de refus de région paramétré au niveau de l'unité organisationnelle, pour une meilleure granularité de la gouvernance, tout en maintenant une gouvernance régionale supplémentaire au niveau de la zone d'atterrissage. Ce contrôle de refus par région personnalisable vous permet d'appliquer les restrictions régionales les mieux adaptées aux besoins spécifiques de votre entreprise. Pour plus d'informations sur le nouveau contrôle de refus de région configurable, voir Contrôle de refus de région appliqué à l'unité d'organisation.

En tant que nouvel outil destiné à améliorer le refus des régions, cette version inclut une nouvelle API qui vous permet de rétablir les paramètres par défaut de vos contrôles activés. `UpdateEnabledControl` Cette API est particulièrement utile dans les cas d'utilisation où vous

devez résoudre rapidement la dérive ou pour garantir par programmation qu'un contrôle n'est pas en état de dérive. Pour plus d'informations sur la nouvelle API, consultez le document de référence sur les API AWS Control Tower

Nouveaux contrôles proactifs

- CT.APIGATEWAY.PR.6: Exiger qu'un domaine REST Amazon API Gateway utilise une politique de sécurité qui spécifie une version minimale du protocole TLS de TLSv1.2
- CT.APPSYNC.PR.2: Exiger la configuration d'une API AWS AppSync GraphQL avec une visibilité privée
- CT.APPSYNC.PR.3: Exiger qu'une API AWS AppSync GraphQL ne soit pas authentifiée à l'aide de clés d'API
- CT.APPSYNC.PR.4: Nécessite un cache d'API AWS AppSync GraphQL pour activer le chiffrement en transit.
- CT.APPSYNC.PR.5: nécessite un cache d'API AWS AppSync GraphQL pour activer le chiffrement au repos.
- CT.AUTOSCALING.PR.9: Exiger un volume Amazon EBS configuré via une configuration de lancement Amazon EC2 Auto Scaling pour chiffrer les données au repos
- CT.AUTOSCALING.PR.10: Exiger qu'un groupe Amazon EC2 Auto Scaling utilise uniquement les types d'instances AWS Nitro lors du remplacement d'un modèle de lancement
- CT.AUTOSCALING.PR.11: Exiger que seuls les types d'instances AWS Nitro prenant en charge le chiffrement du trafic réseau entre les instances soient ajoutés à un groupe Amazon EC2 Auto Scaling, lors du remplacement d'un modèle de lancement
- CT.DAX.PR.3: Exiger un cluster DynamoDB Accelerator pour chiffrer les données en transit avec le protocole TLS (Transport Layer Security)
- CT.DMS.PR.2: Exiger un point de terminaison du Service de Migration de AWS Base de Données (DMS) pour chiffrer les connexions pour les points de terminaison source et cible
- CT.EC2.PR.15: Exiger qu'une instance Amazon EC2 utilise un type d'instance AWS Nitro lors de la création à partir du type de ressource `AWS::EC2::LaunchTemplate`
- CT.EC2.PR.16: Exiger qu'une instance Amazon EC2 utilise un type d'instance AWS Nitro lorsqu'elle est créée à l'aide du type de ressource `AWS::EC2::Instance`
- CT.EC2.PR.17: Exiger qu'un hôte dédié Amazon EC2 utilise un type d'instance AWS Nitro
- CT.EC2.PR.18: Exiger qu'une flotte Amazon EC2 remplace uniquement les modèles de lancement par des types d'instances Nitro AWS

- CT.EC2.PR.19: Exiger qu'une instance Amazon EC2 utilise un type d'instance Nitro qui prend en charge le chiffrement en transit entre les instances lorsqu'elles sont créées à l'aide du type de ressource `AWS::EC2::Instance`
- CT.EC2.PR.20: Exiger qu'une flotte Amazon EC2 remplace uniquement les modèles de lancement par des types d'instances AWS Nitro qui prennent en charge le chiffrement lors du transit entre les instances
- CT.ELASTICACHE.PR.8: Exiger un groupe de ElastiCache réplication Amazon des versions ultérieures de Redis pour activer l'authentification RBAC
- CT.MQ.PR.1: Exiger qu'un courtier Amazon MQ ActiveMQ utilise le mode de déploiement actif/en veille pour une haute disponibilité
- CT.MQ.PR.2: Exiger qu'un courtier Amazon MQ Rabbit MQ utilise le mode cluster multi-AZ pour une haute disponibilité
- CT.MSK.PR.1: Exiger un cluster Amazon Managed Streaming for Apache Kafka (MSK) pour appliquer le chiffrement lors du transit entre les nœuds du cluster broker
- CT.MSK.PR.2: Exiger qu'un cluster Amazon Managed Streaming for Apache Kafka (MSK) soit configuré avec la désactivation PublicAccess
- CT.NETWORK-FIREWALL.PR.5: Exiger le déploiement d'un pare-feu AWS Network Firewall sur plusieurs zones de disponibilité
- CT.RDS.PR.26: nécessite un proxy de base de données Amazon RDS pour exiger des connexions TLS (Transport Layer Security)
- CT.RDS.PR.27: Exiger un groupe de paramètres de cluster de base de données Amazon RDS pour exiger des connexions TLS (Transport Layer Security) pour les types de moteurs pris en charge
- CT.RDS.PR.28: Exiger un groupe de paramètres de base de données Amazon RDS pour exiger des connexions TLS (Transport Layer Security) pour les types de moteurs pris en charge
- CT.RDS.PR.29: Exiger qu'un cluster Amazon RDS ne soit pas configuré pour être accessible au public au moyen de la propriété « PubliclyAccessible »
- CT.RDS.PR.30: Exiger que le chiffrement au repos d'une instance de base de données Amazon RDS soit configuré pour utiliser une clé KMS que vous spécifiez pour les types de moteurs pris en charge
- CT.S3.PR.12: Exiger qu'un point d'accès Amazon S3 possède une configuration Block Public Access (BPA) avec toutes les options définies sur true

Nouveaux contrôles préventifs

- CT.APPSYNC.PV.1Exiger qu'une API AWS AppSync GraphQL soit configurée avec une visibilité privée
- CT.EC2.PV.1Exiger la création d'un instantané Amazon EBS à partir d'un volume EC2 chiffré
- CT.EC2.PV.2Exiger qu'un volume Amazon EBS attaché soit configuré pour chiffrer les données au repos
- CT.EC2.PV.3Exiger qu'un instantané Amazon EBS ne puisse pas être restauré publiquement
- CT.EC2.PV.4Exiger que les API directes d'Amazon EBS ne soient pas appelées
- CT.EC2.PV.5Interdire l'utilisation de l'importation et de l'exportation de machines virtuelles Amazon EC2
- CT.EC2.PV.6Interdire l'utilisation d'actions Amazon EC2 et API obsolètes RequestSpotFleet RequestSpotInstances
- CT.KMS.PV.1Exiger une politique AWS KMS clé comportant une déclaration limitant la création de AWS KMS subventions aux AWS services
- CT.KMS.PV.2Exiger qu'une clé AWS KMS asymétrique contenant du matériel de clé RSA utilisé pour le chiffrement n'ait pas une longueur de clé de 2 048 bits
- CT.KMS.PV.3Exiger qu'une AWS KMS clé soit configurée avec le contrôle de sécurité du verrouillage par politique de contournement activé
- CT.KMS.PV.4Exiger qu'une clé AWS KMS gérée par le client (CMK) soit configurée avec du matériel clé provenant de CloudHSM AWS
- CT.KMS.PV.5Exiger qu'une clé AWS KMS gérée par le client (CMK) soit configurée avec du matériel clé importé
- CT.KMS.PV.6Exiger qu'une clé AWS KMS gérée par le client (CMK) soit configurée avec du matériel clé provenant d'un magasin de clés externe (XKS)
- CT.LAMBDA.PV.1Exiger une URL AWS Lambda de fonction pour utiliser l'authentification basée AWS sur IAM
- CT.LAMBDA.PV.2Exiger qu'une URL de AWS Lambda fonction soit configurée pour que seuls les principaux utilisateurs de votre Compte AWS
- CT.MULTISERVICE.PV.1 : Refuser l'accès à une unité organisationnelle en AWS fonction de la demande Région AWS

Les nouvelles commandes détectives qui améliorent votre posture de gouvernance en matière de souveraineté numérique font partie de la norme AWS Control Tower AWS Security Hub gérée par des services.

Nouvelles commandes de détection

- SH.ACM.2: les certificats RSA gérés par ACM doivent utiliser une longueur de clé d'au moins 2 048 bits
- SH.AppSync.5: les API AWS AppSync GraphQL ne doivent pas être authentifiées avec des clés d'API
- SH.CloudTrail.6: Assurez-vous que le compartiment S3 utilisé pour stocker CloudTrail les journaux n'est pas accessible au public :
- SH.DMS.9: les points de terminaison DMS doivent utiliser le protocole SSL
- SH.DocumentDB.3: Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics
- SH.DynamoDB.3: les clusters DynamoDB Accelerator (DAX) doivent être chiffrés au repos
- SH.EC2.23: Les passerelles de transit EC2 ne doivent pas accepter automatiquement les demandes de pièces jointes VPC
- SH.EKS.1: les points de terminaison du cluster EKS ne doivent pas être accessibles au public
- SH.ElastiCache.3: le basculement automatique doit être activé pour les groupes de ElastiCache réplication
- SH.ElastiCache.4: les groupes de ElastiCache réplication auraient dû être encryption-at-rest activés
- SH.ElastiCache.5: les groupes de ElastiCache réplication auraient dû être encryption-in-transit activés
- SH.ElastiCache.6: Redis AUTH doit être activé pour les groupes de ElastiCache réplication des versions antérieures de Redis
- SH.EventBridge.3: les bus d'événements EventBridge personnalisés doivent être associés à une politique basée sur les ressources
- SH.KMS.4: AWS KMS la rotation des touches doit être activée
- SH.Lambda.3: les fonctions Lambda doivent se trouver dans un VPC
- SH.MQ.5: les courtiers ActiveMQ doivent utiliser le mode de déploiement actif/en veille
- SH.MQ.6: Les courtiers RabbitMQ doivent utiliser le mode de déploiement en cluster
- SH.MSK.1: les clusters MSK doivent être chiffrés lors du transit entre les nœuds du courtier

- SH.RDS.12: l'authentification IAM doit être configurée pour les clusters RDS
- SH.RDS.15: les clusters de base de données RDS doivent être configurés pour plusieurs zones de disponibilité
- SH.S3.17: les compartiments S3 doivent être chiffrés au repos avec des clés AWS KMS

Pour plus d'informations sur les contrôles ajoutés à la norme AWS Control Tower AWS Security Hub gérée par les services, consultez Contrôles applicables à la norme AWS Control : AWS Control Tower dans la documentation. AWS Security Hub

Pour obtenir la liste des régions Régions AWS qui ne prennent pas en charge certains contrôles faisant partie de la norme AWS Control Tower AWS Security Hub gérée par des services, consultez la section Régions non prises en charge.

Nouveau contrôle configurable pour le refus de région au niveau de l'UO

CT.MULTISERVICE.PV.1 : Ce contrôle accepte des paramètres pour spécifier les régions exemptées, les principes IAM et les actions autorisés, au niveau de l'unité d'organisation, plutôt que pour l'ensemble de la zone d'atterrissage de l'AWS Control Tower. Il s'agit d'un contrôle préventif, mis en œuvre par la politique de contrôle des services (SCP).

Pour plus d'informations, consultez la section Contrôle de refus de région appliqué à l'unité d'organisation.

L'API **`UpdateEnabledControl`**

Cette version d'AWS Control Tower ajoute la prise en charge des API suivante pour les contrôles :

- L'`EnableControl`API mise à jour peut configurer des contrôles configurables.
- L'`GetEnabledControl`API mise à jour affiche les paramètres configurés sur un contrôle activé.
- La nouvelle `UpdateEnabledControl` API peut modifier les paramètres d'un contrôle activé.

Pour plus d'informations, consultez le guide de référence des API AWS Control Tower.

AWS Control Tower prend en charge les API de zone d'atterrissage

26 novembre 2023

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower prend désormais en charge la configuration et le lancement de la zone d'atterrissage à l'aide d'API. Vous pouvez créer, mettre à jour, obtenir, répertorier, réinitialiser et supprimer des zones d'atterrissage à l'aide d'API.

Les API suivantes vous permettent de configurer et de gérer votre zone d'atterrissage par programme à l'aide AWS CloudFormation du AWS CLI.

AWS Control Tower prend en charge les API suivantes pour les zones d'atterrissage :

- `CreateLandingZone`—Cet appel d'API crée une zone d'atterrissage à l'aide d'une version de zone d'atterrissage et d'un fichier manifeste.
- `GetLandingZoneOperation`—Cet appel d'API renvoie l'état d'une opération de zone d'atterrissage spécifiée.
- `GetLandingZone`—Cet appel d'API renvoie des informations sur la zone d'atterrissage spécifiée, notamment la version, le fichier manifeste et le statut.
- `UpdateLandingZone`—Cet appel d'API met à jour la version ou le fichier manifeste de la zone d'atterrissage.
- `ListLandingZone`—Cet appel d'API renvoie un identifiant de zone d'atterrissage (ARN) pour une configuration de zone d'atterrissage dans le compte de gestion.
- `ResetLandingZone`—Cet appel d'API réinitialise la zone d'atterrissage aux paramètres spécifiés lors de la dernière mise à jour, ce qui permet de réparer la dérive. Si la zone d'atterrissage n'a pas été mise à jour, cet appel rétablit les paramètres spécifiés lors de la création de la zone d'atterrissage.
- `DeleteLandingZone`—Cet appel d'API met hors service la zone d'atterrissage.

Pour commencer à utiliser les API de zone d'atterrissage, consultez leCommencer à utiliser AWS Control Tower à l'aide des API.

AWS Control Tower prend en charge le balisage pour les contrôles activés

10 novembre 2023

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower prend désormais en charge le balisage des ressources pour les contrôles activés, depuis la console AWS Control Tower ou au moyen d'API. Vous pouvez ajouter, supprimer ou répertorier des balises pour les contrôles activés.

Avec le lancement des API suivantes, vous pouvez configurer des balises pour les contrôles que vous activez dans AWS Control Tower. Les balises vous aident à gérer, identifier, organiser, rechercher et filtrer les ressources. Vous pouvez créer des balises pour classer vos ressources par objectif, propriétaire, environnement ou selon d'autres critères.

AWS Control Tower prend en charge les API suivantes pour le balisage des contrôles :

- `TagResource`—Cet appel d'API ajoute des balises aux contrôles activés dans AWS Control Tower.
- `UntagResource`—Cet appel d'API supprime les balises des contrôles activés dans AWS Control Tower.
- `ListTagsForResource`—Cet appel d'API renvoie des balises pour les contrôles activés dans AWS Control Tower.

Les API de contrôle d'AWS Control Tower sont disponibles Régions AWS là où AWS Control Tower est disponible. Pour obtenir la liste complète des Régions AWS sites dans lesquels AWS Control Tower est disponible, consultez le tableau des AWS régions. Pour obtenir la liste complète des API AWS Control Tower, consultez la référence des API.

AWS Control Tower est disponible dans la région Asie-Pacifique (Melbourne)

3 novembre 2023

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower est disponible dans la région Asie-Pacifique (Melbourne).

Si vous utilisez déjà AWS Control Tower et que vous souhaitez étendre ses fonctionnalités de gouvernance à cette région dans vos comptes, rendez-vous sur la page Paramètres de votre tableau de bord AWS Control Tower, sélectionnez la région, puis mettez à jour votre zone de landing zone. Après une mise à jour de la zone de landing zone, vous devez mettre à jour tous les comptes régis par AWS Control Tower, afin de placer vos comptes et vos unités d'organisation sous gouvernance dans la nouvelle région. Pour plus d'informations, voir À propos des mises à jour.

Pour obtenir la liste complète des régions dans lesquelles AWS Control Tower est disponible, consultez le Région AWS tableau.

Transition vers un nouveau type de produit AWS Service Catalog externe (phase 1)

31 octobre 2023

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

HashiCorp a mis à jour leur licence Terraform. En conséquence, le support pour les produits Open Source de Terraform a été AWS Service Catalog mis à jour et les produits ont été fournis pour un nouveau type de produit, appelé External.

AWS Control Tower ne prend pas en charge les personnalisations d'Account Factory qui reposent sur le type de produit AWS Service Catalog externe. Pour éviter toute interruption des charges de travail et AWS des ressources existantes dans vos comptes, suivez les étapes de transition d'AWS Control Tower dans cet ordre suggéré, d'ici le 14 décembre 2023 :

1. Mettez à niveau votre moteur de référence Terraform existant AWS Service Catalog pour inclure la prise en charge des types de produits externes et open source Terraform. Pour obtenir des instructions sur la mise à jour de votre moteur de référence Terraform, consultez le AWS Service Catalog GitHub référentiel.
2. Accédez à tous AWS Service Catalog les plans Open Source Terraform existants et dupliquez-les pour utiliser le nouveau type de produit externe. Ne mettez pas fin aux plans Open Source Terraform existants.
3. Continuez à utiliser vos plans Open Source Terraform existants pour créer ou mettre à jour des comptes dans AWS Control Tower.

Nouvelle API de contrôle disponible

14 octobre 2023

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower prend désormais en charge une API supplémentaire que vous pouvez utiliser pour déployer et gérer vos contrôles AWS Control Tower, à grande échelle. Pour plus d'informations sur les API de contrôle d'AWS Control Tower, consultez la référence des API.

AWS Control Tower a ajouté une nouvelle API de contrôle.

- `GetEnabledControl`—L'appel d'API fournit des informations sur un contrôle activé.

Nous avons également mis à jour cette API :

`ListEnabledControls`—Cet appel d'API répertorie les contrôles activés par AWS Control Tower sur l'unité organisationnelle spécifiée et les comptes qu'elle contient. Il renvoie désormais des informations supplémentaires dans un `EnabledControlSummary` objet.

Ces API vous permettent d'effectuer plusieurs opérations courantes par programmation. Par exemple :

- Obtenez une liste de tous les contrôles que vous avez activés dans la bibliothèque de contrôles AWS Control Tower.
- Pour tout contrôle activé, vous pouvez obtenir des informations sur les régions dans lesquelles le contrôle est pris en charge, l'identifiant du contrôle (ARN), l'état de dérive du contrôle et le résumé de l'état du contrôle.

Les API de contrôle d'AWS Control Tower sont disponibles Régions AWS là où AWS Control Tower est disponible. Pour obtenir la liste complète des Régions AWS sites dans lesquels AWS Control Tower est disponible, consultez le tableau des AWS régions. Pour obtenir la liste complète des API AWS Control Tower, consultez la référence des API.

AWS Control Tower ajoute des contrôles supplémentaires

5 octobre 2023

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower annonce de nouveaux contrôles proactifs et détectifs.

Les contrôles proactifs dans AWS Control Tower sont mis en œuvre au moyen de AWS CloudFormation Hooks, qui identifient et bloquent les ressources non conformes avant de les AWS CloudFormation approvisionner. Les contrôles proactifs complètent les capacités de contrôle préventif et de détection existantes d'AWS Control Tower.

Nouveaux contrôles proactifs

- [CT.ATHENA.PR.1] Exiger qu'un groupe de travail Amazon Athena chiffre les résultats des requêtes Athena au repos
- [CT.ATHENA.PR.2] Exiger d'un groupe de travail Amazon Athena qu'il crypte les résultats des requêtes Athena au repos avec une clé (KMS) AWS Key Management Service

- [CT.CLOUDTRAIL.PR.4] Exiger un magasin de données d'événements AWS CloudTrail Lake pour activer le chiffrement au repos avec une AWS KMS clé
- [CT.DAX.PR.2] Exiger un cluster Amazon DAX pour déployer des nœuds dans au moins trois zones de disponibilité
- [CT.EC2.PR.14] Exiger un volume Amazon EBS configuré via un modèle de lancement Amazon EC2 pour chiffrer les données au repos
- [CT.EKS.PR.2] Exiger qu'un cluster Amazon EKS soit configuré avec un chiffrement secret à l'aide des AWS clés du service de gestion des clés (KMS)
- [CT.ELASTICLOADBALANCING.PR.14] Exiger un Network Load Balancer pour activer l'équilibrage de charge entre zones
- [CT.ELASTICLOADBALANCING.PR.15] Exiger qu'un groupe cible Elastic Load Balancing v2 ne désactive pas explicitement l'équilibrage de charge entre zones
- [CT.EMR.PR.1] Exiger qu'une configuration de sécurité Amazon EMR (EMR) soit configurée pour chiffrer les données au repos dans Amazon S3
- [CT.EMR.PR.2] Exiger qu'une configuration de sécurité Amazon EMR (EMR) soit configurée pour chiffrer les données au repos dans Amazon S3 à l'aide d'une clé AWS KMS
- [CT.EMR.PR.3] Exiger qu'une configuration de sécurité Amazon EMR (EMR) soit configurée avec le chiffrement du disque local du volume EBS à l'aide d'une clé AWS KMS
- [CT.EMR.PR.4] Exiger qu'une configuration de sécurité Amazon EMR (EMR) soit configurée pour chiffrer les données en transit
- [CT.GLUE.PR.1] Exiger qu'une tâche AWS Glue soit associée à une configuration de sécurité
- [CT.GLUE.PR.2] Exiger une configuration de sécurité AWS Glue pour chiffrer les données dans les cibles Amazon S3 à l'aide de clés AWS KMS
- [CT.KMS.PR.2] Exiger qu'une clé AWS KMS asymétrique contenant du matériel de clé RSA utilisé pour le chiffrement ait une longueur de clé supérieure à 2 048 bits
- [CT.KMS.PR.3] Exiger une politique AWS KMS clé comportant une déclaration limitant la création de AWS KMS subventions aux AWS services
- [CT.LAMBDA.PR.4] Exiger une autorisation de AWS Lambda couche pour accorder l'accès à une AWS organisation ou à un AWS compte spécifique
- [CT.LAMBDA.PR.5] Exiger une URL de AWS Lambda fonction pour utiliser l'authentification basée AWS sur IAM
- [CT.LAMBDA.PR.6] Exiger une politique CORS d'URL de AWS Lambda fonction pour restreindre l'accès à des origines spécifiques

- [CT.NEPTUNE.PR.4] Exiger un cluster de base de données Amazon Neptune pour activer l'exportation des CloudWatch journaux Amazon pour les journaux d'audit
- [CT.NEPTUNE.PR.5] Exiger qu'un cluster de base de données Amazon Neptune définisse une période de conservation des sauvegardes supérieure ou égale à sept jours
- [CT.REDSHIFT.PR.9] Exiger qu'un groupe de paramètres de cluster Amazon Redshift soit configuré pour utiliser le protocole SSL (Secure Sockets Layer) pour le chiffrement des données en transit

Ces nouveaux contrôles proactifs sont disponibles dans les zones commerciales Régions AWS où AWS Control Tower est disponible. Pour plus de détails sur ces contrôles, voir Contrôles proactifs. Pour plus de détails sur les endroits où les commandes sont disponibles, consultez la section Limitations des commandes.

Nouvelles commandes de détection

De nouveaux contrôles ont été ajoutés au Security Hub Service-Managed Standard : AWS Control Tower. Ces contrôles vous aident à améliorer votre posture de gouvernance. Ils font partie du Security Hub Service-Managed Standard : AWS Control Tower, une fois que vous les avez activés sur une unité d'organisation spécifique.

- [SH.Athena.1] Les groupes de travail Athena doivent être chiffrés au repos
- [SH.Neptune.1] Les clusters de base de données Neptune doivent être chiffrés au repos
- [SH.Neptune.2] Les clusters de base de données Neptune doivent publier les journaux d'audit dans Logs CloudWatch
- [SH.Neptune.3] Les instantanés du cluster de base de données Neptune ne doivent pas être publics
- [SH.Neptune.4] La protection contre la suppression des clusters de base de données Neptune doit être activée
- [SH.Neptune.5] Les sauvegardes automatiques des clusters de base de données Neptune doivent être activées
- [SH.Neptune.6] Les instantanés du cluster de base de données Neptune doivent être chiffrés au repos
- [SH.Neptune.7] L'authentification de base de données IAM doit être activée pour les clusters de base de données Neptune

- [SH.Neptune.8] Les clusters de base de données Neptune doivent être configurés pour copier des balises dans des instantanés
- [SH.RDS.27] Les clusters de base de données RDS doivent être chiffrés au repos

Les nouvelles commandes AWS Security Hub de détection sont disponibles dans la plupart des Régions AWS pays où AWS Control Tower est disponible. Pour plus de détails sur ces contrôles, consultez Controls that apply to Service-Managed Standard : AWS Control Tower. Pour plus de détails sur les endroits où les commandes sont disponibles, consultezLimites de contrôle.

Nouveau type de dérive signalé : accès sécurisé désactivé

21 septembre 2023

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

Après avoir configuré la zone d'atterrissage de votre AWS Control Tower, vous pouvez désactiver l'accès sécurisé à AWS Control Tower dans AWS Organizations. Cependant, cela entraîne une dérive.

Avec le type de dérive à accès sécurisé désactivé, AWS Control Tower vous avertit lorsque ce type de dérive se produit, afin que vous puissiez réparer la zone d'atterrissage de votre AWS Control Tower. Pour plus d'informations, consultez la section Types de dérive de la gouvernance.

Quatre supplémentaires Régions AWS

13 septembre 2023

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower est désormais disponible en Asie-Pacifique (Hyderabad), en Europe (Espagne et Zurich) et au Moyen-Orient (Émirats arabes unis).

Si vous utilisez déjà AWS Control Tower et que vous souhaitez étendre ses fonctionnalités de gouvernance à cette région dans vos comptes, rendez-vous sur la page Paramètres de votre tableau de bord AWS Control Tower, sélectionnez la région, puis mettez à jour votre zone de landing zone. Après une mise à jour de la zone de landing zone, vous devez mettre à jour tous les comptes régis par AWS Control Tower, afin de placer vos comptes et vos unités d'organisation sous gouvernance dans la nouvelle région. Pour plus d'informations, voir À propos des mises à jour.

Pour obtenir la liste complète des régions dans lesquelles AWS Control Tower est disponible, consultez le Région AWS tableau.

AWS Control Tower est disponible dans la région de Tel Aviv

28 août 2023

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower annonce sa disponibilité dans la région d'Israël (Tel Aviv).

Si vous utilisez déjà AWS Control Tower et que vous souhaitez étendre ses fonctionnalités de gouvernance à cette région dans vos comptes, rendez-vous sur la page Paramètres de votre tableau de bord AWS Control Tower, sélectionnez la région, puis mettez à jour votre zone de landing zone. Après une mise à jour de la zone de landing zone, vous devez mettre à jour tous les comptes régis par AWS Control Tower, afin de placer vos comptes et vos unités d'organisation sous gouvernance dans la nouvelle région. Pour plus d'informations, voir À propos des mises à jour.

Pour obtenir la liste complète des régions dans lesquelles AWS Control Tower est disponible, consultez le Région AWS tableau.

AWS Control Tower lance 28 nouveaux contrôles proactifs

24 juillet 2023

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower ajoute 28 nouveaux contrôles proactifs pour vous aider à gérer votre AWS environnement.

Les contrôles proactifs améliorent les capacités de gouvernance d'AWS Control Tower dans vos AWS environnements multi-comptes, en bloquant les ressources non conformes avant leur mise en service. Ces contrôles permettent de gérer AWS des services tels qu'Amazon CloudWatch, Amazon Neptune, Amazon et Amazon ElastiCache AWS Step Functions DocumentDB. Les nouvelles commandes vous aident à atteindre des objectifs de contrôle tels que l'établissement de la journalisation et de la surveillance, le chiffrement des données au repos ou l'amélioration de la résilience.

Voici la liste complète des nouvelles commandes :

- [CT.APPSYNC.PR.1] Exiger une API AWS AppSync GraphQL pour activer la journalisation

- [CT.CLOUDWATCH.PR.1] Exiger une alarme CloudWatch Amazon pour qu'une action soit configurée pour l'état de l'alarme
- [CT.CLOUDWATCH.PR.2] Exiger qu'un groupe de journaux CloudWatch Amazon soit conservé pendant au moins un an
- [CT.CLOUDWATCH.PR.3] Exiger qu'un groupe de journaux CloudWatch Amazon soit chiffré au repos avec une clé KMS AWS
- [CT.CLOUDWATCH.PR.4] Exiger l'activation d'une action d'alarme Amazon CloudWatch
- [CT.DOCUMENTDB.PR.1] Exiger qu'un cluster Amazon DocumentDB soit chiffré au repos
- [CT.DOCUMENTDB.PR.2] Exiger que les sauvegardes automatiques soient activées sur un cluster Amazon DocumentDB
- [CT.DYNAMODB.PR.2] Exiger qu'une table Amazon DynamoDB soit chiffrée au repos à l'aide de clés AWS KMS
- [CT.EC2.PR.13] Exiger l'activation de la surveillance détaillée sur une instance Amazon EC2
- [CT.EKS.PR.1] Exiger qu'un cluster Amazon EKS soit configuré avec l'accès public désactivé au point de terminaison du serveur d'API Kubernetes du cluster
- [CT.ELASTICACHE.PR.1] Exiger que les sauvegardes automatiques soient activées sur un cluster ElastiCache Amazon pour Redis
- [CT.ELASTICACHE.PR.2] Exiger que les mises à niveau automatiques des versions mineures soient activées sur un cluster ElastiCache Amazon pour Redis
- [CT.ELASTICACHE.PR.3] Exiger qu'un groupe de réplication ElastiCache Amazon pour Redis active le basculement automatique
- [CT.ELASTICACHE.PR.4] Exiger que le chiffrement au repos soit activé sur un groupe de réplication ElastiCache Amazon
- [CT.ELASTICACHE.PR.5] Exiger qu'un groupe de réplication ElastiCache Amazon pour Redis active le chiffrement en transit
- [CT.ELASTICACHE.PR.6] Exiger qu'un cluster de cache ElastiCache Amazon utilise un groupe de sous-réseaux personnalisé
- [CT.ELASTICACHE.PR.7] Exiger qu'un groupe de réplication ElastiCache Amazon de versions antérieures de Redis dispose de l'authentification Redis AUTH
- [CT.ELASTICBEANSTALK.PR.3] Nécessite un environnement AWS Elastic Beanstalk pour disposer d'une configuration de journalisation
- [CT.LAMBDA.PR.3] Exiger qu'une AWS Lambda fonction se trouve dans un Amazon Virtual Private Cloud (VPC) géré par le client

- [CT.NEPTUNE.PR.1] Exiger qu'un cluster de base de données Amazon Neptune dispose d'une authentification de base de données (IAM) AWS Identity and Access Management
- [CT.NEPTUNE.PR.2] Exiger que la protection contre les suppressions soit activée sur un cluster de base de données Amazon Neptune
- [CT.NEPTUNE.PR.3] Exiger que le chiffrement du stockage soit activé sur un cluster de base de données Amazon Neptune
- [CT.REDSHIFT.PR.8] Exiger le chiffrement d'un cluster Amazon Redshift
- [CT.S3.PR.9] Exiger que S3 Object Lock soit activé dans un compartiment Amazon S3
- [CT.S3.PR.10] Exiger que le chiffrement côté serveur d'un compartiment Amazon S3 soit configuré à l'aide de clés AWS KMS
- [CT.S3.PR.11] Exiger l'activation du versionnement d'un compartiment Amazon S3
- [CT.STEPFUNCTIONS.PR.1] Exiger qu'une AWS Step Functions machine à états active la journalisation
- [CT.STEPFUNCTIONS.PR.2] Exiger qu'une AWS Step Functions machine à états active le suivi AWS X-Ray

Les contrôles proactifs dans AWS Control Tower sont mis en œuvre au moyen de AWS CloudFormation Hooks, qui identifient et bloquent les ressources non conformes avant de les AWS CloudFormation approvisionner. Les contrôles proactifs complètent les capacités de contrôle préventif et de détection existantes d'AWS Control Tower.

Ces nouveaux contrôles proactifs sont disponibles partout Régions AWS où AWS Control Tower est disponible. Pour plus de détails sur ces contrôles, voir Contrôles proactifs.

AWS Control Tower déconseille deux contrôles

18 juillet 2023

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower passe régulièrement en revue ses contrôles de sécurité pour s'assurer qu'ils sont à jour et qu'ils sont toujours considérés comme les meilleures pratiques. Les deux contrôles suivants sont devenus obsolètes à compter du 18 juillet 2023 et seront supprimés de la bibliothèque de contrôles à compter du 18 août 2023. Vous ne pouvez plus activer ces contrôles sur aucune unité organisationnelle. Vous pouvez choisir de désactiver ces contrôles avant la date de suppression.

- [SH.S3.4] Le chiffrement côté serveur doit être activé pour les compartiments S3

- [CT.S3.PR.7] Exiger que le chiffrement côté serveur soit configuré sur un compartiment Amazon S3

Motif de la dépréciation

Depuis janvier 2023, Amazon S3 a configuré le chiffrement par défaut sur tous les compartiments non chiffrés nouveaux et existants afin d'appliquer le chiffrement côté serveur avec des clés gérées S3 (SSE-S3) comme niveau de chiffrement de base pour les nouveaux objets chargés dans ces compartiments. Aucune modification n'a été apportée à la configuration de chiffrement par défaut pour un compartiment existant sur lequel le chiffrement SSE-S3 ou côté serveur avec des clés du service de gestion des AWS clés (KMS) (AWS SSE-KMS) était déjà configuré.

Zone de landing zone d'AWS Control Tower, version 3.2

16 juin 2023

(Mise à jour requise pour la zone de landing zone d'AWS Control Tower vers la version 3.2. Pour plus d'informations, voirMettre à jour votre zone de destination).

La version 3.2 de la zone de landing zone d'AWS Control Tower met à la disposition du grand public les commandes incluses dans le AWS Security Hub Service-Managed Standard : AWS Control Tower. Il permet de visualiser l'état de dérive des commandes incluses dans cette norme dans la console AWS Control Tower.

Cette mise à jour inclut un nouveau rôle lié à un service (SLR), appelé. AWSServiceRoleForAWSControlTower Ce rôle aide AWS Control Tower en créant une règle EventBridge gérée, appelée « AWSControlTowerManagedRuledans chaque compte membre ». Cette règle gérée collecte les événements de AWS Security Hub recherche. Grâce à AWS Control Tower, elle peut déterminer la dérive du contrôle.

Il s'agit de la première règle gérée créée par AWS Control Tower. La règle n'est pas déployée par une pile ; elle est déployée directement à partir des EventBridge API. Vous pouvez consulter la règle dans la EventBridge console ou à l'aide des EventBridge API. Si le `managed-by` champ est renseigné, il affichera le principal du service AWS Control Tower.

Auparavant, AWS Control Tower assumait le AWSControlTowerExecutionrôle d'effectuer des opérations sur les comptes des membres. Ce nouveau rôle et cette nouvelle règle sont mieux alignés sur le principe des meilleures pratiques qui consiste à accorder le moindre privilège lors de l'exécution d'opérations dans un AWS environnement multi-comptes. Le nouveau rôle fournit des

autorisations limitées qui permettent spécifiquement : de créer la règle gérée dans les comptes des membres, de maintenir la règle gérée, de publier des notifications de sécurité via SNS et de vérifier la dérive. Pour plus d'informations, consultez AWSServiceRoleForAWSControlTower.

La mise à jour 3.2 de la zone d'atterrissage inclut également une nouvelle StackSet ressource dans le compte de gestionBP_BASELINE_SERVICE_LINKED_ROLE, qui déploie initialement le rôle lié au service.

Lorsque vous signalez une dérive du contrôle du Security Hub (dans la landing zone 3.2 et versions ultérieures), AWS Control Tower reçoit une mise à jour quotidienne du statut de la part de Security Hub. Bien que les contrôles soient actifs dans chaque région gouvernée, AWS Control Tower envoie les événements AWS Security Hub Finding uniquement à la région d'origine d'AWS Control Tower. Pour plus d'informations, consultez la section Security Hub Control Drift Reporting.

Mise à jour du contrôle Region Deny

Cette version de zone d'atterrissage inclut également une mise à jour du contrôle Region Deny.

Ajout de services mondiaux et d'API

- AWS Billing and Cost Management (`billing:*`)
- AWS CloudTrail (`cloudtrail:LookupEvents`) pour permettre la visibilité des événements mondiaux sur les comptes des membres.
- AWS Facturation consolidée (`consolidatedbilling:*`)
- AWS Application mobile de console de gestion (`consoleapp:*`)
- AWS Niveau gratuit (`freetier:*`)
- Facturation AWS (`invoicing:*`)
- AWS IQ (`iq:*`)
- AWS Notifications aux utilisateurs (`notifications:*`)
- AWS Contacts pour les notifications utilisateur (`notifications-contacts:*`)
- Amazon Payments (`payments:*`)
- AWS Paramètres fiscaux (`tax:*`)

Services globaux et API supprimés

- Supprimé `s3:GetAccountPublic` car il ne s'agit pas d'une action valide.
- Supprimé `s3:PutAccountPublic` car il ne s'agit pas d'une action valide.

AWS Control Tower gère les comptes en fonction de leur identifiant

14 juin 2023

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower crée et gère désormais les comptes que vous créez dans Account Factory en suivant l' AWS identifiant du compte, plutôt que son adresse e-mail.

Lors de la mise en service d'un compte, le demandeur du compte doit toujours disposer des autorisations `CreateAccount` et des `DescribeCreateAccountStatus` autorisations. Cet ensemble d'autorisations fait partie du rôle d'administrateur et est accordé automatiquement lorsqu'un demandeur assume le rôle d'administrateur. Si vous déléguez l'autorisation de provisionner des comptes, vous devrez peut-être ajouter ces autorisations directement aux demandeurs de comptes.

Contrôles de détection supplémentaires du Security Hub disponibles dans la bibliothèque de contrôles AWS Control Tower

12 juin 2023

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower a ajouté dix nouveaux contrôles AWS Security Hub de détection à la bibliothèque de contrôles AWS Control Tower. Ces nouveaux contrôles ciblent des services tels que API Gateway AWS CodeBuild, Amazon Elastic Compute Cloud (EC2), Amazon Elastic Load Balancer, Amazon Redshift, Amazon et. SageMaker AWS WAF Ces nouveaux contrôles vous aident à améliorer votre posture de gouvernance en atteignant les objectifs de contrôle, tels que l'établissement de la journalisation et de la surveillance, la limitation de l'accès au réseau et le chiffrement des données au repos.

Ces contrôles font partie du Security Hub Service-Managed Standard : AWS Control Tower, une fois que vous les avez activés sur une unité d'organisation spécifique.

- [Sh.Account.1] Les coordonnées de sécurité doivent être fournies pour Compte AWS
- [Sh.APIGateway.8] Les routes API Gateway doivent spécifier un type d'autorisation
- [Sh.APIGateway.9] La journalisation des accès doit être configurée pour les étapes API Gateway V2
- [SH. CodeBuild.3] Les journaux CodeBuild S3 doivent être chiffrés

- [SH.EC2.25] Les modèles de lancement EC2 ne doivent pas attribuer d'adresses IP publiques aux interfaces réseau
- [SH.ELB.1] Application Load Balancer doit être configuré pour rediriger toutes les requêtes HTTP vers HTTPS
- [Sh.Redshift.10] Les clusters Redshift doivent être chiffrés au repos
- [SH. SageMaker.2] les instances de SageMaker bloc-notes doivent être lancées dans un VPC personnalisé
- [SH. SageMaker.3] Les utilisateurs ne doivent pas avoir d'accès root aux instances de SageMaker bloc-notes
- [SH.WAF.10] Une ACL Web WAFV2 doit comporter au moins une règle ou un groupe de règles

Les nouvelles AWS Security Hub commandes de détection sont disponibles partout Régions AWS où AWS Control Tower est disponible. Pour plus de détails sur ces contrôles, consultez Controls that apply to Service-Managed Standard : AWS Control Tower.

AWS Control Tower publie des tables de métadonnées de contrôle

7 juin 2023

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower fournit désormais des tables complètes de métadonnées de contrôle dans le cadre de la documentation publiée. Lorsque vous travaillez avec les API de contrôle, vous pouvez consulter l'API ControlIdentifier de chaque contrôle, qui est un ARN unique associé à chaque contrôle. Région AWS Les tableaux incluent les cadres et les objectifs de contrôle couverts par chaque contrôle. Auparavant, ces informations n'étaient disponibles que dans la console.

Les tables incluent également les métadonnées des contrôles Security Hub qui font partie de la norme AWS Security Hub Service-Managed : AWS Control Tower. Pour plus de détails, consultez la section Tableaux des métadonnées de contrôle.

Pour obtenir une liste abrégée des identifiants de contrôle et quelques exemples d'utilisation, consultez la section Identifiants de ressources pour les API et les contrôles.

Support de Terraform pour la personnalisation d'Account Factory

6 juin 2023

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower propose un support régional pour Terraform via Account Factory Customization (AFC). À partir de cette version, vous pouvez utiliser AWS Control Tower et Service Catalog ensemble, pour définir des plans de compte AFC, dans l'open source Terraform. Vous pouvez personnaliser vos ressources nouvelles et existantes Comptes AWS avant de provisionner des ressources dans AWS Control Tower. Par défaut, cette fonctionnalité vous permet de déployer et de mettre à jour des comptes, avec Terraform, dans votre région d'origine AWS Control Tower.

Un plan de compte décrit les ressources et les configurations spécifiques requises lors du provisionnement d' Compte AWS un compte. Vous pouvez utiliser le plan comme modèle pour en créer plusieurs Comptes AWS à grande échelle.

Pour commencer, utilisez le moteur de référence Terraform activé. GitHub Le moteur de référence configure le code et l'infrastructure requis pour que le moteur open source Terraform fonctionne avec Service Catalog. Ce processus de configuration unique prend quelques minutes. Ensuite, vous pouvez définir les exigences de votre compte personnalisé dans Terraform, puis déployer vos comptes à l'aide du flux de travail bien défini d'AWS Control Tower Account Factory. Les clients qui préfèrent travailler avec Terraform peuvent utiliser la personnalisation des comptes AWS Control Tower à grande échelle avec AFC et obtenir un accès immédiat à chaque compte une fois celui-ci provisionné.

Pour savoir comment créer ces personnalisations, consultez Creating Products et Getting started with Terraform open source dans la documentation Service Catalog. Cette fonctionnalité est disponible partout Régions AWS où AWS Control Tower est disponible.

AWS L'autogestion de l'IAM Identity Center est disponible pour la zone de landing zone

6 juin 2023

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower prend désormais en charge un choix facultatif de fournisseur d'identité pour une zone de landing zone AWS Control Tower, que vous pouvez configurer lors de la configuration ou de la mise à jour. Par défaut, la zone de landing zone est activée pour utiliser AWS IAM Identity Center, conformément aux recommandations relatives aux meilleures pratiques définies dans Organizing Your Environment Using Multiple Accounts. AWS Trois alternatives s'offrent à vous :

- Vous pouvez accepter la valeur par défaut et autoriser AWS Control Tower à configurer et à gérer AWS IAM Identity Center pour vous.

- Vous pouvez choisir de gérer vous-même l' AWS IAM Identity Center, en fonction des besoins spécifiques de votre entreprise.
- Vous pouvez éventuellement faire appel à un fournisseur d'identité tiers et le gérer vous-même en le connectant via IAM Identity Center, si nécessaire. Vous devez utiliser l'option du fournisseur d'identité si votre environnement réglementaire vous oblige à faire appel à un fournisseur spécifique ou si vous opérez dans un pays Régions AWS où AWS IAM Identity Center n'est pas disponible.

Pour plus d'informations, consultez Conseils relatifs à l'IAM Identity Center.

La sélection de fournisseurs d'identité au niveau du compte n'est pas prise en charge. Cette fonctionnalité s'applique uniquement à la zone d'atterrissage dans son ensemble. L'option du fournisseur d'identité AWS Control Tower est disponible partout Régions AWS où AWS Control Tower est disponible.

AWS Control Tower résout le problème de la gouvernance mixte pour les unités d'organisation

1er juin 2023

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

Avec cette version, AWS Control Tower empêche le déploiement des contrôles dans une unité organisationnelle (UO) si cette unité d'organisation est dans un état de gouvernance mixte. Une gouvernance mixte se produit dans une unité d'organisation si les comptes ne sont pas mis à jour après qu'AWS Control Tower ait étendu la gouvernance à une nouvelle Région AWS entité ou ait supprimé la gouvernance. Cette version vous aide à garantir la conformité uniforme des comptes des membres de cette unité d'organisation. Pour plus d'informations, consultez Évitez la gouvernance mixte lors de la configuration des régions.

Contrôles proactifs supplémentaires disponibles

19 mai 2023

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower ajoute 28 nouveaux contrôles proactifs pour vous aider à gérer votre environnement multi-comptes et à atteindre des objectifs de contrôle spécifiques, tels que le

chiffrement des données au repos ou la limitation de l'accès au réseau. Des contrôles proactifs sont mis en œuvre avec AWS CloudFormation des hooks qui vérifient vos ressources avant qu'elles ne soient provisionnées. Les nouveaux contrôles peuvent aider à régir AWS des services tels qu'Amazon OpenSearch Service, Amazon EC2 Auto Scaling SageMaker, Amazon, Amazon API Gateway et Amazon Relational Database Service (RDS).

Les contrôles proactifs sont pris en charge dans toutes les Régions AWS zones commerciales où AWS Control Tower est disponible.

Amazon OpenSearch Service

- [CT.OPENSEARCH.PR.1] Exiger un domaine Elasticsearch pour chiffrer les données au repos
- [CT.OPENSEARCH.PR.2] Exiger la création d'un domaine Elasticsearch dans un Amazon VPC spécifié par l'utilisateur
- [CT.OPENSEARCH.PR.3] Exiger un domaine Elasticsearch pour chiffrer les données envoyées entre les nœuds
- [CT.OPENSEARCH.PR.4] Exiger un domaine Elasticsearch pour envoyer des journaux d'erreurs à Amazon Logs CloudWatch
- [CT.OPENSEARCH.PR.5] Exiger un domaine Elasticsearch pour envoyer des journaux d'audit à Amazon Logs CloudWatch
- [CT.OPENSEARCH.PR.6] Exiger qu'un domaine Elasticsearch dispose d'une reconnaissance de zone et d'au moins trois nœuds de données
- [CT.OPENSEARCH.PR.7] Exiger qu'un domaine Elasticsearch possède au moins trois nœuds maîtres dédiés
- [CT.OPENSEARCH.PR.8] Nécessite un domaine Elasticsearch Service pour utiliser TLSv1.2
- [CT.OPENSEARCH.PR.9] Exiger un domaine OpenSearch Amazon Service pour chiffrer les données au repos
- [CT.OPENSEARCH.PR.10] Exiger la création d'un domaine Amazon Service dans un OpenSearch Amazon VPC spécifié par l'utilisateur
- [CT.OPENSEARCH.PR.11] Exiger un domaine OpenSearch Amazon Service pour chiffrer les données envoyées entre les nœuds
- [CT.OPENSEARCH.PR.12] Exiger un domaine Amazon Service pour envoyer des journaux d'erreurs à OpenSearch Amazon Logs CloudWatch
- [CT.OPENSEARCH.PR.13] Exiger un domaine Amazon Service pour envoyer des journaux d'audit à OpenSearch Amazon Logs CloudWatch

- [CT.OPENSEARCH.PR.14] Exiger qu'un domaine OpenSearch Amazon Service dispose d'une reconnaissance de zone et d'au moins trois nœuds de données
- [CT.OPENSEARCH.PR.15] Exiger un domaine OpenSearch Amazon Service pour utiliser un contrôle d'accès précis
- [CT.OPENSEARCH.PR.16] Exiger un domaine Amazon Service pour utiliser TLSv1.2 OpenSearch

Amazon EC2 Auto Scaling

- [CT.AUTOSCALING.PR.1] Exiger qu'un groupe Amazon EC2 Auto Scaling possède plusieurs zones de disponibilité
- [CT.AUTOSCALING.PR.2] Exiger une configuration de lancement de groupe Amazon EC2 Auto Scaling pour configurer les instances Amazon EC2 pour IMDSv2
- [CT.AUTOSCALING.PR.3] Exiger une configuration de lancement d'Amazon EC2 Auto Scaling pour avoir une limite de réponse aux métadonnées à saut unique
- [CT.AUTOSCALING.PR.4] Exiger qu'un groupe Amazon EC2 Auto Scaling associé à un Amazon Elastic Load Balancing (ELB) fasse activer les bilans de santé ELB
- [CT.AUTOSCALING.PR.5] Exiger qu'une configuration de lancement de groupe Amazon EC2 Auto Scaling ne comporte pas d'instances Amazon EC2 avec des adresses IP publiques
- [CT.AUTOSCALING.PR.6] Exiger que tous les groupes Amazon EC2 Auto Scaling utilisent plusieurs types d'instances
- [CT.AUTOSCALING.PR.8] Exiger la configuration des modèles de lancement EC2 d'un groupe Amazon EC2 Auto Scaling

Amazon SageMaker

- [CT.SAGEMAKER.PR.1] Exiger une instance de bloc-notes SageMaker Amazon pour empêcher l'accès direct à Internet
- [CT.SAGEMAKER.PR.2] Exiger le déploiement des instances Amazon Notebook au sein d'un SageMaker Amazon VPC personnalisé
- [CT.SAGEMAKER.PR.3] Exiger que l'accès root soit interdit aux instances d' SageMaker Amazon Notebook

Amazon API Gateway

- [CT.APIGATEWAY.PR.5] Exiger des routes Websocket et HTTP Amazon API Gateway V2 pour spécifier un type d'autorisation

Amazon Relational Database Service (RDS)

- [CT.RDS.PR.25] Exiger que la journalisation soit configurée sur un cluster de bases de données Amazon RDS

Pour plus d'informations, consultez la section Contrôles proactifs.

Contrôles proactifs Amazon EC2 mis à jour

2 mai 2023

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower a mis à jour deux contrôles proactifs : CT.EC2.PR.3 etCT.EC2.PR.4.

Pour le CT.EC2.PR.3 contrôle mis à jour, tout AWS CloudFormation déploiement faisant référence à une liste de préfixes pour une ressource de groupe de sécurité est bloqué, sauf pour le port 80 ou 443.

Pour le CT.EC2.PR.4 contrôle mis à jour, tout AWS CloudFormation déploiement faisant référence à une liste de préfixes pour une ressource de groupe de sécurité est bloqué si le port est 3389, 20, 23, 110, 143, 3306, 8080, 1433, 9200, 9300, 25, 445, 135, 21, 1434, 4333, 5432, 5500, 5601, 22, 3000, 5000, 8088, 8888.

Sept autres Régions AWS disponibles

19 avril 2023

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower est désormais disponible dans sept autres pays Régions AWS : Californie du Nord (San Francisco), Asie-Pacifique (Hong Kong, Jakarta et Osaka), Europe (Milan), Moyen-Orient (Bahreïn) et Afrique (Le Cap). Ces régions supplémentaires pour AWS Control Tower, appelées régions opt-in, ne sont pas actives par défaut, à l'exception de la région USA Ouest (Californie du Nord), qui est active par défaut.

Certains contrôles d'AWS Control Tower ne fonctionnent pas dans certains de ces systèmes supplémentaires Régions AWS où AWS Control Tower est disponible, car ces régions ne prennent pas en charge les fonctionnalités sous-jacentes requises. Pour plus de détails, consultez Limites de contrôle.

Parmi ces nouvelles régions, le CfCT n'est pas disponible en Asie-Pacifique (Jakarta et Osaka). La disponibilité dans les autres Régions AWS catégories reste inchangée.

Pour plus d'informations sur la façon dont AWS Control Tower gère les limites des régions et des contrôles, consultezConsidérations relatives à l'activation des AWS régions optionnelles.

Les points de terminaison vPCE requis par l'AFT ne sont pas disponibles dans la région Moyen-Orient (Bahreïn). Les clients qui déploient AFT dans cette région doivent effectuer le déploiement avec paramètre`aft_vpc_endpoints=false`. Pour plus d'informations, consultez le paramètre dans le fichier README.

Les VPC AWS Control Tower disposent de deux zones de disponibilité dans la région de l'ouest des États-Unis (Californie du Nord)`us-west-1`, en raison d'une limitation d'Amazon EC2. Dans l'ouest des États-Unis (Californie du Nord), six sous-réseaux sont répartis sur deux zones de disponibilité. Pour plus d'informations, consultez Présentation d'AWS Control Tower et des VPC.

AWS Control Tower a ajouté de nouvelles autorisations `AWSControlTowerServiceRolePolicy` qui permettent à AWS Control Tower de passer des appels vers `EnableRegionListRegions`, et des `GetRegionOptStatus` API ont été mises en œuvre par le service de gestion des AWS comptes, afin de les rendre Régions AWS disponibles pour vos comptes partagés dans la zone de landing zone (compte de gestion, compte d'archive des journaux, compte d'audit) et pour vos comptes de membres de l'unité d'organisation. Pour plus d'informations, consultez Politiques gérées pour AWS Control Tower.

Suivi des demandes de personnalisation du compte Account Factory for Terraform (AFT)

16 février 2023

AFT prend en charge le suivi des demandes de personnalisation des comptes. Chaque fois que vous soumettez une demande de personnalisation de compte, AFT génère un jeton de suivi unique qui passe par une machine d' AWS Step Functions état de personnalisation AFT, qui enregistre le jeton dans le cadre de son exécution. Vous pouvez utiliser les requêtes Amazon CloudWatch Logs Insights pour rechercher des plages d'horodatage et récupérer le jeton de demande. Par conséquent, vous

pouvez voir les charges utiles qui accompagnent le jeton, ce qui vous permet de suivre la demande de personnalisation de votre compte tout au long du flux de travail AFT. Pour plus d'informations sur l'AFT, consultez la section Présentation d'AWS Control Tower Account Factory pour Terraform. Pour plus d'informations sur CloudWatch les journaux et les Step Functions, consultez les rubriques suivantes :

- Qu'est-ce qu'Amazon CloudWatch Logs ? dans le guide de l'utilisateur d'Amazon CloudWatch Logs
- Qu'est-ce que c'est AWS Step Functions ? dans le guide AWS Step Functions du développeur

Zone de landing zone d'AWS Control Tower, version 3.1

9 février 2023

(Mise à jour requise pour la zone de landing zone d'AWS Control Tower vers la version 3.1. Pour plus d'informations, voirMettre à jour votre zone de destination)

La version 3.1 de la zone de landing zone d'AWS Control Tower inclut les mises à jour suivantes :

- Avec cette version, AWS Control Tower désactive la journalisation des accès inutile pour votre compartiment de journalisation des accès, qui est le compartiment Amazon S3 dans lequel les journaux d'accès sont stockés dans le compte Log Archive, tout en continuant à activer la journalisation des accès au serveur pour les compartiments S3. Cette version inclut également des mises à jour du contrôle Region Deny qui autorisent des actions supplémentaires pour les services mondiaux, tels que AWS Support Plans et AWS Artifact.
- La désactivation de la journalisation des accès au serveur pour le compartiment de journalisation des accès d'AWS Control Tower oblige Security Hub à créer une recherche pour le compartiment de journalisation des accès du compte Log Archive. En raison d'une AWS Security Hub règle, la journalisation des accès au serveur du compartiment S3 doit être activée [S3.9]. Conformément à Security Hub, nous vous recommandons de supprimer cette constatation particulière, comme indiqué dans la description de cette règle dans le Security Hub. Pour plus d'informations, consultez les informations sur les résultats supprimés.
- La journalisation des accès pour le bucket de journalisation (normal) du compte Log Archive est inchangée dans la version 3.1. Conformément aux meilleures pratiques, les événements d'accès pour ce compartiment sont enregistrés sous forme d'entrées de journal dans le compartiment de journalisation des accès. Pour plus d'informations sur la journalisation des accès, consultez la section Journalisation des demandes à l'aide de la journalisation des accès au serveur dans la documentation Amazon S3.

- Nous avons mis à jour le contrôle Region Deny. Cette mise à jour autorise les actions d'un plus grand nombre de services mondiaux. Pour plus de détails sur ce SCP, voir Refuser l'accès en AWS fonction de la demande Région AWS et Contrôles qui améliorent la protection de la résidence des données.

  Services globaux ajoutés :

  - AWS Account Management (`account:*`)
  - AWS Activer (`activate:*`)
  - AWS Artifact (`artifact:*`)
  - AWS Billing Conductor (`billingconductor:*`)
  - AWS Compute Optimizer (`compute-optimizer:*`)
  - AWS Data Pipeline (`datapipeline:GetAccountLimits`)
  - AWS Device Farm(`devicefarm:*`)
  - AWS Marketplace (`discovery-marketplace:*`)
  - Amazon ECR () `ecr-public:*`
  - AWS License Manager (`license-manager:ListReceivedLicenses`)
  - AWS Lightsail () `lightsail:Get*`
  - Explorateur de ressources AWS (`resource-explorer-2:*`)
  - Amazon S3 (`s3:CreateMultiRegionAccessPoint`,`s3:GetBucketPolicyStatus`,`s3:PutMultiRegionAcc`
  - AWS Savings Plans (`savingsplans:*`)
  - Centre d'identité IAM () `sso:*`
  - AWS Support App (`supportapp:*`)
  - AWS Support Plans (`supportplans:*`)
  - AWS Durabilité (`sustainability:*`)
  - AWS Resource Groups Tagging API (`tag:GetResources`)
  - AWS Marketplace Informations sur les fournisseurs (`vendor-insights:ListEntitledSecurityProfiles`)

Contrôles proactifs généralement disponibles

24 janvier 2023

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

Les contrôles proactifs optionnels, précédemment annoncés en version préliminaire, sont désormais généralement disponibles. Ces contrôles sont qualifiés de proactifs car ils vérifient vos ressources, avant qu'elles ne soient déployées, afin de déterminer si les nouvelles ressources sont conformes aux contrôles activés dans votre environnement. Pour plus d'informations, consultez Des contrôles complets facilitent le provisionnement et la gestion des AWS ressources.

janvier - décembre 2022

En 2022, AWS Control Tower a publié les mises à jour suivantes :

- Opérations de compte simultanées
- Personnalisation de Account Factory (AFC)
- Des contrôles complets facilitent le provisionnement et la gestion des AWS ressources
- État de conformité consultable pour toutes les AWS Config règles
- API pour les contrôles et une nouvelle AWS CloudFormation ressource
- CfCT prend en charge la suppression d'ensembles de piles
- Conservation personnalisée des journaux
- Réparation de la dérive des rôles disponible
- Zone de landing zone d'AWS Control Tower, version 3.0
- La page Organisation combine les vues des unités d'organisation et des comptes
- Inscription et mise à jour simplifiées pour les comptes de membres individuels
- AFT prend en charge la personnalisation automatique des comptes AWS Control Tower partagés
- Opérations simultanées pour tous les contrôles optionnels
- Comptes de sécurité et de journalisation existants
- Zone de landing zone d'AWS Control Tower, version 2.9
- Zone de landing zone d'AWS Control Tower, version 2.8

Opérations de compte simultanées

16 décembre 2022

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower prend désormais en charge les actions simultanées dans Account Factory. Vous pouvez créer, mettre à jour ou inscrire jusqu'à cinq (5) comptes à la fois. Soumettez jusqu'à cinq actions à la suite et consultez l'état d'avancement de chaque demande, tandis que vos comptes finissent de s'accumuler en arrière-plan. Par exemple, vous ne devez plus attendre la fin de chaque processus pour mettre à jour un autre compte ou avant de réenregistrer une unité organisationnelle (UO) complète.

Personnalisation de Account Factory (AFC)

28 novembre 2022

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

La personnalisation des comptes en usine vous permet de personnaliser les comptes nouveaux et existants depuis la console AWS Control Tower. Ces nouvelles fonctionnalités de personnalisation vous permettent de définir des plans de compte, qui sont des AWS CloudFormation modèles contenus dans un produit Service Catalog spécialisé. Les plans fournissent des ressources et des configurations entièrement personnalisées. Vous pouvez également choisir d'utiliser des plans prédéfinis, conçus et gérés par des AWS partenaires, qui vous aident à personnaliser les comptes pour des cas d'utilisation spécifiques.

Auparavant, AWS Control Tower Account Factory ne prenait pas en charge la personnalisation des comptes dans la console. Avec cette mise à jour de Account Factory, vous pouvez prédéfinir les exigences relatives aux comptes et les mettre en œuvre dans le cadre d'un flux de travail bien défini. Vous pouvez appliquer des plans pour créer de nouveaux comptes, inscrire d'autres AWS comptes dans AWS Control Tower et mettre à jour les comptes AWS Control Tower existants.

Lorsque vous approvisionnez, enregistrez ou mettez à jour un compte dans Account Factory, vous sélectionnez le plan à déployer. Les ressources spécifiées dans le plan sont mises à disposition sur votre compte. Lorsque la création de votre compte est terminée, toutes les configurations personnalisées peuvent être utilisées immédiatement.

Pour commencer à personnaliser les comptes, vous pouvez définir les ressources correspondant à votre cas d'utilisation prévu dans un produit Service Catalog. Vous pouvez également sélectionner des solutions gérées par des partenaires dans la bibliothèque AWS Getting Started. Pour plus d'informations, consultez Personnalisez les comptes avec Account Factory Customization (AFC).

Des contrôles complets facilitent le provisionnement et la gestion des AWS ressources

28 novembre 2022

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower prend désormais en charge la gestion complète des contrôles, y compris de nouveaux contrôles proactifs optionnels, mis en œuvre via AWS CloudFormation des hooks. Ces contrôles sont qualifiés de proactifs car ils vérifient vos ressources, avant qu'elles ne soient déployées, afin de déterminer si les nouvelles ressources seront conformes aux contrôles activés dans votre environnement.

Plus de 130 nouveaux contrôles proactifs vous aident à atteindre des objectifs politiques spécifiques pour votre environnement AWS Control Tower, à satisfaire aux exigences des cadres de conformité aux normes du secteur et à régir les interactions avec AWS Control Tower dans plus de vingt autres AWS services.

La bibliothèque de contrôles AWS Control Tower classe ces contrôles en fonction des AWS services et ressources associés. Pour plus de détails, consultez la section Contrôles proactifs.

Dans cette version, AWS Control Tower est également intégrée AWS Security Hub, au moyen de la nouvelle norme Security Hub gérée par les services : AWS Control Tower, qui prend en charge la norme AWS Foundational Security Best Practices (FSBP). Vous pouvez consulter plus de 160 contrôles Security Hub ainsi que les contrôles AWS Control Tower dans la console, et vous pouvez obtenir un score de sécurité Security Hub pour votre environnement AWS Control Tower. Pour plus d'informations, consultez la section Contrôles du Security Hub.

État de conformité consultable pour toutes les AWS Config règles

18 novembre 2022

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower affiche désormais l'état de conformité de toutes les AWS Config règles déployées dans les unités organisationnelles enregistrées auprès d'AWS Control Tower. Vous pouvez consulter l'état de conformité de toutes les AWS Config règles qui affectent vos comptes dans AWS Control Tower, qu'ils soient inscrits ou non, sans avoir à naviguer en dehors de la console

AWS Control Tower. Les clients peuvent choisir de configurer des règles de configuration, appelées contrôles de détection, dans AWS Control Tower, ou de les configurer directement via le AWS Config service. Les règles déployées par AWS Config sont affichées, ainsi que les règles déployées par AWS Control Tower.

Auparavant, AWS Config les règles déployées via le AWS Config service n'étaient pas visibles dans la console AWS Control Tower. Les clients devaient accéder au AWS Config service pour identifier les AWS Config règles non conformes. Vous pouvez désormais identifier toute AWS Config règle non conforme dans la console AWS Control Tower. Pour connaître l'état de conformité de toutes vos règles Config, accédez à la page des détails du compte dans la console AWS Control Tower. Vous verrez une liste indiquant l'état de conformité des contrôles gérés par AWS Control Tower et les règles Config déployées en dehors d'AWS Control Tower.

API pour les contrôles et une nouvelle AWS CloudFormation ressource

1er septembre 2022

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower prend désormais en charge la gestion programmatique des contrôles, également appelés garde-fous, par le biais d'un ensemble d'appels d'API. Une nouvelle AWS CloudFormation ressource prend en charge les fonctionnalités de l'API pour les contrôles. Pour de plus amples informations, veuillez consulter Automatisez les tâches dans AWS Control Tower et Création de AWS Control Tower ressources avec AWS CloudFormation.

Ces API vous permettent d'activer, de désactiver et de consulter l'état de l'application des contrôles dans la bibliothèque AWS Control Tower. Les API incluent la prise en charge de AWS CloudFormation, afin que vous puissiez gérer les AWS ressources en tant que infrastructure-as-code (iAc). AWS Control Tower fournit des contrôles préventifs et de détection facultatifs qui expriment vos intentions politiques concernant l'ensemble d'une unité organisationnelle (UO) et chaque AWS compte au sein de l'UO. Ces règles restent en vigueur lorsque vous créez de nouveaux comptes ou modifiez des comptes existants.

API incluses dans cette version

- EnableControl— Cet appel d'API active un contrôle. Il lance une opération asynchrone qui crée AWS des ressources sur l'unité organisationnelle spécifiée et les comptes qu'elle contient.
- DisableControl— Cet appel d'API désactive un contrôle. Il lance une opération asynchrone qui supprime les AWS ressources de l'unité organisationnelle spécifiée et les comptes qu'elle contient.

- GetControlOperation— Renvoie le statut d'un particulier EnableControlou d'une DisableControlopération.
- ListEnabledControls— Répertorie les contrôles activés par AWS Control Tower sur l'unité organisationnelle spécifiée et les comptes qu'elle contient.

Pour consulter la liste des noms de contrôle pour les contrôles facultatifs, consultez la section Identifiants de ressources pour les API et les contrôles dans le guide de l'utilisateur d'AWS Control Tower.

CfCT prend en charge la suppression d'ensembles de piles

26 août 2022

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

Les personnalisations pour AWS Control Tower (CfCT) prennent désormais en charge la suppression d'ensembles de piles, en définissant un paramètre dans le `manifest.yaml` fichier. Pour plus d'informations, consultez Suppression d'un ensemble de piles.

> **Important**
>
> Lorsque vous définissez la valeur de `enable_stack_set_deletion` to pour la première fois`true`, la prochaine fois que vous invoquerez CfCT, TOUTES les ressources qui commencent par le préfixe`CustomControlTower-`, auxquelles est associée la balise `Key:AWS_Solutions, Value: CustomControlTowerStackSet` clé et qui ne sont pas déclarées dans le fichier manifeste sont préparées pour être supprimées.

Conservation personnalisée des journaux

15 août 2022

(Mise à jour requise pour la zone de landing zone d'AWS Control Tower. Pour plus d'informations, voirMettre à jour votre zone de destination)

AWS Control Tower permet désormais de personnaliser la politique de rétention pour les compartiments Amazon S3 qui stockent vos CloudTrail journaux AWS Control Tower. Vous pouvez personnaliser votre politique de conservation des journaux Amazon S3, par tranches de jours ou d'années, jusqu'à un maximum de 15 ans.

Si vous choisissez de ne pas personnaliser la conservation des journaux, les paramètres par défaut sont de 1 an pour la journalisation standard du compte et de 10 ans pour la journalisation des accès.

Cette fonctionnalité est disponible pour les clients existants via AWS Control Tower lorsque vous mettez à jour ou réparez votre zone d'atterrissage, et pour les nouveaux clients via le processus de configuration d'AWS Control Tower.

Réparation de la dérive des rôles disponible

11 août 2022

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower prend désormais en charge la réparation de la dérive des rôles. Vous pouvez rétablir un rôle requis sans avoir à réparer complètement votre zone d'atterrissage. Si ce type de réparation de dérive est nécessaire, la page d'erreur de la console indique les étapes à suivre pour restaurer le rôle, afin que votre zone d'atterrissage soit à nouveau disponible.

Zone de landing zone d'AWS Control Tower, version 3.0

29 juillet 2022

(Mise à jour requise pour la zone de landing zone d'AWS Control Tower vers la version 3.0. Pour plus d'informations, voirMettre à jour votre zone de destination)

La version 3.0 de la zone de landing zone d'AWS Control Tower inclut les mises à jour suivantes :

- La possibilité de choisir des AWS CloudTrail parcours au niveau de l'organisation ou de se désinscrire des CloudTrail sentiers gérés par AWS Control Tower.
- Deux nouvelles commandes de détection pour déterminer si des activités AWS CloudTrail de journalisation sont enregistrées sur vos comptes.
- La possibilité d'agréger AWS Config des informations sur les ressources mondiales de votre région d'origine uniquement.
- Une mise à jour de la Région refuse le contrôle.
- Une mise à jour de la politique gérée, AWSControlTowerServiceRolePolicy.
- Nous ne créons plus le rôle IAM ni `aws-controltower-CloudWatchLogsRole` le groupe de CloudWatch log `aws-controltower/CloudTrailLogs` dans chaque compte inscrit. Auparavant, nous les avions créés dans chaque compte pour le suivi de son compte. Avec les parcours d'organisation, nous n'en créons qu'un dans le compte de gestion.

Les sections suivantes fournissent plus de détails sur chaque nouvelle fonctionnalité.

CloudTrail Sentiers au niveau de l'organisation dans AWS Control Tower

Avec la version 3.0 de landing zone, AWS Control Tower prend désormais en charge les trails au niveau de l'organisation AWS CloudTrail .

Lorsque vous mettez à jour votre zone d'atterrissage AWS Control Tower vers la version 3.0, vous avez la possibilité de sélectionner les AWS CloudTrail sentiers au niveau de l'organisation comme préférence de journalisation, ou de vous désinscrire des CloudTrail sentiers gérés par AWS Control Tower. Lorsque vous passez à la version 3.0, AWS Control Tower supprime les traces existantes au niveau du compte pour les comptes inscrits après une période d'attente de 24 heures. AWS Control Tower ne supprime pas les traces au niveau du compte pour les comptes non inscrits. Dans le cas peu probable où la mise à jour de votre zone d'atterrissage échouerait, mais que l'échec se produirait alors qu'AWS Control Tower a déjà créé le journal au niveau de l'organisation, vous risquez de devoir payer des frais supplémentaires pour les journaux au niveau de l'organisation et au niveau du compte, jusqu'à ce que votre opération de mise à jour soit terminée avec succès.

À compter de la landing zone 3.0, AWS Control Tower ne prend plus en charge les traces de gestion au niveau du compte. AWS AWS Control Tower crée plutôt un journal au niveau de l'organisation, actif ou inactif, en fonction de votre sélection.

> **Note**
>
> Après la mise à jour vers la version 3.0 ou ultérieure, vous n'avez pas la possibilité de continuer avec les CloudTrail traces au niveau du compte gérées par AWS Control Tower.

Aucune donnée de journalisation n'est perdue dans les journaux agrégés de votre compte, car les journaux restent dans le compartiment Amazon S3 existant dans lequel ils sont stockés. Seuls les sentiers sont supprimés, pas les journaux existants. Si vous sélectionnez l'option permettant d'ajouter des traces au niveau de l'organisation, AWS Control Tower ouvre un nouveau chemin vers un nouveau dossier dans votre compartiment Amazon S3 et continue d'envoyer les informations de journalisation à cet emplacement. Si vous choisissez de ne pas participer aux sentiers gérés par AWS Control Tower, vos journaux existants restent inchangés dans le compartiment.

Conventions de dénomination des chemins pour le stockage des journaux

- Les journaux de suivi des comptes sont stockés avec un chemin de la forme suivante : `/org id/AWSLogs/…`

- Les journaux de suivi des organisations sont stockés sous la forme suivante : `/org id/AWSLogs/org id/…`

Le chemin créé par AWS Control Tower pour les CloudTrail sentiers au niveau de votre organisation est différent du chemin par défaut pour un journal créé manuellement au niveau de l'organisation, qui aurait la forme suivante :

- `/AWSLogs/org id/…`

Pour plus d'informations sur la dénomination des CloudTrail chemins, consultez la section Trouver vos fichiers CloudTrail journaux.

> **Tip**
>
> Si vous envisagez de créer et de gérer vos propres traces au niveau de votre compte, nous vous recommandons de créer les nouvelles pistes avant de terminer la mise à jour de la version 3.0 de la zone de landing zone d'AWS Control Tower, afin de commencer à vous connecter immédiatement.

À tout moment, vous pouvez choisir de créer de nouveaux CloudTrail parcours au niveau du compte ou de l'organisation et de les gérer vous-même. La possibilité de choisir des CloudTrail pistes au niveau de l'organisation gérées par AWS Control Tower est disponible lors de toute mise à jour de la zone de landing zone vers la version 3.0 ou ultérieure. Vous pouvez accepter ou non les parcours organisés au niveau de l'organisation chaque fois que vous mettez à jour votre zone de landing zone.

Si vos journaux sont gérés par un service tiers, assurez-vous de donner le nouveau nom de chemin d'accès à votre service.

> **Note**
>
> Pour les zones d'atterrissage de la version 3.0 ou ultérieure, les AWS CloudTrail traces au niveau du compte ne sont pas prises en charge par AWS Control Tower. Vous pouvez créer et gérer vos propres traces au niveau de votre compte à tout moment, ou vous pouvez opter pour les pistes au niveau de l'organisation gérées par AWS Control Tower.

Enregistrer AWS Config les ressources de la région d'origine uniquement

Dans la version 3.0 de landing zone, AWS Control Tower a mis à jour la configuration de base AWS Config afin d'enregistrer les ressources globales dans la région d'origine uniquement. Après la mise à jour vers la version 3.0, l'enregistrement des ressources pour les ressources globales est activé uniquement dans votre région d'origine.

Cette configuration est considérée comme une bonne pratique. Il est recommandé par AWS Security Hub et AWS Config permet de réaliser des économies en réduisant le nombre d'éléments de configuration créés lors de la création, de la modification ou de la suppression de ressources globales. Auparavant, chaque fois qu'une ressource globale était créée, mise à jour ou supprimée, que ce soit par un client ou par un AWS service, un élément de configuration était créé pour chaque élément dans chaque région gouvernée.

Deux nouvelles commandes de détection pour la AWS CloudTrail journalisation

Dans le cadre de la modification des AWS CloudTrail pistes au niveau de l'organisation, AWS Control Tower introduit deux nouvelles commandes de détection qui vérifient si elles CloudTrail sont activées. Le premier contrôle comporte des instructions obligatoires et il est activé sur l'unité d'organisation de sécurité lors de la configuration ou des mises à jour de la zone d'atterrissage de la version 3.0 et des versions ultérieures. Le second contrôle fait l'objet de directives fortement recommandées et est éventuellement appliqué à toute unité d'organisation autre que l'unité d'organisation de sécurité, pour laquelle la protection de contrôle obligatoire est déjà appliquée.

Contrôle obligatoire : détecter si les comptes partagés relevant de l'unité organisationnelle de sécurité sont activés AWS CloudTrail ou si CloudTrail Lake est activé

Contrôle fortement recommandé : détectez si un compte est activé AWS CloudTrail ou si CloudTrail Lake est activé

Pour plus d'informations sur les nouveaux contrôles, consultez la bibliothèque de contrôles AWS Control Tower.

Une mise à jour du contrôle des refus par région

Nous avons mis à jour la NotActionliste dans la section Region Deny Control pour inclure les actions de certains services supplémentaires, listés ci-dessous :

```
            “chatbot:*”,
            "s3:GetAccountPublic",
            "s3:DeleteMultiRegionAccessPoint",
```

```
            "s3:DescribeMultiRegionAccessPointOperation",
            "s3:GetMultiRegionAccessPoint",
            "s3:GetMultiRegionAccessPointPolicy",
            "s3:GetMultiRegionAccessPointPolicyStatus",
            "s3:ListMultiRegionAccessPoints",
            "s3:GetStorageLensConfiguration",
            “s3:GetStorageLensDashboard",
            “s3:ListStorageLensConfigurations”
            “s3:GetAccountPublicAccessBlock“,,
            “s3:PutAccountPublic",
            “s3:PutAccountPublicAccessBlock“,
```

Vidéo de procédure

Cette vidéo (3:07) explique comment mettre à jour votre zone d'atterrissage AWS Control Tower existante vers la version 3. Pour un visionnage de meilleure qualité, sélectionnez l'icône dans le coin inférieur droit de la vidéo pour l'afficher en plein écran. Le sous-titrage est disponible.

Présentation vidéo de la mise à jour d'une zone d'atterrissage AWS Control Tower existante vers la zone d'atterrissage 3.

La page Organisation combine les vues des unités d'organisation et des comptes

18 juillet 2022

(Aucune mise à jour requise pour la zone d'atterrissage d'AWS Control Tower)

La nouvelle page Organisation d'AWS Control Tower présente une vue hiérarchique de toutes les unités organisationnelles (UO) et de tous les comptes. Il combine les informations des pages UO et Comptes, qui existaient auparavant.

Sur la nouvelle page, vous pouvez voir les relations entre les UO parents et leurs UO et comptes imbriqués. Vous pouvez agir sur les groupements de ressources. Vous pouvez configurer l'affichage des pages. Par exemple, vous pouvez développer ou réduire la vue hiérarchique, filtrer la vue pour afficher uniquement les comptes ou les unités d'organisation, choisir de n'afficher que vos comptes inscrits et vos unités d'organisation enregistrées, ou vous pouvez afficher des groupes de ressources connexes. Il est plus facile de s'assurer que l'ensemble de votre organisation est correctement mis à jour.

Inscription et mise à jour simplifiées pour les comptes de membres individuels

31 mai 2022

(Aucune mise à jour requise pour la zone d'atterrissage d'AWS Control Tower)

AWS Control Tower vous offre désormais une capacité améliorée pour mettre à jour et inscrire les comptes des membres individuellement. Chaque compte indique quand une mise à jour est disponible, ce qui vous permet de vous assurer plus facilement que vos comptes membres incluent la dernière configuration. Vous pouvez mettre à jour votre zone de landing zone, remédier à la dérive de votre compte ou inscrire un compte dans une unité d'organisation enregistrée, en quelques étapes simples.

Lorsque vous mettez à jour un compte, il n'est pas nécessaire d'inclure l'unité organisationnelle (UO) complète du compte dans chaque action de mise à jour. Par conséquent, le temps nécessaire pour mettre à jour un compte individuel est considérablement réduit.

Vous pouvez inscrire des comptes dans les unités d'organisation AWS Control Tower avec l'aide supplémentaire de la console AWS Control Tower. Les comptes existants que vous inscrivez dans AWS Control Tower doivent toujours répondre aux conditions requises, et vous devez ajouter le `AWSControlTowerExecution` rôle. Ensuite, vous pouvez choisir n'importe quelle unité d'organisation enregistrée et y inscrire le compte en cliquant sur le bouton S'inscrire.

Nous avons séparé la fonctionnalité d'inscription d'un compte du flux de travail de création de compte dans Account Factory, afin de mieux distinguer ces processus similaires et d'éviter les erreurs de configuration lors de la saisie des informations de compte.

AFT prend en charge la personnalisation automatique des comptes AWS Control Tower partagés

27 mai 2022

(Aucune mise à jour requise pour la zone d'atterrissage d'AWS Control Tower)

Account Factory for Terraform (AFT) peut désormais personnaliser et mettre à jour par programmation tous vos comptes gérés par AWS Control Tower, y compris le compte de gestion, le compte d'audit et le compte d'archivage des journaux, ainsi que vos comptes inscrits. Vous pouvez centraliser la personnalisation de votre compte et la gestion des mises à jour, tout en protégeant la sécurité des configurations de votre compte, car vous définissez le rôle qui exécute le travail.

Le AWSAFTExecutionrôle existant déploie désormais les personnalisations dans tous les comptes. Vous pouvez configurer des autorisations IAM avec des limites qui limitent l'accès au AWSAFTExecutionrôle en fonction de vos exigences commerciales et de sécurité. Vous pouvez également déléguer par programmation les autorisations de personnalisation approuvées dans ce rôle, pour les utilisateurs de confiance. En tant que bonne pratique, nous vous recommandons de limiter les autorisations à celles qui sont nécessaires pour déployer les personnalisations requises.

AFT crée désormais le nouveau AWSAFTServicerôle pour déployer les ressources AFT dans tous les comptes gérés, y compris les comptes partagés et le compte de gestion. Les ressources étaient auparavant déployées par le AWSAFTExecutionrôle.

Les comptes partagés et de gestion d'AWS Control Tower ne sont pas approvisionnés via Account Factory, ils ne contiennent donc pas de produits provisionnés correspondants. AWS Service Catalog Par conséquent, vous n'êtes pas en mesure de mettre à jour les comptes partagés et de gestion dans Service Catalog.

Opérations simultanées pour tous les contrôles optionnels

18 mai 2022

(Aucune mise à jour requise pour la zone d'atterrissage d'AWS Control Tower)

AWS Control Tower prend désormais en charge les opérations simultanées pour les contrôles préventifs, ainsi que pour les contrôles de détection.

Grâce à cette nouvelle fonctionnalité, toute commande optionnelle peut désormais être appliquée ou supprimée simultanément, améliorant ainsi la facilité d'utilisation et les performances de toutes les commandes optionnelles. Vous pouvez activer plusieurs contrôles optionnels sans attendre la fin des opérations de contrôle individuelles. Les seules périodes restreintes sont celles où AWS Control Tower est en train de configurer sa zone de landing zone ou lors de l'extension de la gouvernance à une nouvelle organisation.

Fonctionnalités prises en charge pour les contrôles préventifs :

- Appliquez et supprimez différents contrôles préventifs sur la même unité d'organisation.
- Appliquez et supprimez simultanément différents contrôles préventifs sur différentes unités d'organisation.
- Appliquez et supprimez le même contrôle préventif sur plusieurs unités d'organisation simultanément.

- Vous pouvez appliquer et supprimer simultanément tous les contrôles préventifs et de détection.

Vous pouvez découvrir ces améliorations de la simultanéité des contrôles dans toutes les versions publiées d'AWS Control Tower.

Lorsque vous appliquez des contrôles préventifs à des unités d'organisation imbriquées, les contrôles préventifs affectent tous les comptes et unités d'organisation imbriqués sous l'unité d'organisation cible, même si ces comptes et unités d'organisation ne sont pas enregistrés auprès d'AWS Control Tower. Les contrôles préventifs sont mis en œuvre à l'aide des politiques de contrôle des services (SCP), qui en font partie AWS Organizations. Les contrôles Detective sont mis en œuvre à l'aide de AWS Config règles. Les garde-fous restent en vigueur lorsque vous créez de nouveaux comptes ou que vous apportez des modifications à vos comptes existants, et AWS Control Tower fournit un rapport récapitulatif indiquant dans quelle mesure chaque compte est conforme aux politiques que vous avez activées. Pour obtenir la liste complète des contrôles disponibles, consultez la bibliothèque de contrôles AWS Control Tower.

Comptes de sécurité et de journalisation existants

16 mai 2022

(Disponible lors de la configuration initiale.)

AWS Control Tower vous permet désormais de spécifier un AWS compte existant en tant que compte de sécurité ou de journalisation AWS Control Tower, lors du processus de configuration initiale de la zone de landing zone. Grâce à cette option, AWS Control Tower n'a plus besoin de créer de nouveaux comptes partagés. Le compte de sécurité, appelé compte d'audit par défaut, est un compte restreint qui permet à vos équipes de sécurité et de conformité d'accéder à tous les comptes de votre zone de landing zone. Le compte de journalisation, appelé compte Log Archive par défaut, fonctionne comme un référentiel. Il stocke les journaux des activités de l'API et des configurations de ressources de tous les comptes de votre zone de landing zone.

En intégrant vos comptes de sécurité et de journalisation existants, il est plus facile d'étendre la gouvernance d'AWS Control Tower à vos organisations existantes ou de passer à AWS Control Tower depuis une autre zone de landing zone. L'option vous permettant d'utiliser les comptes existants s'affiche lors de la configuration initiale de la zone d'atterrissage. Il inclut des contrôles pendant le processus de configuration, qui garantissent le succès du déploiement. AWS Control Tower implémente les rôles et les contrôles nécessaires sur vos comptes existants. Il ne supprime ni ne fusionne aucune ressource ou donnée existante dans ces comptes.

Limitation : si vous envisagez d'intégrer AWS des comptes existants dans AWS Control Tower en tant que comptes d'audit et d'archivage des journaux, et si ces comptes disposent de AWS Config ressources existantes, vous devez supprimer les AWS Config ressources existantes avant de pouvoir les inscrire dans AWS Control Tower.

Zone de landing zone d'AWS Control Tower, version 2.9

22 avril 2022

(Mise à jour requise pour la zone de landing zone d'AWS Control Tower vers la version 2.9. Pour plus d'informations, voirMettre à jour votre zone de destination)

La version 2.9 d'AWS Control Tower landing zone met à jour le redirecteur de notifications Lambda pour qu'il utilise le runtime Python version 3.9. Cette mise à jour corrige la dépréciation de la version 3.6 de Python, prévue pour juillet 2022. Pour les informations les plus récentes, consultez la page d'obsolescence de Python.

Zone de landing zone d'AWS Control Tower, version 2.8

10 février 2022

(Mise à jour requise pour la zone de landing zone d'AWS Control Tower vers la version 2.8. Pour plus d'informations, voirMettre à jour votre zone de destination)

La version 2.8 de la zone de landing zone d'AWS Control Tower ajoute des fonctionnalités conformes aux récentes mises à jour des meilleures pratiques AWS fondamentales en matière de sécurité.

Dans cette version :

- La journalisation des accès est configurée pour le compartiment de journaux d'accès du compte Log Archive, afin de suivre l'accès au compartiment de journaux d'accès S3 existant.
- Support pour la politique de cycle de vie est ajouté. Le journal d'accès du compartiment de journaux d'accès S3 existant est défini sur une durée de conservation par défaut de 10 ans.
- En outre, cette version met à jour AWS Control Tower afin d'utiliser le rôle AWS Service Linked (SLR) fourni par AWS Config, dans tous les comptes gérés (à l'exception du compte de gestion), afin que vous puissiez configurer et gérer les règles de configuration conformément aux AWS Config meilleures pratiques. Les clients qui ne procèdent pas à la mise à niveau continueront à utiliser leur rôle existant.
- Cette version rationalise le processus de configuration KMS d'AWS Control Tower pour le chiffrement AWS Config des données et améliore les messages d'état associés dans. CloudTrail

- La version inclut une mise à jour du contrôle de refus des régions, afin de permettre à la `route53-application-recovery` fonctionnalité d'entrer dans`us-west-2`.
- Mise à jour : le 15 février 2022, nous avons supprimé la file d'attente des lettres mortes pour les fonctions AWS Lambda.

Informations supplémentaires :

- Si vous mettez hors service votre zone de landing zone, AWS Control Tower ne supprime pas le rôle lié au AWS Config service.
- Si vous désapprovisionnez un compte Account Factory, AWS Control Tower ne supprime pas le rôle lié au AWS Config service.

Pour mettre à jour votre zone d'atterrissage vers la version 2.8, accédez à la page des paramètres de la zone d'atterrissage, sélectionnez la version 2.8, puis choisissez Mettre à jour. Après avoir mis à jour votre zone de landing zone, vous devez mettre à jour tous les comptes régis par AWS Control Tower, comme indiqué dansGestion des mises à jour de configuration dans AWS Control Tower.

janvier - décembre 2021

En 2021, AWS Control Tower a publié les mises à jour suivantes :

- Fonctionnalités de refus régional
- Fonctionnalités de résidence des données
- AWS Control Tower présente le provisionnement et la personnalisation des comptes Terraform
- Nouvel événement du cycle de vie disponible
- AWS Control Tower permet des unités d'organisation imbriquées
- Detective Control Concurrence
- Deux nouvelles régions disponibles
- Désélection de région
- AWS Control Tower fonctionne avec des systèmes de gestion des AWS clés
- Contrôles renommés, fonctionnalités inchangées
- AWS Control Tower scanne les SCP tous les jours pour vérifier leur dérive
- Noms personnalisés pour les unités d'organisation et les comptes
- Zone de landing zone d'AWS Control Tower, version 2.7

- Trois nouvelles AWS régions disponibles
- Gouverner uniquement les régions sélectionnées
- AWS Control Tower étend désormais la gouvernance aux unités d'organisation existantes de vos AWS organisations
- AWS Control Tower fournit des mises à jour de compte en masse

Fonctionnalités de refus régional

30 novembre 2021

(Aucune mise à jour n'est requise pour la zone d'atterrissage d'AWS Control Tower.)

AWS Control Tower propose désormais des fonctionnalités de refus de région, qui vous aident à limiter l'accès aux AWS services et aux opérations pour les comptes inscrits dans votre environnement AWS Control Tower. La fonctionnalité de refus de région complète les fonctionnalités de sélection et de désélection de région existantes dans AWS Control Tower. Ensemble, ces fonctionnalités vous aident à résoudre les problèmes de conformité et de réglementation, tout en équilibrant les coûts associés à l'expansion dans de nouvelles régions.

Par exemple, AWS les clients en Allemagne peuvent refuser l'accès aux AWS services dans les régions situées en dehors de la région de Francfort. Vous pouvez sélectionner des régions restreintes lors du processus de configuration d'AWS Control Tower ou sur la page des paramètres de la zone d'atterrissage. La fonctionnalité Region Deny est disponible lorsque vous mettez à jour votre version de la zone de landing zone d'AWS Control Tower. Certains AWS services sont exemptés des fonctionnalités de refus par région. Pour en savoir plus, voir Configurer le contrôle de refus des régions.

Fonctionnalités de résidence des données

30 novembre 2021

(Aucune mise à jour requise pour la zone d'atterrissage d'AWS Control Tower)

AWS Control Tower propose désormais des contrôles spécialement conçus pour garantir que les données clients que vous téléchargez vers les AWS services se trouvent uniquement dans les AWS régions que vous spécifiez. Vous pouvez sélectionner la AWS ou les régions dans lesquelles les données de vos clients sont stockées et traitées. Pour obtenir la liste complète des AWS régions dans lesquelles AWS Control Tower est disponible, consultez le tableau des AWS régions.

Pour un contrôle granulaire, vous pouvez appliquer des contrôles supplémentaires, tels que Interdire les connexions Amazon Virtual Private Network (VPN) ou interdire l'accès à Internet pour une instance Amazon VPC. Vous pouvez consulter l'état de conformité des contrôles dans la console AWS Control Tower. Pour obtenir la liste complète des contrôles disponibles, consultez la bibliothèque de contrôles AWS Control Tower.

AWS Control Tower présente le provisionnement et la personnalisation des comptes Terraform

29 novembre 2021

(Mise à jour facultative pour la zone de landing zone d'AWS Control Tower)

Vous pouvez désormais utiliser Terraform pour provisionner et mettre à jour des comptes personnalisés via AWS Control Tower, avec AWS Control Tower Account Factory for Terraform (AFT).

AFT fournit un pipeline unique d'infrastructure Terraform en tant que code (IaC), qui approvisionne les comptes gérés par AWS Control Tower. Les personnalisations effectuées au cours du provisionnement permettent de respecter vos politiques commerciales et de sécurité, avant que vous ne donniez les comptes aux utilisateurs finaux.

Le pipeline de création de compte automatisé AFT surveille jusqu'à ce que le provisionnement du compte soit terminé, puis il continue, déclenchant des modules Terraform supplémentaires qui améliorent le compte avec les personnalisations nécessaires. Dans le cadre du processus de personnalisation, vous pouvez configurer le pipeline pour installer vos propres modules Terraform personnalisés, et vous pouvez choisir d'ajouter l'une des options de fonctionnalité AFT, fournies par AWS pour les personnalisations courantes.

Commencez à utiliser AWS Control Tower Account Factory pour Terraform en suivant les étapes décrites dans le guide de l'utilisateur d'AWS Control Tower et en téléchargeant AFT pour votre instance Terraform. Déployez AWS Control Tower Account Factory pour Terraform (AFT) AFT prend en charge les distributions Open Source Terraform Cloud, Terraform Enterprise et Terraform.

Nouvel événement du cycle de vie disponible

18 novembre 2021

(Aucune mise à jour requise pour la zone d'atterrissage d'AWS Control Tower)

L'`PrecheckOrganizationalUnit`événement enregistre si des ressources bloquent le succès de la tâche de gouvernance Extend, y compris les ressources des unités d'organisation imbriquées. Pour plus d'informations, consultez `PrecheckOrganizationalUnit`.

AWS Control Tower permet des unités d'organisation imbriquées

16 novembre 2021

(Aucune mise à jour requise pour la zone d'atterrissage d'AWS Control Tower)

AWS Control Tower vous permet désormais d'inclure des unités d'organisation imbriquées dans votre zone de landing zone.

AWS Control Tower prend en charge les unités organisationnelles (UO) imbriquées, ce qui vous permet d'organiser les comptes en plusieurs niveaux hiérarchiques et d'appliquer des contrôles préventifs de manière hiérarchique. Vous pouvez enregistrer des unités d'organisation contenant des unités d'organisation imbriquées, créer et enregistrer des unités d'organisation sous des unités d'organisation parentes et activer des contrôles sur toutes les unités d'organisation enregistrées, quelle que soit leur profondeur. Pour prendre en charge cette fonctionnalité, la console indique le nombre de comptes et d'unités d'organisation gouvernés.

Avec les unités d'organisation imbriquées, vous pouvez aligner vos unités d'organisation AWS Control Tower sur la stratégie AWS multi-comptes, et vous pouvez réduire le temps nécessaire pour activer les contrôles sur plusieurs unités d'organisation, en appliquant les contrôles au niveau de l'unité d'organisation parent.

Considérations clés

1. Vous pouvez enregistrer des unités d'organisation à plusieurs niveaux existantes auprès d'AWS Control Tower, une unité d'organisation à la fois, en commençant par l'unité d'organisation de niveau supérieur, puis en descendant dans l'arborescence. Pour plus d'informations, consultez Passez d'une structure d'unité d'organisation plate à une structure d'unité d'organisation imbriquée.
2. Les comptes relevant directement d'une unité d'organisation enregistrée sont inscrits automatiquement. Les comptes situés plus bas dans l'arborescence peuvent être inscrits en enregistrant leur OU parent immédiat.
3. Les contrôles préventifs (SCP) sont hérités automatiquement vers le bas de la hiérarchie ; les SCP appliqués au parent sont hérités par toutes les unités d'organisation imbriquées.
4. Les contrôles Detective (règles de AWS configuration) ne sont PAS hérités automatiquement.

5. La conformité aux contrôles de détection est signalée par chaque unité d'organisation.
6. La dérive du SCP sur une unité d'organisation affecte tous les comptes et unités d'organisation associés à celle-ci.
7. Vous ne pouvez pas créer de nouvelles unités d'organisation imbriquées sous l'unité d'organisation de sécurité (unité d'organisation principale).

Detective Control Concurrence

5 novembre 2021

(Mise à jour facultative pour la zone de landing zone d'AWS Control Tower)

Les contrôles de détection d'AWS Control Tower prennent désormais en charge les opérations simultanées pour les contrôles de détection, ce qui améliore la facilité d'utilisation et les performances. Vous pouvez activer plusieurs contrôles de détection sans attendre la fin des opérations de contrôle individuelles.

Fonctionnalités prises en charge :

- Activez différents contrôles de détection sur la même unité d'organisation (par exemple, détectez si le MFA est activé pour l'utilisateur root et détectez si l'accès public en écriture aux compartiments Amazon S3 est autorisé).
- Activez simultanément différentes commandes de détection sur différentes unités d'organisation.
- La messagerie d'erreur Guardrail a été améliorée afin de fournir des conseils supplémentaires pour les opérations de contrôle simultanées prises en charge.

Non pris en charge dans cette version :

- L'activation simultanée du même contrôle de détection sur plusieurs unités d'organisation n'est pas prise en charge.
- La simultanéité des contrôles préventifs n'est pas prise en charge.

Vous pouvez découvrir les améliorations apportées par Detective Control à la concurrence dans toutes les versions d'AWS Control Tower. Il est recommandé aux clients qui n'utilisent pas actuellement la version 2.7 d'effectuer une mise à jour de la zone d'atterrissage afin de bénéficier d'autres fonctionnalités, telles que la sélection et la désélection de régions, disponibles dans la dernière version.

Deux nouvelles régions disponibles

29 juillet 2021

(Mise à jour requise pour la zone de landing zone d'AWS Control Tower)

AWS Control Tower est désormais disponible dans deux AWS régions supplémentaires : l'Amérique du Sud (Sao Paulo) et l'Europe (Paris). Cette mise à jour étend la disponibilité d'AWS Control Tower à 15 AWS régions.

Si vous utilisez AWS Control Tower pour la première fois, vous pouvez le lancer immédiatement dans toutes les régions prises en charge. Lors du lancement, vous pouvez sélectionner les régions dans lesquelles vous souhaitez qu'AWS Control Tower crée et gère votre environnement multi-comptes.

Si vous disposez déjà d'un environnement AWS Control Tower et que vous souhaitez étendre ou supprimer les fonctionnalités de gouvernance d'AWS Control Tower dans une ou plusieurs régions prises en charge, rendez-vous sur la page des paramètres de la zone d'atterrissage de votre tableau de bord AWS Control Tower, puis sélectionnez les régions. Après avoir mis à jour votre zone de landing zone, vous devez mettre à jour tous les comptes régis par AWS Control Tower.

Désélection de région

29 juillet 2021

(Mise à jour facultative pour la zone de landing zone d'AWS Control Tower)

La désélection de la région AWS Control Tower améliore votre capacité à gérer l'empreinte géographique de vos ressources AWS Control Tower. Vous pouvez désélectionner les régions que vous ne souhaitez plus confier à AWS Control Tower. Cette fonctionnalité vous permet de résoudre les problèmes de conformité et de réglementation tout en équilibrant les coûts associés à l'expansion dans de nouvelles régions.

La désélection de région est disponible lorsque vous mettez à jour la version de la zone de landing zone d'AWS Control Tower.

Lorsque vous utilisez Account Factory pour créer un nouveau compte ou inscrire un compte de membre préexistant, ou lorsque vous sélectionnez Extend Governance pour inscrire des comptes dans une unité organisationnelle préexistante, AWS Control Tower déploie ses capacités de gouvernance, notamment la journalisation, la surveillance et les contrôles centralisés, dans les régions que vous avez choisies dans les comptes. Choisir de désélectionner une région et de supprimer la gouvernance d'AWS Control Tower de cette région supprime cette fonctionnalité de

gouvernance, mais cela n'empêche pas vos utilisateurs de déployer des AWS ressources ou des charges de travail dans ces régions.

AWS Control Tower fonctionne avec des systèmes de gestion des AWS clés

28 juillet 2021

(Mise à jour facultative pour la zone de landing zone d'AWS Control Tower)

AWS Control Tower vous offre la possibilité d'utiliser une AWS clé du service de gestion des clés (AWS KMS). Une clé est fournie et gérée par vous pour sécuriser les services déployés par AWS Control Tower, y compris AWS CloudTrail AWS Config, et les données Amazon S3 associées. AWS Le chiffrement KMS est un niveau de chiffrement amélioré par rapport au chiffrement SSE-S3 qu'AWS Control Tower utilise par défaut.

L'intégration du support AWS KMS dans AWS Control Tower est conforme aux bonnes pratiques AWS fondamentales en matière de sécurité, qui recommandent une couche de sécurité supplémentaire pour vos fichiers journaux sensibles. Vous devez utiliser des clés AWS gérées par KMS (SSE-KMS) pour le chiffrement au repos. AWS La prise en charge du chiffrement KMS est disponible lorsque vous configurez une nouvelle zone d'atterrissage ou lorsque vous mettez à jour votre zone d'atterrissage AWS Control Tower existante.

Pour configurer cette fonctionnalité, vous pouvez sélectionner la configuration des clés KMS lors de la configuration initiale de votre zone d'atterrissage. Vous pouvez choisir une clé KMS existante ou sélectionner un bouton qui vous dirige vers la console AWS KMS pour en créer une nouvelle. Vous avez également la possibilité de passer du chiffrement par défaut au SSE-KMS ou à une autre clé SSE-KMS.

Pour une zone de landing zone AWS Control Tower existante, vous pouvez effectuer une mise à jour pour commencer à utiliser les clés AWS KMS.

Contrôles renommés, fonctionnalités inchangées

26 juillet 2021

(Aucune mise à jour requise pour la zone d'atterrissage d'AWS Control Tower)

AWS Control Tower est en train de réviser certains noms et descriptions de contrôle afin de mieux refléter les intentions politiques du contrôle. Les noms et descriptions révisés vous aident à

comprendre de manière plus intuitive la manière dont les contrôles incarnent les politiques de vos comptes. Par exemple, nous avons modifié en partie le nom des contrôles de détection, passant de « Interdire » à « Détecter », car le contrôle de détection lui-même n'arrête pas une action spécifique, il détecte uniquement les violations des politiques et émet des alertes via le tableau de bord.

Les fonctionnalités de contrôle, les instructions et la mise en œuvre restent inchangées. Seuls les noms et les descriptions des contrôles ont été révisés.

AWS Control Tower scanne les SCP tous les jours pour vérifier leur dérive

11 mai 2021

(Aucune mise à jour requise pour la zone d'atterrissage d'AWS Control Tower)

AWS Control Tower effectue désormais des analyses automatisées quotidiennes de vos SCP gérés afin de vérifier que les contrôles correspondants sont correctement appliqués et qu'ils n'ont pas été modifiés. Si un scan détecte une dérive, vous recevrez une notification. AWS Control Tower envoie une seule notification par problème de dérive. Ainsi, si votre zone d'atterrissage est déjà en état de dérive, vous ne recevrez aucune notification supplémentaire à moins qu'un nouvel élément de dérive ne soit trouvé.

Noms personnalisés pour les unités d'organisation et les comptes

16 avril 2021

(Aucune mise à jour requise pour la zone d'atterrissage d'AWS Control Tower)

AWS Control Tower vous permet désormais de personnaliser le nom de votre zone de landing zone. Vous pouvez conserver les noms recommandés par AWS Control Tower pour les unités organisationnelles (UO) et les comptes principaux, ou vous pouvez modifier ces noms lors du processus initial de configuration de la zone de landing zone.

Les noms par défaut fournis par AWS Control Tower pour les unités d'organisation et les comptes principaux sont conformes aux recommandations relatives aux bonnes pratiques AWS multicomptes. Toutefois, si votre entreprise applique des politiques de dénomination spécifiques, ou si vous possédez déjà une unité d'organisation ou un compte portant le même nom recommandé, la nouvelle fonctionnalité de dénomination des unités d'organisation et des comptes vous donne la flexibilité nécessaire pour répondre à ces contraintes.

Indépendamment de cette modification du flux de travail lors de la configuration, l'unité d'organisation auparavant connue sous le nom d'unité d'organisation principale est désormais appelée unité

d'organisation de sécurité, et l'unité d'organisation précédemment appelée unité d'organisation personnalisée est désormais appelée unité d'organisation Sandbox. Nous avons apporté cette modification afin de mieux nous aligner sur les directives générales relatives aux AWS meilleures pratiques en matière de dénomination.

Les nouveaux clients verront ces nouveaux noms d'unités d'organisation. Les clients existants continueront de voir les noms originaux de ces unités d'organisation. Il se peut que vous rencontriez des incohérences dans la dénomination des unités d'organisation lors de la mise à jour de notre documentation avec les nouveaux noms.

Pour commencer à utiliser AWS Control Tower depuis la console de AWS gestion, accédez à la console AWS Control Tower et sélectionnez Set up landing zone en haut à droite. Pour plus d'informations, vous pouvez en savoir plus sur la planification de votre zone d'atterrissage AWS Control Tower.

Zone de landing zone d'AWS Control Tower, version 2.7

8 avril 2021

(Mise à jour requise pour la zone de landing zone d'AWS Control Tower vers la version 2.7. Pour plus d'informations, voirMettre à jour votre zone de destination)

Avec la version 2.7 d'AWS Control Tower, AWS Control Tower introduit quatre nouveaux contrôles préventifs obligatoires d'archivage des journaux qui mettent en œuvre une politique portant uniquement sur les ressources de la tour de contrôle AWS. Nous avons ajusté les directives relatives à quatre contrôles d'archivage de journaux existants, passant de obligatoires à facultatifs, car ils définissent la politique pour les ressources extérieures à AWS Control Tower. Ce changement et cette extension de contrôle permettent de séparer la gouvernance des archives de journaux pour les ressources au sein d'AWS Control Tower de la gouvernance des ressources extérieures à AWS Control Tower.

Les quatre contrôles modifiés peuvent être utilisés conjointement avec les nouveaux contrôles obligatoires pour assurer la gouvernance d'un ensemble plus large d'archives de AWS journaux. Les environnements AWS Control Tower existants maintiendront ces quatre contrôles modifiés activés automatiquement, pour garantir la cohérence de l'environnement ; toutefois, ces contrôles facultatifs peuvent désormais être désactivés. Les nouveaux environnements AWS Control Tower doivent permettre tous les contrôles électifs. Les environnements existants doivent désactiver les contrôles auparavant obligatoires avant d'ajouter le chiffrement aux compartiments Amazon S3 qui ne sont pas déployés par AWS Control Tower.

Nouveaux contrôles obligatoires :

- Interdire les modifications apportées à la configuration de chiffrement pour les compartiments S3 créés par AWS Control Tower dans l'archive des journaux
- Interdire les modifications apportées à la configuration de journalisation pour les compartiments S3 créés par AWS Control Tower dans l'archive des journaux
- Interdire les modifications apportées à la politique des compartiments pour les compartiments S3 créés par AWS Control Tower dans les archives de journaux
- Interdire les modifications apportées à la configuration du cycle de vie pour les compartiments S3 créés par AWS Control Tower dans l'archive des journaux

Les directives sont passées de obligatoires à facultatives :

- Interdire les modifications apportées à la configuration du chiffrement pour tous les compartiments Amazon S3 [Auparavant : activer le chiffrement au repos pour l'archivage des journaux]
- Interdire les modifications apportées à la configuration de journalisation pour tous les compartiments Amazon S3 [Auparavant : activer la journalisation des accès pour l'archivage des journaux]
- Interdire les modifications apportées à la politique des compartiments pour tous les compartiments Amazon S3 [Auparavant : interdire les modifications de politique relatives à l'archivage des journaux]
- Interdire les modifications apportées à la configuration du cycle de vie pour tous les compartiments Amazon S3 [Auparavant : définir une politique de conservation pour l'archivage des journaux]

La version 2.7 d'AWS Control Tower inclut des modifications apportées au plan de la zone d'atterrissage d'AWS Control Tower qui peuvent entraîner une incompatibilité avec les versions précédentes après la mise à niveau vers la version 2.7.

- En particulier, la version 2.7 d'AWS Control Tower `BlockPublicAccess` s'active automatiquement sur les compartiments S3 déployés par AWS Control Tower. Vous pouvez désactiver cette valeur par défaut si votre charge de travail nécessite un accès à plusieurs comptes. Pour plus d'informations sur ce qui se passe lorsque `BlockPublicaccess` cette option est activée, consultez Blocage de l'accès public à votre espace de stockage Amazon S3.
- La version 2.7 d'AWS Control Tower inclut une exigence pour le protocole HTTPS. Toutes les demandes envoyées aux compartiments S3 déployés par AWS Control Tower doivent utiliser

le protocole SSL (Secure Socket Layer). Seules les requêtes HTTPS sont autorisées à être transmises. Si vous utilisez le protocole HTTP (sans SSL) comme point de terminaison pour envoyer les demandes, cette modification génère une erreur de refus d'accès, susceptible d'interrompre votre flux de travail. Cette modification ne peut pas être annulée après la mise à jour 2.7 de votre zone d'atterrissage.

Nous vous recommandons de modifier vos demandes afin d'utiliser le protocole TLS au lieu du protocole HTTP.

Trois nouvelles AWS régions disponibles

8 avril 2021

(Mise à jour requise pour la zone de landing zone d'AWS Control Tower)

AWS Control Tower est disponible dans trois AWS régions supplémentaires : la région Asie-Pacifique (Tokyo), la région Asie-Pacifique (Séoul) et la région Asie-Pacifique (Mumbai). Une mise à jour de la zone d'atterrissage vers la version 2.7 est nécessaire pour étendre la gouvernance à ces régions.

Votre zone de landing zone n'est pas automatiquement étendue à ces régions lorsque vous effectuez la mise à jour vers la version 2.7. Vous devez les afficher et les sélectionner dans le tableau des régions pour les inclure.

Gouverner uniquement les régions sélectionnées

19 février 2021

(Aucune mise à jour requise pour la zone d'atterrissage d'AWS Control Tower)

La sélection de la région AWS Control Tower permet de mieux gérer l'empreinte géographique de vos ressources AWS Control Tower. Pour augmenter le nombre de régions dans lesquelles vous hébergez AWS des ressources ou des charges de travail (pour des raisons de conformité, de réglementation, de coût ou autres), vous pouvez désormais sélectionner les régions supplémentaires à gouverner.

La sélection de la région est disponible lorsque vous configurez une nouvelle zone d'atterrissage ou que vous mettez à jour la version de votre zone d'atterrissage AWS Control Tower. Lorsque vous utilisez Account Factory pour créer un nouveau compte ou inscrire un compte de membre préexistant, ou lorsque vous utilisez Extend Governance pour inscrire des comptes dans une unité

organisationnelle préexistante, AWS Control Tower déploie ses capacités de gouvernance consistant à centraliser la journalisation, la surveillance et les contrôles dans les régions que vous avez choisies dans les comptes. Pour plus d'informations sur la sélection des régions, consultezConfigurez vos régions AWS Control Tower.

AWS Control Tower étend désormais la gouvernance aux unités d'organisation existantes de vos AWS organisations

28 janvier 2021

(Aucune mise à jour requise pour la zone d'atterrissage d'AWS Control Tower)

Étendez la gouvernance aux unités organisationnelles (UO) existantes (celles qui ne font pas partie d'AWS Control Tower) depuis la console AWS Control Tower. Grâce à cette fonctionnalité, vous pouvez intégrer des unités d'organisation de haut niveau et des comptes inclus sous la gouvernance d'AWS Control Tower. Pour plus d'informations sur l'extension de la gouvernance à l'ensemble d'une unité d'organisation, consultezEnregistrer une unité organisationnelle existante auprès d'AWS Control Tower.

Lorsque vous enregistrez une unité d'organisation, AWS Control Tower effectue une série de vérifications pour garantir la réussite de l'extension de la gouvernance et de l'inscription des comptes au sein de l'unité d'organisation. Pour plus d'informations sur les problèmes courants associés à l'enregistrement initial d'une unité d'organisation, consultezCauses courantes d'échec lors de l'enregistrement ou du réenregistrement.

Vous pouvez également consulter la page Web du produit AWS Control Tower ou YouTube visionner cette vidéo expliquant comment démarrer avec AWS Control Tower pour AWS Organizations.

AWS Control Tower fournit des mises à jour de compte en masse

28 janvier 2021

(Aucune mise à jour requise pour la zone d'atterrissage d'AWS Control Tower)

Grâce à la fonctionnalité de mise à jour groupée, vous pouvez désormais mettre à jour tous les comptes d'une unité AWS Organizations organisationnelle (UO) enregistrée contenant jusqu'à 300 comptes, en un seul clic, depuis le tableau de bord AWS Control Tower. Cela est particulièrement utile lorsque vous mettez à jour votre zone d'atterrissage AWS Control Tower et que vous devez également mettre à jour vos comptes inscrits pour les aligner sur la version actuelle de la zone d'atterrissage.

Cette fonctionnalité vous permet également de maintenir vos comptes à jour lorsque vous mettez à jour votre zone d'atterrissage AWS Control Tower pour l'étendre à de nouvelles régions, ou lorsque vous souhaitez réenregistrer une unité d'organisation pour vous assurer que tous les comptes de cette unité d'organisation sont soumis aux derniers contrôles appliqués. La mise à jour groupée des comptes élimine le besoin de mettre à jour un compte à la fois ou d'utiliser un script externe pour effectuer la mise à jour sur plusieurs comptes.

Pour plus d'informations sur la mise à jour d'une zone d'atterrissage, consultezMettre à jour votre zone de destination.

Pour plus d'informations sur l'enregistrement ou le réenregistrement d'une UO, consultezEnregistrer une unité organisationnelle existante auprès d'AWS Control Tower.

janvier - décembre 2020

En 2020, AWS Control Tower a publié les mises à jour suivantes :

- La console AWS Control Tower est désormais liée à des règles de AWS configuration externes
- AWS Control Tower est désormais disponible dans d'autres régions
- Mise à jour du garde-corps
- La console AWS Control Tower fournit plus de détails sur les unités d'organisation et les comptes
- Utilisez AWS Control Tower pour configurer de nouveaux AWS environnements multi-comptes dans AWS Organizations
- Personnalisations pour la solution AWS Control Tower
- Disponibilité générale de la version 2.3 d'AWS Control Tower
- Provisionnement de compte en une seule étape dans AWS Control Tower
- Outil de mise hors service d'AWS Control Tower
- Notifications d'événements relatifs au cycle de vie d'AWS Control Tower

La console AWS Control Tower est désormais liée à des règles de AWS configuration externes

29 décembre 2020

(Mise à jour requise pour la zone de landing zone d'AWS Control Tower vers la version 2.6. Pour plus d'informations, voirMettre à jour votre zone de destination)

AWS Control Tower inclut désormais un agrégateur au niveau de l'organisation, qui aide à détecter les règles de configuration AWS externes. Cela vous permet de voir dans la console AWS Control Tower l'existence de règles de AWS configuration créées en externe en plus des règles de AWS configuration créées par AWS Control Tower. L'agrégateur permet à AWS Control Tower de détecter les règles externes et de fournir un lien vers la console AWS Config sans qu'AWS Control Tower ait besoin d'accéder à des comptes non gérés.

Grâce à cette fonctionnalité, vous disposez désormais d'une vue consolidée des contrôles de détection appliqués à vos comptes, ce qui vous permet de suivre la conformité et de déterminer si vous avez besoin de contrôles supplémentaires pour votre compte. Pour plus d'informations, consultez Comment AWS Control Tower agrège les AWS Config règles dans les unités d'organisation et les comptes non gérés.

AWS Control Tower est désormais disponible dans d'autres régions

18 novembre 2020

(Mise à jour requise pour la zone de landing zone d'AWS Control Tower vers la version 2.5. Pour plus d'informations, voirMettre à jour votre zone de destination)

AWS Control Tower est désormais disponible dans 5 AWS régions supplémentaires :

- Région Asie-Pacifique (Singapour)
- Région Europe (Francfort)
- Région Europe (Londres)
- Région Europe (Stockholm)
- Région Canada (Centre)

L'ajout de ces 5 AWS régions est le seul changement introduit dans la version 2.5 d'AWS Control Tower.

AWS Control Tower est également disponible dans les régions USA Est (Virginie du Nord), USA Est (Ohio), USA Ouest (Oregon), Europe (Irlande) et Asie-Pacifique (Sydney). Avec ce lancement, AWS Control Tower est désormais disponible dans 10 AWS régions.

Cette mise à jour de la zone d'atterrissage inclut toutes les régions répertoriées et ne peut pas être annulée. Après avoir mis à jour votre zone de landing zone vers la version 2.5, vous devez mettre à jour manuellement tous les comptes inscrits pour qu'AWS Control Tower règne dans les 10 AWS

régions prises en charge. Pour plus d'informations, veuillez consulter Configurez vos régions AWS Control Tower.

Mise à jour du garde-corps

8 octobre 2020

(Aucune mise à jour requise pour la zone d'atterrissage d'AWS Control Tower)

Une version mise à jour a été publiée pour le contrôle obligatoire`AWS-GR_IAM_ROLE_CHANGE_PROHIBITED`.

Cette modification du contrôle est nécessaire car le `AWSControlTowerExecution` rôle doit être activé pour les comptes inscrits automatiquement dans AWS Control Tower. La version précédente du contrôle empêche la création de ce rôle.

Pour plus d'informations, consultez Interdire les modifications apportées aux rôles AWS IAM définis par AWS Control Tower et AWS CloudFormation dans le guide de référence d'AWS Control Tower Controls.

La console AWS Control Tower fournit plus de détails sur les unités d'organisation et les comptes

22 juillet 2020

(Aucune mise à jour requise pour la zone d'atterrissage d'AWS Control Tower)

Vous pouvez consulter vos organisations et comptes qui ne sont pas inscrits à AWS Control Tower, ainsi que les organisations et les comptes inscrits.

Dans la console AWS Control Tower, vous pouvez consulter plus de détails sur vos AWS comptes et unités organisationnelles (UO). La page Comptes répertorie désormais tous les comptes de votre organisation, quel que soit l'unité d'organisation ou le statut d'inscription dans AWS Control Tower. Vous pouvez désormais rechercher, trier et filtrer dans toutes les tables.

Utilisez AWS Control Tower pour configurer de nouveaux AWS environnements multi-comptes dans AWS Organizations

22 avril 2020

(Aucune mise à jour requise pour la zone d'atterrissage d'AWS Control Tower)

AWS Organizations les clients peuvent désormais utiliser AWS Control Tower pour gérer les unités organisationnelles (UO) et les comptes nouvellement créés en tirant parti de ces nouvelles fonctionnalités :

- AWS Organizations Les clients existants peuvent désormais configurer une nouvelle zone de landing zone pour les nouvelles unités organisationnelles (UO) dans leur compte de gestion existant. Vous pouvez créer de nouvelles unités d'organisation dans AWS Control Tower et créer de nouveaux comptes dans ces unités d'organisation grâce à la gouvernance d'AWS Control Tower.
- AWS Organizations les clients peuvent inscrire des comptes existants à l'aide du processus d'inscription ou à l'aide de scripts.

AWS Control Tower fournit un service d'orchestration qui utilise d'autres AWS services. Il est conçu pour les entreprises disposant de plusieurs comptes et pour les équipes qui recherchent le moyen le plus simple de configurer leur AWS environnement multi-comptes, nouveau ou existant, et de gouverner à grande échelle. Dans une organisation régie par AWS Control Tower, les administrateurs du cloud savent que les comptes de l'organisation sont conformes aux politiques établies. Les constructeurs en bénéficient car ils peuvent créer de nouveaux AWS comptes rapidement, sans se soucier indûment de la conformité.

Pour plus d'informations sur la configuration d'une zone d'atterrissage, consultezPlanifiez la zone de landing de votre AWS Control Tower. Vous pouvez également consulter la page Web du produit AWS Control Tower ou YouTube visionner cette vidéo expliquant comment démarrer avec AWS Control Tower pour AWS Organizations.

Outre cette modification, la fonctionnalité de provisionnement rapide des comptes dans AWS Control Tower a été renommée « Enroll account ». Il permet désormais l'enregistrement de AWS comptes existants ainsi que la création de nouveaux comptes. Pour plus d'informations, consultez Inscrire un compte existant.

Personnalisations pour la solution AWS Control Tower

17 mars 2020

(Aucune mise à jour requise pour la zone d'atterrissage d'AWS Control Tower)

AWS Control Tower inclut désormais une nouvelle implémentation de référence qui vous permet d'appliquer facilement des modèles et des politiques personnalisés à votre zone de landing AWS Control Tower.

Grâce aux personnalisations d'AWS Control Tower, vous pouvez utiliser des AWS CloudFormation modèles pour déployer de nouvelles ressources sur les comptes existants et nouveaux au sein de votre organisation. Vous pouvez également appliquer des politiques de contrôle des services (SCP) personnalisées à ces comptes, en plus des SCP déjà fournies par AWS Control Tower. Les personnalisations du pipeline AWS Control Tower s'intègrent aux événements et aux notifications relatifs au cycle de vie d'AWS Control Tower (Événements liés au cycle de vie dans AWS Control Tower) afin de garantir que les déploiements de ressources restent synchronisés avec votre zone de landing zone.

La documentation de déploiement de cette architecture de solution AWS Control Tower est disponible sur la page Web AWS des solutions.

Disponibilité générale de la version 2.3 d'AWS Control Tower

5 mars 2020

(Mise à jour requise pour la zone de landing zone d'AWS Control Tower. Pour plus d'informations, voirMettre à jour votre zone de destination.)

AWS Control Tower est désormais disponible dans la AWS région Asie-Pacifique (Sydney), en plus des régions USA Est (Ohio), USA Est (Virginie du Nord), USA Ouest (Oregon) et Europe (Irlande). L'ajout de la région Asie-Pacifique (Sydney) est le seul changement introduit pour la version 2.3 d'AWS Control Tower.

Si vous n'avez jamais utilisé AWS Control Tower auparavant, vous pouvez le lancer dès aujourd'hui dans l'une des régions prises en charge. Si vous utilisez déjà AWS Control Tower et que vous souhaitez étendre ses fonctionnalités de gouvernance à la région Asie-Pacifique (Sydney) dans vos comptes, rendez-vous sur la page Paramètres de votre tableau de bord AWS Control Tower. À partir de là, mettez à jour votre zone de landing zone avec la dernière version. Ensuite, mettez à jour vos comptes individuellement.

> **Note**
>
> La mise à jour de votre zone de landing zone ne met pas automatiquement à jour vos comptes. Si vous avez plusieurs comptes, les mises à jour requises peuvent prendre beaucoup de temps. C'est pourquoi nous vous recommandons d'éviter d'étendre la zone d'atterrissage de votre AWS Control Tower à des régions dans lesquelles vous n'avez pas besoin de vos charges de travail pour fonctionner.

Pour plus d'informations sur le comportement attendu des contrôles de détection à la suite d'un déploiement dans une nouvelle région, consultez Configurer vos régions AWS Control Tower.

Provisionnement de compte en une seule étape dans AWS Control Tower

2 mars 2020

(Aucune mise à jour requise pour la zone d'atterrissage d'AWS Control Tower)

AWS Control Tower prend désormais en charge le provisionnement de comptes en une seule étape via la console AWS Control Tower. Cette fonctionnalité vous permet de configurer de nouveaux comptes depuis la console AWS Control Tower.

Pour utiliser le formulaire simplifié, accédez à Account Factory dans la console AWS Control Tower, puis choisissez Quick account provisioning. AWS Control Tower attribue la même adresse e-mail au compte provisionné et à l'utilisateur d'authentification unique (IAM Identity Center) créé pour le compte. Si vous souhaitez que ces deux adresses e-mail soient différentes, vous devez approvisionner votre compte via Service Catalog.

Mettez à jour les comptes que vous créez grâce au provisionnement rapide des comptes à l'aide de Service Catalog et de l'usine de comptes AWS Control Tower, comme pour tout autre compte.

> **Note**
>
> En avril 2020, la fonctionnalité Quick Account Provisioning a été renommée Enroll account. En juin 2022, la possibilité de créer et de mettre à jour des comptes dans la console AWS Control Tower a été séparée de la possibilité d'inscrire AWS des comptes. Pour plus d'informations, consultez Inscrire un compte existant.

Outil de mise hors service d'AWS Control Tower

28 février 2020

(Aucune mise à jour requise pour la zone d'atterrissage d'AWS Control Tower)

AWS Control Tower prend désormais en charge un outil de mise hors service automatique pour vous aider à nettoyer les ressources allouées par AWS Control Tower. Si vous n'avez plus l'intention d'utiliser AWS Control Tower pour votre entreprise, ou si vous avez besoin d'un redéploiement majeur

de vos ressources organisationnelles, vous souhaiterez peut-être nettoyer les ressources créées lors de la configuration initiale de votre zone de landing zone.

Pour mettre hors service votre zone d'atterrissage à l'aide d'un processus principalement automatisé, contactez AWS Support pour obtenir de l'aide concernant les étapes supplémentaires requises. Pour plus d'informations sur la mise hors service, consultez. Procédure pas à pas : mise hors service d'une zone d'atterrissage d'une AWS Control Tower

Notifications d'événements relatifs au cycle de vie d'AWS Control Tower

22 janvier 2020

(Aucune mise à jour requise pour la zone d'atterrissage d'AWS Control Tower)

AWS Control Tower annonce la disponibilité des notifications d'événements liés au cycle de vie. Un événement du cycle de vie marque la fin d'une action AWS Control Tower susceptible de modifier l'état des ressources telles que les unités organisationnelles (UO), les comptes et les contrôles créés et gérés par AWS Control Tower. Les événements du cycle de vie sont enregistrés en tant qu' AWS CloudTrail événements et transmis à Amazon EventBridge en tant qu'événements.

AWS Control Tower enregistre les événements du cycle de vie à la fin des actions suivantes qui peuvent être effectuées à l'aide du service : création ou mise à jour d'une zone d'atterrissage ; création ou suppression d'une UO ; activation ou désactivation d'un contrôle sur une UO ; utilisation de Account Factory pour créer un nouveau compte ou pour déplacer un compte vers une autre UO.

AWS Control Tower utilise plusieurs AWS services pour créer et gérer un AWS environnement multi-comptes conforme aux meilleures pratiques. L'exécution d'une action AWS Control Tower peut prendre plusieurs minutes. Vous pouvez suivre les événements du cycle de vie dans les CloudTrail journaux pour vérifier si l'action AWS Control Tower initiale s'est bien déroulée. Vous pouvez créer une EventBridge règle pour vous avertir lorsqu' CloudTrail un événement du cycle de vie est enregistré ou pour déclencher automatiquement l'étape suivante de votre flux de travail d'automatisation.

janvier - décembre 2019

Du 1er janvier au 31 décembre 2019, AWS Control Tower a publié les mises à jour suivantes :

- Disponibilité générale de la version 2.2 d'AWS Control Tower
- Nouveaux contrôles électifs dans AWS Control Tower

- Nouveaux contrôles de détection dans AWS Control Tower
- AWS Control Tower accepte les adresses e-mail pour les comptes partagés avec des domaines différents de ceux du compte de gestion
- Disponibilité générale de la version 2.1 d'AWS Control Tower

Disponibilité générale de la version 2.2 d'AWS Control Tower

13 novembre 2019

(Mise à jour requise pour la zone de landing zone d'AWS Control Tower. Pour plus d'informations, voirMettre à jour votre zone de destination.)

La version 2.2 d'AWS Control Tower fournit trois nouveaux contrôles préventifs qui empêchent la dérive des comptes :

- Interdire les modifications apportées aux groupes de CloudWatch journaux Amazon Logs définis par AWS Control Tower
- Interdire la suppression des autorisations d' AWS Config agrégation créées par AWS Control Tower
- Interdire la suppression de l'archive de journaux

Un contrôle est une règle de haut niveau qui fournit une gouvernance continue de votre AWS environnement global. Lorsque vous créez votre zone d'atterrissage AWS Control Tower, celle-ci ainsi que toutes les unités organisationnelles (UO), les comptes et les ressources sont conformes aux règles de gouvernance appliquées par les contrôles que vous avez choisis. Lorsque vous et les membres de votre organisation utilisez la zone d'atterrissage, des modifications (accidentelles ou intentionnelles) de ce statut de conformité peuvent survenir. La détection des dérives vous aide à identifier les ressources qui nécessitent des modifications ou des mises à jour de configuration pour remédier à la dérive. Pour plus d'informations, consultez Détectez et corrigez les dérives dans AWS Control Tower.

Nouveaux contrôles électifs dans AWS Control Tower

05 septembre 2019

(Aucune mise à jour requise pour la zone d'atterrissage d'AWS Control Tower)

AWS Control Tower inclut désormais les quatre nouvelles commandes électives suivantes :

- Interdire les actions de suppression sur les compartiments Amazon S3 sans MFA
- Interdire les modifications apportées à la configuration de réplication pour les compartiments Amazon S3
- Interdire les actions en tant qu'utilisateur root
- Interdire la création de clés d'accès pour l'utilisateur root

Un contrôle est une règle de haut niveau qui fournit une gouvernance continue de votre AWS environnement global. Les barrières de sécurité vous permettent d'exprimer vos intentions de stratégie. Pour plus d'informations, consultez À propos des contrôles dans AWS Control Tower.

Nouveaux contrôles de détection dans AWS Control Tower

25 août 2019

(Aucune mise à jour requise pour la zone d'atterrissage d'AWS Control Tower)

AWS Control Tower inclut désormais les huit nouvelles commandes de détection suivantes :

- Détecter si la gestion des versions pour les compartiments Amazon S3 est activée
- Détecter si le MFA est activé pour les utilisateurs IAM de la console AWS
- Détecter si le MFA est activé pour les utilisateurs IAM
- Détecter si l'optimisation Amazon EBS est activée pour les instances Amazon EC2
- Détecter si des volumes Amazon EBS sont attachés à des instances Amazon EC2
- Détecter si l'accès public aux instances de base de données Amazon RDS est activé
- Détecter si l'accès public aux instantanés de base de données Amazon RDS est activé
- Détecter si le chiffrement du stockage est activé pour les instances de base de données Amazon RDS

Un contrôle est une règle de haut niveau qui fournit une gouvernance continue de votre AWS environnement global. Un contrôle de détection détecte la non-conformité des ressources de vos comptes, telles que les violations des politiques, et émet des alertes via le tableau de bord. Pour plus d'informations, consultez À propos des contrôles dans AWS Control Tower.

AWS Control Tower accepte les adresses e-mail pour les comptes partagés avec des domaines différents de ceux du compte de gestion

01 août 2019

(Aucune mise à jour requise pour la zone d'atterrissage d'AWS Control Tower)

Dans AWS Control Tower, vous pouvez désormais soumettre des adresses e-mail pour des comptes partagés (archive de journaux et membre d'audit) et des comptes enfants (vendus via Account Factory) dont le domaine est différent de l'adresse e-mail du compte de gestion. Cette fonctionnalité n'est disponible que lorsque vous créez une nouvelle zone de landing zone et que vous configurez de nouveaux comptes enfants.

Disponibilité générale de la version 2.1 d'AWS Control Tower

24 juin 2019

(Mise à jour requise pour la zone de landing zone d'AWS Control Tower. Pour plus d'informations, voir Mettre à jour votre zone d'atterrissage.)

AWS Control Tower est désormais généralement disponible et pris en charge pour une utilisation en production. AWS Control Tower est destiné aux organisations disposant de plusieurs comptes et aux équipes qui recherchent le moyen le plus simple de configurer leur nouvel AWS environnement multi-comptes et de gouverner à grande échelle. Avec AWS Control Tower, vous pouvez vous assurer que les comptes de votre organisation sont conformes aux politiques établies. Les utilisateurs finaux des équipes distribuées peuvent créer rapidement de nouveaux AWS comptes.

À l'aide d'AWS Control Tower, vous pouvez configurer une zone de destination qui utilise les meilleures pratiques, telles que la configuration d'une structure multi-comptes utilisant AWS Organizations, la gestion des identités des utilisateurs et des accès fédérés avec AWS IAM Identity Center, l'activation du provisionnement des comptes via Service Catalog et la création d'une archive de journaux centralisée à l'aide de et. AWS CloudTrail AWS Config

Pour une gouvernance continue, vous pouvez activer des contrôles préconfigurés, qui sont des règles clairement définies pour la sécurité, les opérations et la conformité. Les barrières de sécurité aident à empêcher le déploiement de ressources non conformes aux politiques et à surveiller en permanence les ressources déployées pour détecter toute non-conformité. Le tableau de bord AWS Control Tower fournit une visibilité centralisée sur un AWS environnement, notamment sur les comptes provisionnés, les contrôles activés et le statut de conformité des comptes.

Vous pouvez configurer un nouvel environnement multi-comptes en un seul clic dans la console AWS Control Tower. L'utilisation d'AWS Control Tower n'entraîne aucun frais supplémentaire ni engagement initial. Vous ne payez que pour les AWS services que vous avez activés pour configurer une zone d'atterrissage et mettre en œuvre les contrôles sélectionnés.

Historique du document

- Dernière mise à jour de la documentation : 20 mai 2024

Le tableau suivant décrit les modifications importantes apportées au guide de l'utilisateur d'AWS Control Tower. Pour recevoir des notifications en cas de mise à jour de cette documentation, abonnez-vous au flux RSS.

Modification	Description	Date
AWS Control Tower prend en charge jusqu'à 100 opérations de contrôle simultanées	Une augmentation du quota d'opérations de contrôle simultanées à 100.	20 mai 2024
AWS Control Tower est disponible dans la région de AWS Calgary Ouest (Canada)	AWS Control Tower est disponible dans la région du Canada Ouest (Calgary).	3 mai 2024
AWS Control Tower prend en charge les ajustements de quotas en libre-service	AWS Control Tower est intégré à AWS Service Quotas dans la console.	25 avril 2024
Documentation des commandes déplacée vers un nouveau guide	AWS Control Tower a publié le guide de référence sur les contrôles.	21 avril 2024
Marquage des `EnabledControl` ressources dans AWS CloudFormation	AWS Control Tower prend en charge l'ajout de balises aux `EnabledControl` ressources au moyen de AWS CloudFormation modèles.	22 février 2024
API de base disponibles	AWS Control Tower a publié de nouvelles API pour enregistrer les unités d'organisation par programmation.	14 février 2024

Zone de landing zone d'AWS Control Tower, version 3.3	La version 3.3 de la zone de landing zone d'AWS Control Tower est disponible.	14 décembre 2023
AWS Control Tower annonce des contrôles destinés à renforcer la souveraineté numérique	AWS Control Tower a publié un ensemble de contrôles pour aider les clients à répondre aux exigences de souverain eté numérique.	27 novembre 2023
AWS Control Tower prend en charge les API de zone d'atterrissage	AWS Control Tower prend en charge la configuration et le lancement de zones d'atterri ssage à l'aide de nouvelles API.	26 novembre 2023
AWS Control Tower prend en charge le balisage des commandes activées	AWS Control Tower prend en charge le balisage des commandes activées, dans la console et avec les nouvelles API.	10 novembre 2023
AWS Control Tower disponible en Asie-Pacifique (Melbourne) Région AWS	Disponible dans la région Asie-Pacifique (Melbourne).	3 novembre 2023
Nouvelle API de contrôle disponible	AWS Control Tower a publié une nouvelle API de contrôle.	14 octobre 2023
AWS Control Tower lance de nouvelles commandes	AWS Control Tower a publié de nouveaux contrôles proactifs et détectifs.	5 octobre 2023
AWS Control Tower signale une dérive liée à la désactiva tion de l'accès sécurisé	AWS Control Tower avertit les clients en cas de dérive, s'ils désactivent l'accès sécurisé à AWS Control Tower dans AWS Organizations.	21 septembre 2023

AWS Control Tower est disponible en quatre versions supplémentaires Régions AWS	Disponible en Asie-Pacifique (Hyderabad), en Europe (Espagne et Zurich) et au Moyen-Orient (Émirats arabes unis).	13 septembre 2023
AWS Control Tower est disponible dans la région de Tel Aviv	AWS Control Tower est disponible dans la région de Tel Aviv, il-central-1.	28 août 2023
AWS Control Tower lance 28 nouveaux contrôles proactifs	AWS Control Tower a publié 28 nouveaux contrôles proactifs.	24 juillet 2023
AWS Control Tower déconseil le 2 contrôles	AWS Control Tower supprimer a deux contrôles de la bibliothèque de contrôles à compter du 18 août 2023.	18 juillet 2023
La zone de landing zone 3.2 d'AWS Control Tower est disponible	La version 3.2 de la zone de landing zone d'AWS Control Tower est disponible.	16 juin 2023
AWS Control Tower gère les comptes en fonction de leur identifiant	AWS Control Tower suit l' AWS ID du compte plutôt que son adresse e-mail.	14 juin 2023
Contrôles de détection supplémentaires du Security Hub disponibles	AWS Control Tower ajoute dix nouveaux contrôles à la bibliothèque de contrôles, pour le Security Hub Service-Managed Standard : AWS Control Tower.	12 juin 2023

AWS Control Tower publie des tables de métadonnées de contrôle	AWS Control Tower fournit désormais des tables de métadonnées de contrôle dans le cadre de la documentation publiée.	7 juin 2023
Support de Terraform pour la personnalisation d'Account Factory	Support régional pour les plans open source Terraform dans AFC.	6 juin 2023
AWS L'autogestion IAM est disponible pour la zone d'atterrissage	AWS Control Tower aide désormais les clients à choisir leur fournisseur d'identité pour une zone de landing zone.	6 juin 2023
Nouveau rôle ajouté	AWS Control Tower a ajouté un nouveau rôle lié au service et AWSServiceRoleForA WSControlTowerla politique associée. AWSContro lTowerAccountServiceRolePol icy	1er juin 2023
Mise à jour sur la gouvernance mixte	Mise à jour pour informer les clients concernant la gouvernance mixte.	1er juin 2023
Contrôles proactifs supplémen taires disponibles	Les nouveaux contrôles proactifs vous aident à gérer votre environnement multi-comptes et à atteindre des objectifs de contrôle spécifiqu es.	19 mai 2023

Sept régions supplémentaires disponibles	AWS Control Tower est désormais disponible dans sept autres pays Régions AWS : Californie du Nord (San Francisco), Asie-Pacifique (Hong Kong, Jakarta et Osaka), Europe (Milan), Moyen-Orient (Bahreïn) et Afrique (Le Cap).	19 avril 2023
Passage à une politique gérée	Nous avons modifié le AWSControlTowerServiceRolePolicyafin qu'AWS Control Tower puisse appeler les `GetRegionOptStatus` APIEnableRegion ,`ListRegions` , mises en œuvre par le service de gestion des AWS comptes.	6 avril 2023
Suivi des demandes de personnalisation du compte généralement disponible	AWS Control Tower permet désormais de suivre les demandes de personnalisation des comptes à l'aide du flux de travail Account Factory for Terraform (AFT).	16 février 2023
Mise à jour des meilleures pratiques IAM	Guide mis à jour pour s'aligner sur les recommandations des meilleures pratiques de l'IAM. Pour plus d'informations, consultez Bonnes pratiques de sécurité dans IAM.	15 février 2023
La zone de landing zone 3.1 d'AWS Control Tower est disponible	La zone de landing zone 3.1 d'AWS Control Tower est disponible.	9 février 2023

Contrôles proactifs généralement disponibles	Les contrôles proactifs sont lancés depuis le statut de prévisualisation jusqu'à la disponibilité générale.	24 janvier 2023
Opérations de compte simultanées	AWS Control Tower prend désormais en charge jusqu'à cinq (5) actions simultanées dans Account Factory. Vous pouvez créer, mettre à jour ou inscrire jusqu'à cinq comptes à la fois.	16 décembre 2022
Les contrôles proactifs facilitent le provisionnement des ressources	AWS Control Tower prend désormais en charge les contrôles proactifs, mis en œuvre via AWS CloudFormation des hooks.	28 novembre 2022
Personnalisation du compte en usine disponible	AWS Control Tower prend désormais en charge le provisionnement de comptes grâce à des modèles de compte personnalisables, appelés plans, directement depuis la console AWS Control Tower.	28 novembre 2022
État de conformité consultable pour toutes les AWS Config règles	AWS Control Tower affiche désormais l'état de conformité de toutes les AWS Config règles déployées dans les unités organisationnelles enregistrées auprès d'AWS Control Tower.	18 novembre 2022

Passage à une politique gérée	Nous l'avons modifiée AWSControlTowerSer viceRolePolicyafin qu'AWS Control Tower puisse assumer le `AWSControlTowerBlu eprintAccess` rôle, ce qui est nécessaire pour les personnalisations d'Account Factory.	28 octobre 2022
API pour les contrôles, les AWS CloudFormation ressources	AWS Control Tower prend désormais en charge l'activat ion et la désactivation des contrôles par le biais d'un ensemble d'appels d'API et d'une nouvelle AWS CloudFormation ressource.	1er septembre 2022
CfCT prend en charge la suppression d'ensembles de piles	CfCT prend en charge la suppression d'ensembles de piles, en définissant un paramètre dans le fichier manifeste.	26 août 2022
Conservation personnalisée des journaux	Vous pouvez personnaliser la politique de conservation pour les compartiments Amazon S3 qui stockent vos CloudTrai l journaux AWS Control Tower, par tranches de jours ou d'années, jusqu'à un maximum de 15 ans.	15 août 2022

Réparation de la dérive des rôles disponible	AWS Control Tower prend en charge la réparation de la dérive des rôles, sans réparation complète de la zone d'atterrissage.	11 août 2022
Version 3.0 disponible	La version 3.0 de la zone de landing zone d'AWS Control Tower passe des pistes basées sur les comptes à des AWS CloudTrail pistes basées sur l'organisation, et met à jour la politique gérée pour permettre les pistes au niveau de l'organisation. Il vous permet d'agréger AWS Config des informations uniquement dans votre région d'origine. La version 3.0 inclut également une mise à jour du contrôle de refus de la région et deux nouvelles commandes de détection.	29 juillet 2022
La page Organisation combine les vues des unités d'organisation et des comptes	La nouvelle page d'organisation d'AWS Control Tower présente une vue hiérarchique de toutes les unités organisationnelles (UO) et de tous les comptes.	18 juillet 2022

Passage à une politique gérée	Nous avons modifié le AWSControlTowerSer viceRolePolicyafin que les clients puissent disposer de AWS CloudTrail traces au niveau de l'organisation pour agréger AWS CloudTrail les journaux.	20 juin 2022
Inscription et mise à jour simplifiées pour les comptes des membres	AWS Control Tower vous permet désormais d'inscrire et de mettre à jour les comptes de membres individuellement, depuis votre zone de landing zone. Chaque compte indique quand il est disponible pour une mise à jour. Nous avons séparé le bouton Enregistrer un compte du flux de travail de création de compte dans Account Factory.	31 mai 2022
AFT prend en charge la personnalisation des comptes partagés	AWS Control Tower Account Factory pour Terraform prend désormais en charge la personnalisation du compte de gestion, de l'archivage des journaux et des comptes d'audit AWS Control Tower.	27 mai 2022
Opérations simultanées pour tous les contrôles optionnels	AWS Control Tower vous permet désormais d'appliquer et de supprimer simultanément des mesures de protection préventives facultatives, ainsi que des contrôles de détection .	18 mai 2022

Comptes de sécurité et de journalisation existants	AWS Control Tower permet désormais d'intégrer les comptes de sécurité et de journalisation existants, plutôt que d'en créer de nouveaux lors de la configuration de la zone de landing zone.	16 mai 2022
Version 2.9 disponible	La version 2.9 d'AWS Control Tower landing zone met à jour le redirecteur de notifications Lambda pour qu'il utilise le runtime Python version 3.9.	22 avril 2022
Support mis à jour pour les AWS meilleures pratiques, version 2.8 disponible	La version 2.8 d'AWS Control Tower landing zone fournit une assistance supplémen taire pour garantir que vos charges de travail et vos AWS comptes sont conformes aux AWS meilleures pratiques.	10 février 2022
Refuser le contrôle des régions	AWS Control Tower inclut désormais un contrôle qui vous permet de restreindre l'accès aux AWS régions, afin de répondre aux préoccupa tions réglementaires et de conformité.	30 novembre 2021
Contrôles de résidence des données	AWS Control Tower prend désormais en charge des contrôles qui vous aident à gérer la résidence des données avec un contrôle granulaire.	30 novembre 2021

Fabrique de comptes AWS Control Tower pour Terraform	AWS Control Tower prend désormais en charge Terraform pour le provisionnement et la mise à jour automatisés des comptes.	29 novembre 2021
Nouvel événement du cycle de vie disponible	L'`PrecheckOrganizationalUnit` événement enregistre si des ressources bloquent le succès de la tâche de gouvernance Extend, y compris les ressources des unités d'organisation imbriquées.	18 novembre 2021
UO imbriqués disponibles	AWS Control Tower permet désormais à votre zone de landing de contenir des structures UO imbriquées.	16 novembre 2021
Detective Control Concurrence	Les contrôles de détection d'AWS Control Tower prennent désormais en charge les opérations d'activation et de désactivation simultanées.	5 novembre 2021
Deux nouvelles régions disponibles	AWS Control Tower est désormais disponible dans deux nouvelles AWS régions, la région Europe (Paris) et la région Amérique du Sud (São Paulo).	29 juillet 2021
Désélection de la région	Vous pouvez désélectionner AWS les régions que vous ne souhaitez plus gouverner via AWS Control Tower.	29 juillet 2021

Clés KMS disponibles	Vous pouvez éventuellement créer ou choisir des clés KMS que vous gérez pour chiffrer vos données et vos ressources.	28 juillet 2021
Passage à une politique gérée	Nous l'avons modifiée AWSControlTowerServiceRolePolicyafin que les clients puissent utiliser leurs propres clés de chiffrement KMS pour les AWS CloudTrail journaux.	28 juillet 2021
Les noms des contrôles ont été modifiés, les fonctionnalités restent inchangées	Certains noms et descriptions de contrôle ont été mis à jour afin de mieux refléter les intentions politiques du contrôle, sans modification des fonctionnalités.	26 juillet 2021
Analyses automatisées des SCP gérés	AWS Control Tower effectue des analyses automatisées quotidiennes des SCP gérés afin de détecter toute dérive.	11 mai 2021
Noms personnalisés pour les unités d'organisation et les comptes	AWS Control Tower vous permet de fournir des noms personnalisés pendant le processus de configuration de la zone d'atterrissage, pour les UO et les comptes essentiels, sans créer de dérive.	16 avril 2021

La mise hors service d'une zone d'atterrissage est en libre-service	AWS Control Tower vous permet désormais de mettre hors service une zone d'atterrissage sans contacter le AWS Support. La mise hors service est un processus semi-automatisé qui ne peut être annulé. Ce n'est pas la même chose que de supprimer manuellement toutes les ressources AWS Control Tower.	9 avril 2021
Trois régions supplémentaires	AWS Control Tower est désormais disponible dans trois AWS régions supplémentaires : la région Asie-Pacifique (Tokyo), la région Asie-Pacifique (Séoul) et la région Asie-Pacifique (Mumbai).	08 avril 2021

Nouvelles commandes Log Archive, version 2.7 de la zone d'atterrissage disponible	Quatre nouveaux contrôles d'archivage des journaux assurent la gouvernance de l'archivage des journaux sur les ressources d'AWS Control Tower, indépendamment de la gouvernance des ressource s extérieures à AWS Control Tower. Les directives relatives à quatre contrôles existants sont passées de obligatoires à facultatives. La version 2.7 de la zone de landing zone AWS Control Tower inclut une exigence de protocole HTTPS, qui ne peut pas être annulée après la mise à jour.	08 avril 2021
Sélection de la région	La sélection de la région AWS Control Tower permet de mieux gérer l'emprein te géographique de vos ressources AWS Control Tower. Pour augmenter le nombre de régions dans lesquelles vous hébergez AWS des ressources ou des charges de travail (pour des raisons de conformité, de réglementation, de coût ou autres), vous pouvez désormais sélectionner les régions supplémentaires à gouverner.	19 février 2021

Enregistrez une unité d'organisation et gérez tous ses comptes avec AWS Control Tower en une seule fois	AWS Control Tower ajoute la possibilité d'enregistrer une unité d'organisation, ce qui permet d'intégrer plusieurs comptes à la gouvernance en même temps.	28 janvier 2021
Mises à jour multiples de comptes dans les unités d'organisation enregistrées	Vous pouvez désormais mettre à jour tous les comptes de n'importe quelle unité AWS Organizations organisationnelle (UO) enregistrée contenant jusqu'à 300 comptes, en un seul clic, depuis le tableau de bord AWS Control Tower. La fonctionnalité de mise à jour de comptes multiples, également appelée mise à jour groupée, élimine le besoin de mettre à jour un compte à la fois ou d'utiliser un script externe pour effectuer la mise à jour sur plusieurs comptes simultanément.	28 janvier 2021
Nouveau rôle pour l'agrégation des unités d'organisation et des comptes non gérés	Un nouveau rôle aide à détecter AWS Config les règles externes, de sorte qu'AWS Control Tower n'a pas besoin d'accéder à des comptes non gérés.	29 décembre 2020

AWS Control Tower est disponible dans un plus grand nombre de AWS régions.	AWS Control Tower est désormais disponible pour être déployée dans la région Asie-Pacifique (Singapour), la région Europe (Francfort), la région Europe (Londres), la région Europe (Stockholm) et la région Canada (centre). Avec ce lancement, AWS Control Tower est désormais disponible dans 10 AWS régions. Cette mise à jour de la zone d'atterrissage inclut toutes les régions répertoriées, et elle ne peut pas être annulée. Après avoir mis à jour votre zone de landing zone vers la version 2.5, vous devez mettre à jour manuellement tous les comptes inscrits pour qu'AWS Control Tower règne dans les 10 AWS régions prises en charge.	18 novembre 2020
Mise à jour du contrôle	Une version mise à jour a été publiée pour le contrôle obligatoire`AWS-GR_IAM_ROLE_CHANGE_PROHIBITED` . Le contrôle mis à jour permet de faciliter l'inscription automatique des comptes.	8 octobre 2020

La page d'informations associées est désormais disponible pour AWS Control Tower	La page d'informations associée permet de trouver plus facilement les tâches courantes qui peuvent être utiles après avoir configuré votre zone de landing zone AWS Control Tower.	18 septembre 2020
La console AWS Control Tower fournit plus de détails sur les unités d'organisation et les comptes.	Dans la console AWS Control Tower, vous pouvez consulter plus de détails sur vos AWS comptes et unités organisat ionnelles (UO). La page « Comptes » répertorie désormais tous les comptes de votre organisation, quel que soit l'unité d'organisation ou le statut d'inscription dans AWS Control Tower. Vous pouvez désormais rechercher, trier et filtrer dans toutes les tables.	22 juillet 2020
AWS Control Tower permet aux organisations existante s de configurer une zone de landing zone	Vous pouvez désormais lancer une zone de landing zone pour AWS Control Tower dans une organisation existante, afin de l'intégrer à la gouvernance. La fonctionnalité Quick Account Provisioning d'AWS Control Tower a été renommée « Enroll account » et permet désormais l'inscription de AWS comptes existants ainsi que la création de nouveaux comptes.	16 avril 2020

AWS Control Tower est désormais disponible en Asie-Pacifique	AWS Control Tower est désormais disponible pour être déployée dans la AWS région Asie-Pacifique (Sydney). Cette version nécessite des mises à jour manuelles des comptes vendus, uniquement si vous prévoyez d'exécuter des charges de travail en Asie-Pacifique (Sydney).	3 mars 2020
La mise hors service d'une zone d'atterrissage d'AWS Control Tower est possible	AWS Support peut vous aider à mettre définitivement hors service une zone d'atterrissage grâce à un processus essentiellement automatisé qui préserve vos organisations, bien qu'un nettoyage manuel soit nécessaire.	27 février 2020
Le provisionnement rapide des comptes est disponible dans AWS Control Tower	Le provisionnement rapide de compte facilite le lancement de nouveaux comptes membres lorsque la zone de destination est à jour, avec la fonction Inscrire un compte.	20 février 2020
Les événements du cycle de vie sont suivis dans AWS Control Tower	Les événements du cycle de vie fournissent des informations supplémentaires sur certains événements de l'AWS Control Tower, afin de faciliter l'automatisation des flux de travail.	12 décembre 2019

Les pages de paramètres et d'activités sont disponibles pour AWS Control Tower	Les pages Paramètres et Activités facilitent la mise à jour de votre zone de destination et l'affichage des événements consignés.	30 novembre 2019
Des contrôles préventifs supplémentaires sont disponibles pour AWS Control Tower	Les contrôles préventifs d'AWS Control Tower permettent à votre organisation et à vos ressources de rester alignées sur votre environnement.	6 septembre 2019
Des contrôles de détection supplémentaires sont disponibles pour AWS Control Tower	Les contrôles Detective d'AWS Control Tower fournissent des informations sur l'état de votre organisation et de ses ressources.	27 août 2019
AWS Control Tower est désormais disponible pour tous	AWS Control Tower est un service qui offre le moyen le plus simple de configurer et de gérer votre AWS environnement multi-comptes à grande échelle.	24 juin 2019

AWS Glossaire

Pour la AWS terminologie la plus récente, consultez le AWS glossaire dans la Glossaire AWS référence.

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.