



Guide de l'utilisateur

AWS Control Tower



AWS Control Tower: Guide de l'utilisateur

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques et la présentation commerciale d'Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n'est pas d'Amazon, d'une manière susceptible de créer une confusion parmi les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Qu'est-ce qu'AWS Control Tower ?	1
Fonctionnalités	1
Comment AWS Control Tower interagit avec les autres services AWS	2
Utilisez-vous AWS Control Tower pour la première fois ?	3
Comment ça marche	4
Structure d'une zone d'atterrissage d'une tour de contrôle AWS	4
Que se passe-t-il lorsque vous configurez une zone d'atterrissage	4
Quels sont les comptes partagés ?	5
Comment fonctionnent les commandes	6
Comment fonctionne AWS Control Tower avec StackSets	7
Terminologie	9
Tarifification	13
.....	13
Configuration	14
Inscrivez-vous pour AWS	14
Inscrivez-vous pour un Compte AWS	14
Création d'un utilisateur doté d'un accès administratif	15
.....	16
Étape suivante	16
Premiers pas	17
Guide de démarrage rapide	17
Contrôles avant le lancement	19
Considérations pour les AWS IAM Identity Center clients (IAM Identity Center)	20
Démarez depuis la console	21
Attentes relatives à la configuration de la zone d'atterrissage	22
Étape 1 : Créez les adresses e-mail de votre compte partagé	23
Étape 2. Configurez et lancez votre zone d'atterrissage	25
Étape 3. Vérifiez et configurez la zone d'atterrissage	33
Faites vos premiers pas avec APIs.	34
Attentes relatives à la configuration de la zone d'atterrissage avec APIs	35
Étape 1 : Configurez votre zone de landing zone	36
Étape 2 : Lancez votre zone de landing zone	39
Identifiez votre zone de landing	43
Mettez à jour votre zone de landing zone	44

Réinitialisez la zone d'atterrissage pour résoudre le problème de dérive	45
Démantelez votre zone d'atterrissage	46
Consultez l'état des opérations de votre zone d'atterrissage	47
Exemples : configurer une zone de landing zone AWS Control Tower avec des API uniquement	50
Lancez une zone d'atterrissage en utilisant AWS CloudFormation	57
Étapes suivantes	63
Limitations et quotas	65
Limitations connues de AWS Control Tower	65
Demander une augmentation de quota	67
Limites de contrôle	68
Trouvez les commandes et les régions disponibles	70
Limitations basées sur les AWS services sous-jacents	73
Différences régionales	75
Nouveau : Guide de référence d'AWS Control Tower Controls	76
Bonnes pratiques pour les administrateurs	77
Expliquer l'accès aux utilisateurs	77
Expliquer l'accès aux ressources	77
Expliquer les contrôles préventifs	78
Planifiez votre zone de landing	79
Comparez les fonctionnalités	80
Lancer AWS Control Tower dans une organisation existante	81
Lancez AWS Control Tower dans une nouvelle organisation	83
Bonnes pratiques : configurer une zone d'atterrissage AWS multi-comptes	83
Suivez les directives relatives AWS à plusieurs comptes	84
Directives pour la mise en place d'un environnement bien conçu	85
Exemple de AWS Control Tower avec une structure d'unité d'organisation multi-comptes complète	88
À propos de The Root	89
Conseils administratifs pour la configuration de la zone d'atterrissage	89
Recommandations pour la configuration de groupes, de rôles et de politiques	91
Conseils sur les ressources AWS de Control Tower	92
Quand se connecter en tant qu'utilisateur root	94
AWS Organizations orientation	95
IAMConseils relatifs au centre d'identité	97
Conseils d'Account Factory	99

Conseils pour s'abonner à Topics SNS	99
Conseils pour les KMS clés	100
Mises à jour de la zone	101
Politiques relatives aux services basés sur l'IA	103
Gestion des mises à jour de configuration	105
À propos des mises à	107
Mettez à jour votre zone de landing zone	108
Procédure de mise à jour standard	108
Sélectionnez une version de zone d'atterrissage	109
Mises à jour du compte, versions de la zone d'atterrissage et données de référence	110
Schémas des zones d'atterrissage	111
Résolvez la dérive avec Reset and Re-register	121
Fournir et mettre à jour des comptes à l'aide de l'automatisation	122
Automatisez les tâches	124
AWS CloudShell et le AWS CLI	126
Obtenir IAM des autorisations pour AWS CloudShell	127
Interagissez avec AWS Control Tower via AWS CloudShell	128
AWS CloudFormation ressources	131
AWS Control Tower et AWS CloudFormation modèles	131
En savoir plus sur AWS CloudFormation	132
Personnalisez votre zone de landing	133
.....	133
Personnalisation depuis la console AWS Control Tower	133
Automatisez les personnalisations en dehors de la console AWS Control Tower	135
Avantages des personnalisations pour AWS Control Tower (CfCT)	135
Exemples supplémentaires de CfCT	136
Présentation des personnalisations pour AWS Control Tower (CfCT)	137
Architecture	137
Coût	140
Services relatifs aux composants	140
AWS CodeCommit	140
AWS CodePipeline	141
AWS Key Management Service	141
AWS Lambda	142
Amazon Simple Notification Service	142
Amazon Simple Storage Service	142

Amazon Simple Queue Service	143
AWS Step Functions	143
AWS Systems Manager Parameter Store	143
Considérations relatives au déploiement	143
Préparation au déploiement	143
Pour mettre à jour les personnalisations pour AWS Control Tower	145
Modèle et code source	145
Code source	146
Déployez CfCT	146
Prérequis	146
Étapes de déploiement	146
Étape 1. Lancement de la pile	147
Étape 2. Création d'un package personnalisé	151
Mettre à jour la pile	152
Suppression d'un ensemble de piles	153
Configurer Amazon S3 comme source de configuration	154
Métriques opérationnelles	155
Guide de personnalisation du CfCT	156
Vue d'ensemble du pipeline de code	157
Définition d'une configuration personnalisée	159
Root OU	166
UO imbriquée	168
Créez vos propres personnalisations	169
Mises à niveau de la version	177
Réseaux	180
VPC et AWS régions dans AWS Control Tower	180
Présentation d'AWS Control Tower et des VPC	181
.....	181
CIDR et peering pour VPC et AWS Control Tower	182
Rôles et autorisations	185
Rôles et comptes	186
Rôles et création de comptes	186
AWSControlTowerExecutionrôle	187
Conditions facultatives pour vos relations de confiance	188
Comment AWS Control Tower agrège AWS Config règles relatives aux comptes non gérés OUs	191

Rôles programmatiques et relations de confiance pour le compte d'audit AWS de la Control Tower	193
Approvisionnement automatique des comptes avec des rôles IAM	197
Gérez les ressources	199
Configuration des régions	200
Configurez les régions AWS de votre Control Tower	201
Évitez la gouvernance mixte lors de la configuration des régions	203
À propos des régions optionnelles	205
Configurer le contrôle de refus des régions	208
Considérations relatives au refus de contrôle des régions au niveau de l'UO	209
Comptes	211
Méthodes d'approvisionnement	211
Que se passe-t-il lorsque AWS Control Tower crée un compte ?	213
Autorisations nécessaires	213
.....	214
À propos des comptes	214
Considérations relatives à l'ajout de comptes de sécurité ou de journalisation existants	215
Consultez vos comptes	215
Ressources du compte partagé	216
À propos des comptes partagés	227
À propos des comptes des membres	230
Inscrire un existant Compte AWS	230
Que se passe-t-il lors de l'inscription au compte	231
Inscription de comptes existants auprès de VPCs	232
Conditions préalables à l'inscription	233
Créez un compte	234
Si le compte ne répond pas aux prérequis	238
Exemples de AWS Config CLI commandes pour l'état des ressources	240
Ajoutez manuellement le IAM rôle requis à un rôle existant Compte AWS et inscrivez-le	240
Inscription automatique des AWS Organizations comptes	243
Inscrire des comptes disposant de ressources existantes AWS Config	244
Étape 1 : contactez le support client avec un ticket, pour ajouter le compte à la liste d'autorisation d'AWS Control Tower	246
Étape 2 : créer un nouveau rôle IAM dans le compte membre	247
Étape 3 : Identifier les AWS régions disposant de ressources préexistantes	248
Étape 4 : Identifier les AWS régions dépourvues de AWS Config ressources	248

Étape 5 : Modifier les ressources existantes dans chaque AWS région	248
Étape 5a. AWS Config ressources pour les enregistreurs	248
Étape 5b. Modifier les ressources du canal de AWS Config distribution	249
Étape 5c. Modifier les ressources AWS Config d'autorisation d'agrégation	250
Étape 6 : créer des ressources là où elles n'existent pas, dans les régions régies par AWS Control Tower	250
Étape 7 : enregistrer l'unité d'organisation auprès d'AWS Control Tower	252
Account Factory	252
Autorisations	252
Création et provisionnement d'un compte	253
Considérations relatives au compte	254
Mettre à jour et déplacer des comptes	255
Modifier l'adresse e-mail d'un compte inscrit	257
Modifier le nom d'un compte inscrit	258
Configurer les VPC paramètres Amazon	259
Désinscrire un compte	260
Fermer un compte	262
Ressources d'Account Factory	264
Personnalisation de Account Factory (AFC)	265
Configuration pour la personnalisation	268
Créez un compte personnalisé à partir d'un plan	274
Inscrivez et personnalisez des comptes	275
Ajouter un plan à un compte AWS Control Tower	276
Mettre à jour un plan	276
Supprimer un plan d'un compte	277
Les plans des partenaires	278
Considérations relatives aux personnalisations d'Account Factory (AFC)	278
En cas d'erreur de plan	279
Personnalisation de votre document de politique pour les plans de l'AFC sur la base de CloudFormation	280
Autorisations supplémentaires requises pour créer un produit Service Catalog basé sur Terraform	282
AWS Control Tower Account Factory pour Terraform (AFT)	283
Prérequis	283
Création d'un nouveau compte	284
Demandes de comptes multiples	286

Mettre à jour un compte existant	286
Déployer AFT	287
AFTvue d'ensemble	292
Versions prises en charge	295
Activer les options de fonctionnalités	299
Ressources pour l'AFT	302
Rôles obligatoires	306
Services relatifs aux composants	310
Pipeline de provisionnement de comptes AFT	312
Personnaliser le compte	315
Alternative VCS	322
Protection des données	324
Supprimer un compte	325
Métriques opérationnelles	327
Guide de dépannage	328
Dérive	333
Détection de la dérive	333
Résolution de la dérive	335
Considérations relatives à la dérive et aux SCP scans	335
Types de dérive à résoudre immédiatement	337
Modifications réparables apportées aux ressources	337
Dérive et provisionnement de compte	338
Types de dérive de gouvernance	338
Déplacement du compte membre	339
Suppression de compte membre	341
Mise à jour imprévue vers Managed SCP	342
SCP Rattaché à l'unité d'organisation gérée	343
SCP Détaché de l'unité d'exploitation gérée	344
SCP Attaché au compte du membre	345
UO de base supprimée	346
Security Hub contrôle la dérive	347
Accès sécurisé désactivé	348
Si vous gérez des ressources en dehors d'AWS Control Tower	349
Référence à des ressources extérieures à AWS Control Tower	350
Modification externe des noms des ressources AWS Control Tower	351
Suppression de l'unité d'organisation de sécurité	352

Supprimer un compte de l'unité d'organisation de sécurité	352
Modifications externes mises à jour automatiquement	355
Organizations	358
Vidéo de démonstration	359
.....	359
Étendre la gouvernance à une organisation existante	359
Vidéo : Activer une zone d'atterrissage dans une zone existante AWS Organizations	361
Considérations relatives à IAM Identity Center et aux organisations existantes	361
Accès à d'autres AWS services	361
UO imbriquées	361
Vidéo de procédure	362
Passez d'une structure d'unité d'organisation plate à une structure d'unité d'organisation imbriquée	362
Contrôles préalables à l'enregistrement des unités d'exploitation imbriquées	363
UO et rôles imbriqués	363
Que se passe-t-il lors de l'enregistrement et du réenregistrement des unités d'organisation et des comptes imbriqués	364
Considérations relatives à l'enregistrement des unités d'organisation imbriquées	364
Limites de l'UO imbriquée	364
UO imbriquées et conformité	365
UO imbriquées et dérive	366
UO et contrôles imbriqués	366
Les unités d'organisation imbriquées et la racine	368
Enregistrez une UO pour inscrire plusieurs comptes	368
Enregistrer une UO existante	370
Création d'une nouvelle UO	371
Causes courantes d'échec lors de l'enregistrement ou du réenregistrement	372
Mettre à jour les organisations	375
Quand effectuer la mise à jour OUs et comptes	375
Mettre à jour plusieurs comptes dans une unité d'organisation	376
Que se passe-t-il lors de la réinscription	376
Mettre à jour un seul compte	377
Services intégrés	378
AWS CloudFormation	378
CloudTrail	379
CloudWatch	379

AWS Config	379
AWS Identity and Access Management	380
AWS Key Management Service	380
AWS Lambda	381
AWS Organizations	381
Considérations	382
Amazon S3	382
Security Hub	382
AWS Service Catalog	383
Transition vers un type de produit externe	383
Amazon SNS	385
Step Functions	385
Gestion des identités et des accès	386
Authentification	386
Contrôle d'accès	389
Centre d'identité IAM et AWS Control Tower	389
.....	389
Groupes d'utilisateurs, rôles et ensembles d'autorisations	390
Ce qu'il faut savoir sur les comptes IAM Identity Center et AWS Control Tower	391
Groupes de centres d'identité IAM pour AWS Control Tower	392
Vue d'ensemble de la gestion de l'accès aux ressources avec IAM	396
AWSRessources et opérations de la Control Tower	397
À propos de la propriété des ressources	397
Gérez l'accès aux ressources	398
Spécifiez les éléments de politique : actions, effets et principes	408
Spécification de conditions dans une politique	409
Prévenez les attaques confuses des adjoints	409
Politiques IAM pour AWS Control Tower	410
Autorisations requises pour utiliser la console AWS Control Tower	410
AWS ControlTowerAdmin rôle	411
AWS ControlTowerServiceRolePolicy	412
AWS ControlTowerStackSetRole	417
AWS ControlTowerCloudTrailRole	418
AWSControlTowerBlueprintAccess exigences relatives aux rôles	419
AWSServiceRoleForAWSControlTower	420
AWSControlTowerAccountServiceRolePolicy	421

Politiques gérées pour AWS Control Tower	423
Sécurité	428
Protection des données	428
Chiffrement au repos	430
Chiffrement en transit	430
Restreindre l'accès au contenu	430
Validation de la conformité	431
Résilience	432
Sécurité de l'infrastructure	432
Journalisation et surveillance	434
À propos de la connexion à AWS Control Tower	435
Politique de compartiment S3	436
Vue d'ensemble du monitoring	438
Journalisation des actions d'AWS Control Tower avec AWS CloudTrail	439
Informations sur AWS Control Tower dans CloudTrail	439
Exemple : entrées dans le fichier journal d'AWS Control Tower	442
Surveillez l'évolution des ressources avec AWS Config	443
Gérer les coûts de configuration	444
Afficher les données de l' AWS Config enregistreur sur les comptes inscrits	446
Résolution des problèmes AWS Config dans AWS Control Tower	446
Evènements du cycle de vie	448
CreateManagedAccount	451
UpdateManagedAccount	453
EnableGuardrail	454
DisableGuardrail	455
SetupLandingZone	457
UpdateLandingZone	458
RegisterOrganizationalUnit	460
DeregisterOrganizationalUnit	462
PrecheckOrganizationalUnit	463
Notifications utilisateur	465
Procédures	468
Procédure pas à pas : passer d'ALZ à AWS Control Tower	468
Procédure pas à pas : Automatisez le provisionnement des comptes dans AWS Control Tower par les API Service Catalog	469
Exemple d'entrée de provisionnement pour l'API Service Catalog	471

Vidéo de procédure	472
Procédure pas à pas : configurer AWS Control Tower sans VPC	473
Supprimer le VPC AWS Control Tower	473
Créer un compte dans AWS Control Tower sans VPC	474
Procédure pas à pas : configurer des groupes de sécurité dans AWS Control Tower avec AWS Firewall Manager	475
Configuration de groupes de sécurité avec AWS Firewall Manager	476
Procédure pas à pas : mise hors service d'une zone d'atterrissage d'une AWS Control Tower .	476
Vue d'ensemble du processus de mise hors service	477
Ressources non supprimées lors de la mise hors service	479
Comment mettre hors service une zone d'atterrissage	489
.....	490
Configuration après la mise hors service d'une zone d'atterrissage	491
Résolution des problèmes	494
Échec de lancement de la zone de destination	494
Erreur indiquant que la zone d'atterrissage n'est pas à jour	495
Échec du provisionnement du nouveau compte	495
Échec de l'inscription d'un compte existant	496
Impossible de mettre à jour un compte Account Factory	497
Impossible de mettre à jour la zone d'atterrissage	498
Erreur de défaillance mentionnant AWS Config	500
Erreur Aucun chemin de lancement trouvé	502
Réception d'une erreur Autorisations insuffisantes	502
Les contrôles Detective n'ont aucun effet sur les comptes	503
Erreur de dépassement du taux renvoyée par l' AWS Organizations API	503
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	504
AWS Support	506
Références	507
Inscription partielle de comptes	509
Variation des opérations entre la console AWS Control Tower et les API pour les lignes de base	510
Valeurs de référence et paramètres de version par défaut	510
AWSControlTowerBaseline table	511
Exemples : enregistrer une unité d'organisation AWS Control Tower avec des API uniquement	516

API Exemples de référence	518
DisableBaseline	518
EnableBaseline	518
GetBaseline	520
GetBaselineOperation	521
GetEnabledBaseline	522
ListBaselines	523
ListEnabledBaselines	524
ResetEnabledBaseline	526
UpdateEnabledBaseline	527
Informations supplémentaires	529
Tutoriels et ateliers	529
Réseaux	180
Sécurité, identité et journalisation	530
Déploiement des ressources et gestion des charges de travail	531
Travailler avec des organisations et des comptes existants	531
Automatisation et intégration	531
Migration des charges de travail	532
Services AWS connexes	532
AWS Marketplace solutions	533
Notes de mise à jour	534
Janvier 2024 - En cours	534
AWSControl Tower prend en charge jusqu'à 1 000 comptes par unité d'organisation	535
AWSControl Tower ajoute une sélection de versions pour les zones d'atterrissage	535
Contrôle descriptif API disponible, accès étendu aux régions et aux contrôles	536
AWSControl Tower soutient AFT et CfCT dans les régions optionnelles	537
AWSControl Tower ajoute le ListLandingZoneOperations API	537
AWSControl Tower prend en charge jusqu'à 100 opérations de contrôle simultanées	538
AWSControl Tower disponible en AWS Canada Ouest (Calgary)	538
AWSControl Tower prend en charge les ajustements de quotas en libre-service	540
AWSControl Tower publie le guide de référence sur les contrôles	540
AWSControl Tower met à jour et renomme deux contrôles proactifs	540
Les contrôles obsolètes ne sont plus disponibles	541
AWSControl Tower prend en charge le balisage des EnabledControl ressources dans AWS CloudFormation	542

AWSControl Tower prend en charge APIs l'enregistrement et la configuration des unités d'organisation avec des lignes de base	542
janvier - décembre 2023	544
Transition vers le nouveau AWS Service Catalog Type de produit externe (phase 3)	545
AWSZone d'atterrissage de la Control Tower, version 3.3	545
Transition vers le nouveau AWS Service Catalog Type de produit externe (phase 2)	546
AWSControl Tower annonce des contrôles pour favoriser la souveraineté numérique	547
AWSControl Tower soutient la zone d'atterrissage APIs	552
AWSControl Tower prend en charge le balisage pour les commandes activées	553
AWSControl Tower disponible dans la région Asie-Pacifique (Melbourne)	554
Transition vers le nouveau AWS Service Catalog Type de produit externe (phase 1)	555
Nouveau contrôle API disponible	555
AWSControl Tower ajoute des commandes supplémentaires	556
Nouveau type de dérive signalé : accès sécurisé désactivé	559
Quatre supplémentaires Régions AWS	559
AWSControl Tower disponible dans la région de Tel Aviv	560
AWSControl Tower lance 28 nouveaux contrôles proactifs	560
AWSControl Tower déconseille deux commandes	562
AWSZone d'atterrissage de la Control Tower, version 3.2	563
AWSControl Tower gère les comptes en fonction de leur identifiant	565
Contrôles de détection supplémentaires du Security Hub disponibles dans la bibliothèque de contrôles AWS Control Tower	565
AWSControl Tower publie des tables de métadonnées de contrôle	566
Support de Terraform pour la personnalisation d'Account Factory	566
AWS IAML'autogestion du centre d'identité est disponible pour la zone de landing zone	567
AWSControl Tower résout le problème de la gouvernance mixte pour OUs	568
Contrôles proactifs supplémentaires disponibles	568
Contrôles EC2 proactifs Amazon mis à jour	571
Sept supplémentaires Régions AWS available	571
Account Factory for Terraform (AFT) : suivi des demandes de personnalisation du compte	572
AWSZone d'atterrissage de la Control Tower, version 3.1	573
Contrôles proactifs généralement disponibles	574
janvier - décembre 2022	575
Opérations de compte simultanées	575
Personnalisation de Account Factory (AFC)	576

Des commandes complètes aident à AWS approvisionnement et gestion des ressources ...	576
État de conformité consultable par tous AWS Config rules	577
API pour les commandes et un nouveau AWS CloudFormation ressource	578
CfCT prend en charge la suppression d'ensembles de piles	579
Conservation personnalisée des journaux	579
Réparation de la dérive des rôles disponible	579
AWSZone d'atterrissage de la Control Tower, version 3.0	580
La page Organisation combine les vues OUs et les comptes	584
Inscription et mise à jour simplifiées pour les comptes de membres individuels	584
AFT prend en charge la personnalisation automatique des comptes AWS Control Tower partagés	585
Opérations simultanées pour tous les contrôles optionnels	586
Comptes de sécurité et de journalisation existants	587
AWSZone d'atterrissage de la Control Tower, version 2.9	587
AWSZone d'atterrissage de la Control Tower, version 2.8	588
janvier - décembre 2021	589
Fonctionnalités de refus régional	589
Fonctionnalités de résidence des données	590
AWSControl Tower présente le provisionnement et la personnalisation des comptes Terraform	590
Nouvel événement du cycle de vie disponible	591
AWSControl Tower permet d'imbriquer OUs	591
Detective Control Concurrence	592
Deux nouvelles régions disponibles	593
Désélection de la région	594
AWSControl Tower fonctionne avec AWS Systèmes de gestion des clés	594
Contrôles renommés, fonctionnalités inchangées	595
AWSControl Tower scanne SCPs tous les jours pour détecter toute dérive	595
Noms OUs et comptes personnalisés	596
AWSZone d'atterrissage de la Control Tower, version 2.7	597
Trois nouveaux AWS Régions disponibles	598
Gouverner uniquement les régions sélectionnées	599
AWSControl Tower étend désormais la gouvernance à l'existant OUs dans votre AWS organisations	599
AWSControl Tower fournit des mises à jour groupées des comptes	600
janvier - décembre 2020	601

AWSLa console Control Tower est désormais reliée à une interface externe AWS Règles de configuration	601
AWSControl Tower est désormais disponible dans d'autres régions	602
Mise à jour du garde-corps	602
AWSLa console Control Tower affiche plus de détails sur OUs les comptes	603
Utilisez AWS Control Tower pour configurer de nouveaux comptes multiples AWS environnements dans AWS Organizations	603
Personnalisations de la AWS solution Control Tower	604
Disponibilité générale de la version 2.3 de AWS Control Tower	605
Provisionnement de compte en une seule étape dans Control Tower AWS	605
AWSOutil de mise hors service de Control Tower	606
AWSNotifications d'événements liés au cycle de vie de la Control Tower	606
janvier - décembre 2019	607
Disponibilité générale de la version 2.2 de AWS Control Tower	607
Nouvelles commandes électives dans AWS Control Tower	608
Nouvelles commandes de détective dans AWS Control Tower	609
AWSControl Tower accepte les adresses e-mail pour les comptes partagés avec des domaines différents de ceux du compte de gestion	609
Disponibilité générale de la version 2.1 de AWS Control Tower	610
Historique de la documentation	611
AWS Glossaire	631
.....	dcxxxii

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 Organizations. Pour 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, consultez [AWS 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, consultez [Comment 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 plus d'informations, consultez [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 plus d'informations, consultez [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. AWS Pour 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 Catalog The

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 Organizations ou 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 d'atterrissage de votre AWS Control Tower](#) et [AWS stratégie multi-comptes pour votre zone de landing AWS zone de 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 [Déterminez 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, consultez [Gestion 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 la création et la modification des ressources AWS de la 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'action CloudTrail. 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

- [Déterminez 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 AWS de Control Tower.

Tout d'abord, il est bon de savoir que 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 OUs, 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 Organizations](#) est 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 Control Tower s'appuie sur la création AWS Organizations de comptes, l'application de contrôles préventifs au niveau de l'unité d'organisation et la fourniture d'une facturation centralisée.
- Un [AWS compte Account Factory](#) est un AWS compte approvisionné 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 de AWS Control Tower a été déployée. Vous pouvez voir votre région d'origine dans les paramètres de votre zone d'atterrissage.
- [AWS Service Catalog](#) vous 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 StackSets](#) sont 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 (OU). Par exemple, la ligne de base appelée `AWSControlTowerBaseline` est disponible pour vous aider à vous inscrire OUs auprès AWS de 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.
- Drift : 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 que AWS Control Tower crée automatiquement lorsque vous configurez votre zone d'atterrissage : 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 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 SCPs 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 IAM utilisateur](#)) 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 de l'ensemble de votre environnement AWS Control Tower. Chaque contrôle applique une seule règle. Des contrôles préventifs sont mis en œuvre avec SCPs. Les contrôles Detective sont mis en œuvre avec AWS Config des règles. Les contrôles proactifs sont mis en œuvre avec AWS CloudFormation des crochets. Pour de plus amples informations, veuillez consulter [Comment fonctionnent les commandes](#).
- **Zone d'atterrissage** : une zone d'atterrissage est un environnement cloud qui propose un point de départ recommandé, notamment des comptes par défaut, une structure de compte, des 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.
- **UO imbriquée** : Une UO imbriquée dans AWS Control Tower est une UO contenue dans une autre UO. Une UO imbriquée peut avoir exactement une UO parent, et chaque compte peut être membre d'une UO précise. Imbriqué OUs crée une hiérarchie. Lorsque vous associez une politique à l'un des comptes de la hiérarchie, elle se répercute sur tous les comptes OUs et situés en dessous. OUs 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 UO peut avoir exactement une UO parent.
- **UO enfant** : toute UO située en dessous de l'UO actuelle dans la hiérarchie. Une UO peut avoir plusieurs enfants OUs.
- **Hiérarchie de l'UO** : dans AWS Control Tower, la hiérarchie des unités imbriquées OUs peut comporter jusqu'à cinq niveaux. L'ordre de nidification est appelé niveaux. Le sommet de la hiérarchie est désigné comme niveau 1.
- **UO de haut niveau** : Une UO de haut niveau est une UO située directement sous la racine, et non la racine elle-même. La racine n'est pas considérée comme une unité d'organisation.

- **Gouvernée** : une région gouvernée est gérée et contrôlée dans votre environnement par AWS Control Tower, conformément aux politiques de gouvernance définies par votre organisation. Les Régions AWS sont surveillées afin de respecter les meilleures pratiques et les politiques organisationnelles. Vos ressources dans ces régions sont protégées lorsque vous activez les commandes AWS de la Control Tower.
- **Non gouvernée** : les régions affichant le statut Non gouvernée ne sont ni contrôlées ni surveillées par AWS Control Tower. Ils ne respectent Régions AWS généralement pas les mêmes politiques de gouvernance que celles appliquées par AWS Control Tower. Vous pouvez créer des ressources dans ces régions, mais ces ressources ne sont pas protégées par les contrôles AWS de la Control Tower.
- **Refusé** : une région refusée est bloquée spécifiquement par AWS Control Tower. Dans votre environnement AWS Control Tower, vous ne pouvez pas y allouer de ressources Régions AWS.

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 Config. Pour de plus amples informations, veuillez consulter [Tarification AWS 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, consultez [Surveillez 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 d'utiliser AWS Control Tower pour la première fois, suivez les étapes décrites dans cette section pour créer un AWS compte et protégez votre AWS Control Tower compte de gestion. Pour plus d'informations sur les tâches de configuration supplémentaires spécifiques pour AWS Control Tower, voir [Commencer à utiliser AWS Control Tower](#).

Inscrivez-vous pour AWS

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

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

Inscrivez-vous pour un Compte AWS

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

Pour vous inscrire à un Compte AWS

1. Ouvrez l'<https://portal.aws.amazon.com/billing/inscription>.
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 AWS est créé. L'utilisateur root a accès à tous Services AWS et les ressources du compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les [tâches nécessitant un accès utilisateur racine](#).

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. À tout moment, vous pouvez consulter l'activité actuelle de votre compte et gérer votre compte 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 Compte AWS, sécurisez votre Utilisateur racine d'un compte AWS, activer AWS IAM Identity Center, et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous au [AWS Management Console](#) en tant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre Compte AWS adresse e-mail. Sur la page suivante, saisissez votre mot de passe.

Pour obtenir de l'aide pour vous connecter à l'aide de l'utilisateur root, consultez [la section Connexion en tant qu'utilisateur root](#) dans Connexion à AWS Guide de l'utilisateur

2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur root.

Pour obtenir des instructions, voir [Activer un MFA appareil virtuel pour votre Compte AWS utilisateur root \(console\)](#) dans le guide de IAM l'utilisateur.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

Pour obtenir des instructions, voir [Activation AWS IAM Identity Center](#) dans le .AWS IAM Identity Center Guide de l'utilisateur

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 avec la valeur par défaut Répertoire IAM Identity Center](#) dans le .AWS IAM Identity Center Guide de l'utilisateur

Connexion en tant qu'utilisateur doté d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL identifiant envoyé à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

Pour obtenir de l'aide pour vous connecter à l'aide d'un utilisateur d'IAM Identity Center, consultez la section [Connexion au AWS portail d'accès](#) dans le Connexion à AWS Guide de l'utilisateur

Attribution d'un accès à d'autres utilisateurs

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme à la meilleure pratique consistant à appliquer les autorisations du moindre privilège.

Pour obtenir des instructions, voir [Créer un ensemble d'autorisations](#) dans le AWS IAM Identity Center Guide de l'utilisateur

2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

Pour obtenir des instructions, voir [Ajouter des groupes](#) dans AWS IAM Identity Center Guide de 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 votre AWS Control Tower comptes, dans le AWS Organizations .

- [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 souhaitez peut-être consulter la section intitulée «[Planifiez la zone d'atterrissage de votre AWS Control Tower](#)», avant de continuer.

Rubriques

- [Guide de démarrage rapide d'AWS Control Tower](#)
- [Prérequis : vérifications automatisées avant le lancement de votre compte de gestion](#)
- [Commencez à utiliser AWS Control Tower depuis la console](#)
- [Commencez à utiliser AWS Control Tower en utilisant APIs](#)
- [Étapes suivantes](#)

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](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.

Commencez à utiliser AWS Control Tower depuis la console

Cette procédure de démarrage est destinée aux administrateurs AWS de 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 souhaitez peut-être consulter la section intitulée «[Planifiez la zone d'atterrissage de votre AWS Control Tower](#)», avant de continuer.

Rubriques

- [Attentes relatives à la configuration de la zone d'atterrissage](#)
- [Étape 1 : Créez les adresses e-mail de votre compte partagé](#)
- [Étape 2. Configurez et lancez votre zone d'atterrissage](#)
- [Étape 3. Vérifiez et configurez la zone d'atterrissage](#)

Attentes relatives à la configuration de la zone d'atterrissage

Le processus de configuration de la zone d'atterrissage de votre AWS Control Tower comporte plusieurs étapes. Certains aspects de la zone d'atterrissage AWS de votre 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 niveaux supérieurs OUs sont nommés Security et Sandbox. Pour de plus amples informations, veuillez consulter [Directives pour la mise en place d'un environnement bien conçu](#).
- Lors de l'installation, vous pouvez sélectionner des noms personnalisés pour les comptes partagés créés par AWS Control Tower, appelés archive des 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 que AWS Control Tower utilisera comme comptes d'audit et d'archivage des journaux. Si vous envisagez 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 vous configurez 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 vous pouvez choisir de ne pas choisir les sentiers gérés par AWS Control Tower et de gérer vos propres CloudTrail sentiers. Vous pouvez

accepter ou non les parcours organisés 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 approvisionner des comptes de membres personnalisés à partir de la console Control Tower. AWS Vous pourrez personnaliser les comptes ultérieurement si vous ne disposez pas d'un plan. Consultez [Personnalisez les comptes avec Account Factory Customization \(AFC\)](#).

Choix de configuration irréversibles

- 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 VPCs, ils ne VPC CIDRs peuvent pas être modifiés une fois qu'ils ont été créés.

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

Si vous configurez votre zone d'atterrissage dans une nouvelle zone Compte AWS, consultez [Configuration](#).

- Pour configurer votre zone d'atterrissage 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 les comptes enregistrés OUs 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 d'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 s'assurer qu'aucune ressource n'est en conflit avec les exigences de 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 de plus amples informations, veuillez consulter [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 de la AWS Control Tower (OUs) afin de l'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.

Étape 2. Configurez et lancez votre zone d'atterrissage

Avant de lancer la zone d'atterrissage AWS de votre Control Tower, déterminez la région d'origine la plus appropriée. Pour de plus amples informations, veuillez consulter [Conseils administratifs pour la configuration de la zone d'atterrissage](#).

Important

Changer de région d'origine après avoir déployé la zone d'atterrissage de votre AWS Control Tower nécessite la 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'entrée [Commencez à utiliser AWS Control Tower en utilisant APIs](#).

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. Vérifiez 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 pour l'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 (OUs)

Si vous acceptez les noms par défaut de ces dernières OUs, vous n'avez aucune action à effectuer pour que l'installation continue. Pour modifier les noms des OUs, entrez les nouveaux noms directement dans le champ du formulaire.

- **OU 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**.
- **OU supplémentaire** — AWS Control Tower peut configurer une ou plusieurs unités supplémentaires OUs 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 le [Directives pour la mise en place d'un environnement bien conçu](#). Si vous avez déjà une unité d'organisation existante dans Control Tower AWS Organizations, vous pouvez voir apparaître l'option permettant de ne pas configurer 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 la facturation AWS de 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 que 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 des utilisateurs, des rôles et des 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 une fédération directe de comptes, soit pour une fédération de comptes multiples via Identity Center. IAM Vous pourrez modifier cette sélection ultérieurement.

Par défaut, AWS Control Tower configure 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 de plus amples informations, veuillez consulter [IAM Conseils relatifs au centre d'identité](#).

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 KMS clé 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 KMS clé. 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 KMS clé

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

Pour utiliser une KMS clé avec AWS Control Tower, vous devez mettre à jour la politique de KMS clé 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 KMS clé, vous pouvez ajouter des autorisations en tant que groupe dans une seule JSON déclaration ou ligne par ligne.

La procédure décrit comment mettre à jour la politique de KMS clé 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'identifiant du compte de gestion sur lequel la AWS Control Tower sera configurée.
- **YOUR-HOME-REGION**— la région d'origine que vous allez sélectionner lors de la configuration AWS de Control Tower.
- **YOUR-KMS-KEY-ID**— l'ID de KMS clé qui sera utilisé avec la politique.

Pour mettre à jour la politique KMS clé

1. Ouvrez la AWS KMS console à l'adresse <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 KMS clé 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 KMS clé

L'exemple de politique suivant montre à quoi pourrait ressembler votre politique KMS clé 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 KMS clé 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 KMS clé 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 également [Spécification de conditions dans une politique](#).

Le AWS Key Management Service (AWS KMS) vous permet de créer des clés multirégionales et KMS des clés asymétriques ; toutefois, AWS Control Tower ne prend pas en charge les clés multirégionales ou asymétriques. AWSControl 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 de Control Tower.

Pour plus d'informations à ce sujet AWS KMS, consultez [le guide du AWS KMS développeur](#).

Notez que les données des clients dans AWS Control Tower sont cryptées 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 provisionner des comptes de membres personnalisés depuis la console Control Tower. AWS Vous pourrez personnaliser les comptes ultérieurement si vous ne disposez pas d'un plan. Consultez [Personnalisez les comptes avec Account Factory Customization \(AFC\)](#).

Étape 3. Vérifiez et configurez la zone d'atterrissage

La section suivante de la configuration vous 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 êtes prêt, choisissez Je comprends les autorisations que 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 root, l'unité d'organisation de sécurité et les comptes partagés. D'autres AWS ressources sont créées, modifiées ou supprimées.

Confirmer SNS les abonnements

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.

Commencez à utiliser AWS Control Tower en utilisant APIs

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

Dans cette procédure, vous APIs utiliserez AWS Control Tower et d'autres AWS services pour configurer et lancer une zone d'atterrissage. Ils vous APIs 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 la zone d'atterrissage de votre AWS Control Tower, effectuez les tâches préalables suivantes :

- Déterminez la région d'origine la plus appropriée. Pour de plus amples informations, veuillez consulter [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 avec APIs](#)
- [Étape 1 : Configurez votre zone de landing zone](#)
- [Étape 2 : Lancez votre zone de landing zone](#)
- [Identifiez votre zone de landing](#)
- [Mettez à jour votre zone de landing zone](#)
- [Réinitialisez la zone d'atterrissage pour résoudre le problème de dérive](#)
- [Démantelez votre zone d'atterrissage](#)
- [Consultez l'état des opérations de votre zone d'atterrissage](#)
- [Exemples : configurer une zone de landing zone AWS Control Tower avec des API uniquement](#)
- [Lancez une zone d'atterrissage en utilisant AWS CloudFormation](#)

Attentes relatives à la configuration de la zone d'atterrissage avec APIs

Le processus de configuration de la zone d'atterrissage de votre AWS Control Tower comporte plusieurs étapes. Certains aspects de la zone d'atterrissage AWS de votre 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 une fois que vous avez configuré votre zone d'atterrissage. Par défaut, les fondamentaux s'appellent Security et Sandbox. Pour de plus amples informations, veuillez consulter [Directives pour la mise en place d'un environnement bien conçu](#).
- Lors de l'installation, vous pouvez sélectionner des noms personnalisés pour les comptes partagés créés par AWS Control Tower, appelés archive des 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 APIs, vous devez spécifier les AWS comptes existants que AWS Control Tower utilisera comme comptes d'audit et d'archivage des journaux. Pour spécifier AWS des comptes existants, si ces comptes ont AWS Config des 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 le configurez 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 vous pouvez choisir de ne pas choisir les sentiers gérés par AWS Control Tower et de gérer vos propres CloudTrail sentiers. Vous pouvez accepter ou non les parcours organisés 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 VPCs, ils ne VPC CIDRs 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, voir [Exemples : 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 la zone d'atterrissage de votre AWS Control Tower comporte plusieurs étapes. Certains aspects de la zone d'atterrissage de votre 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 la zone d'atterrissage de la AWS Control Tower APIs, vous devez APIs d'abord appeler 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 IAM rôle ou un utilisateur du centre d'IAM identité disposant des autorisations requises pour appeler la zone de landing zone APIs.

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

1. Appelez le AWS Organizations `CreateOrganization` API et activez toutes les fonctionnalités pour créer l'unité d'organisation fondamentale. AWSControl 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
```

AWSControl Tower peut configurer un ou plusieurs modules supplémentaires OUs. 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 le [AWS stratégie multi-comptes pour votre zone de landing AWS zone de 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 la zone d'atterrissage APIs pour configurer AWS Control Tower pour la première fois, vous devez utiliser les AWS comptes de sécurité et d'archivage des 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 de AWS Organizations APIs.

1. Appelez le 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 l'état de l'CreateAccountopération à l'aide du AWS Organizations DescribeAccountAPI.

Étape 3. Créez les rôles de service requis

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

- [AWSControlTowerAdmin](#)
- [AWSControlTowerCloudTrailRole](#)
- [AWSControlTowerStackSetRole](#)
- [AWSControlTowerConfigAggregatorRoleForOrganizations](#)

Pour plus d'informations sur ces rôles et leurs politiques, consultez [Utilisation de politiques basées sur l'identité \(politiques IAM\) pour AWS Control Tower](#).

Pour créer un IAM rôle, procédez comme suit :

1. Créez un IAM rôle doté des autorisations nécessaires pour appeler toutes les zones de landing zone APIs. 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:ListLandingZoneOperations",
        "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

La AWS Control Tower `CreateLandingZone` API 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

AWSControl Tower ne prend pas en charge le refus de contrôle par région lors de l'utilisation APIs pour configurer et lancer une zone d'atterrissage. Après avoir lancé avec succès votre zone d'atterrissage à l'aide de la console Control TowerAPIs, vous pouvez utiliser la console AWS Control Tower pour [configurer le refus de contrôle de la région](#).

1. Appelez la AWS Control Tower CreateLandingZoneAPI. Cela 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-ecfXXXXXXXXXX"
  },
  "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-446XXXXXXXXXX"
}

```

2. Appelez le GetLandingZoneOperation API pour vérifier le statut de l'CreateLandingZoneopération. GetLandingZoneOperationAPIRenvoie le statut SUCCEEDFAILED, ouIN_PROGRESS.

```
aws controltower get-landing-zone-operation --operation-identifler "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 telSUCCEEDED, vous pouvez appeler le GetLandingZone API pour vérifier la configuration de la zone d'atterrissage.

```
aws controltower get-landing-zone --landing-zone-identifiant "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": "Security"
        }
      },
      "centralizedLogging": {
        "accountId": "222222222222",
        "configurations": {
```

```

        "loggingBucket": {
            "retentionDays": 60
        },
        "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXXX",
        "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 auprès AWS de Control Tower. Cela 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.

ARNs Les zones d'atterrissage sont uniques au niveau régional.

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

Pour les [régions optionnelles](#), l'identifiant de la zone d'atterrissage **ListLandingZones** API n'est renvoyé que si vous les appelez API dans la même région que leur région API d'origine. Par exemple, si votre zone d'atterrissage est configurée dans af-south-1 et que vous appelez **ListLandingZones** af-south-1, l'identifiant de la zone d'atterrissage est renvoyé. API Si votre zone d'atterrissage est configurée dans af-south-1 et que vous appelez **ListLandingZones** ap-east-1, l'identifiant de la zone d'atterrissage ne sera pas renvoyé. API

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 mises à jour à la configuration de votre zone d'atterrissage, vous pouvez appeler le fichier manifeste mis à jour UpdateLandingZone API et y faire référence. Cela API renvoie un `OperationIdentifier`, que vous pouvez ensuite utiliser lorsque vous appelez le `GetLandingZoneOperation` API pour vérifier l'état de l'opération de mise à jour.

Pour mettre à jour la zone d'atterrissage

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

```
aws controltower update-landing-zone --landing-zone-version 3.3 --landing-zone-
identifiant "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": "Security"
    },
    "sandbox": {
      "name": "Sandbox"
    }
  },
  "centralizedLogging": {
    "accountId": "222222222222",
    "configurations": {
      "loggingBucket": {
        "retentionDays": 2555
      },
      "accessLoggingBucket": {
        "retentionDays": 2555
      },
    }
  }
}
```

```
"kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXXX"
  },
  "enabled": true
},
"securityRoles": {
  "accountId": "333333333333"
},
"accessManagement": {
  "enabled": true
}
}
```

Sortie :

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

-  Réenregistrez éventuellement l'unité d'organisation pour mettre à jour les comptes
- Pour les AWS Control Tower enregistrées OUs 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 Ré-enregistrer 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 (OUs), comptes et 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 le `GetLandingZoneAPI`. Cela 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 le `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, les appels `ResetLandingZone` maintiennent cette configuration désactivée IAM d'Identity Center.

Vous ne pouvez utiliser le que `ResetLandingZone` API si vous utilisez la dernière version de zone d'atterrissage disponible. Vous pouvez appeler `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. Appelle le `GetLandingZoneAPI`. Si le API renvoie un statut de dérive de `DRIFTED`, votre zone d'atterrissage est en dérive.
2. Appelez le `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-446XXXXXXXXXX"
}
```

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 `DeleteLandingZoneAPI`. Cela API renvoie un `OperationIdentifier`, que vous pouvez ensuite utiliser lorsque vous appelez le `GetLandingZoneOperation` API pour vérifier l'état de l'opération de suppression.

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

Sortie :

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

Consultez l'état des opérations de votre zone d'atterrissage

L'`ListLandingZoneOperationsAPI` vous permet de consulter l'état des opérations AWS Control Tower qui exécutent des actions sur votre zone de landing zone.

Pour plus d'informations sur cette opération d'API, consultez [ListLandingZoneOperations](#).

ListLandingZoneOperations

Exemple d'entrée et de sortie pour **ListLandingZoneOperations**.

Cet exemple montre comment appeler l'API sans paramètres.

```
aws controltower --region us-east-1 list-landing-zone-operations
{
```



```

"landingZoneOperations": [
  {
    "operationIdentifier": "873fe98d-1ecc-4154-b593-86e4a95ebfXX",
    "operationType": "CREATE",
    "status": "FAILED"
  },
  {
    "operationIdentifier": "0016d43d-a307-4ad8-a2a2-b427b8eb1cXX",
    "operationType": "DELETE",
    "status": "SUCCEEDED"
  },
  {
    "operationIdentifier": "002b8b5a-6bb7-4c40-89cd-5822a73d13XX",
    "operationType": "CREATE",
    "status": "SUCCEEDED"
  },
  {
    "operationIdentifier": "008886a0-f7a2-4df3-90e8-6e9f936507XX",
    "operationType": "CREATE",
    "status": "FAILED"
  }
]
}

```

Cet exemple montre comment appeler l'API et spécifier le nombre maximum de résultats.

```
aws controltower --region us-east-1 list-landing-zone-operations --max-results 1
```

```

{
  "landingZoneOperations": [
    {
      "operationIdentifier": "873fe98d-1ecc-4154-b593-86e4a95ebfXX",
      "operationType": "CREATE",
      "status": "FAILED"
    }
  ],
  "nextToken": "AAMAATFMzwP0QysYY8npWgstfcHGQBj-
XCC18ISyd9mkQmzLR7ZFMket4F0aWv8tUTtnsTW0nfb1Up_Q9U-
nX9_6lEsLHs0R1hceDKskHr0_3fm8KdPTa6ofxMt5SPw8WF7-Jsvw2rJVvhj4DHDipo-y1HVK_eZ__Z3-
0zInm403cIHxhbjGPgqCX6FeKr8lwgTDK0ejkLYZ9w7J5aqPAKLfVP8KKNda5g0VfMj1wdl4J2nwnHI-
UuCTIZ5nUEgXgUHaFq6Ma1pLDfGefZQJn5HmDhhgd5yvqzSRH1BtrHpdV_N1EVP8u3JJr3eWQHe9jNB021ihD4Mdcbm3SJg
VXRwTUIBInrit4Hs1NtPE8-IC1gxCjGoYPGtuWBPumK-pUPE="
}

```

Cet exemple montre comment appeler l'API et obtenir un résultat paginé avec `nextToken`.

```
aws controltower --region us-east-1 list-landing-zone-operations --next-token
AAMAATFMzwP0QysYY8npWgstfcHGQBj-XCC18ISyd9mkQmzLR7ZFMket4F0aWv8tUTtnsTW0nfb1Up_Q9U-
nX9_6lEsLHs0R1hceDKskHr0_3fm8KdPTa6ofxMt5SPw8WF7-Jsvw2rJVvhj4DHDipo-y1HVK_eZ__Z3-
OzInm403cIHxhbjGPgqCX6FeKr8lwgTDK0ejkLYZ9w7J5aqPAKLfVP8KKNda5g0VfMj1wdl4J2nwnHI-
UuCTIZ5nUEgXgUHaFq6Ma1pLDfGefZQJn5HmDhhgd5yvqzSRH1BtrHpdV_N1EVP8u3JJr3eWQHe9jNB021ihD4Mdcbm3Sjg
VXRwTUIBInrit4Hs1NtPE8-IC1gxCjGoYPGtuWBPumK-pUPE=

{
  "landingZoneOperations": [
    {
      "operationIdentifier": "0016d43d-a307-4ad8-a2a2-b427b8eb1cXX",
      "operationType": "DELETE",
      "status": "SUCCEEDED"
    },
    {
      "operationIdentifier": "002b8b5a-6bb7-4c40-89cd-5822a73d13XX",
      "operationType": "CREATE",
      "status": "SUCCEEDED"
    },
    {
      "operationIdentifier": "008886a0-f7a2-4df3-90e8-6e9f936507XX",
      "operationType": "CREATE",
      "status": "FAILED"
    }
  ]
}
```

Cet exemple montre comment appeler l'API avec un filtre.

```
aws controltower --region us-east-1 list-landing-zone-operations --filter '{"types":
["CREATE"],"statuses":["FAILED"]}'

{
  "landingZoneOperations": [
    {
      "operationIdentifier": "873fe98d-1ecc-4154-b593-86e4a95ebfXX",
      "operationType": "CREATE",
      "status": "FAILED"
    },
    {
      "operationIdentifier": "008886a0-f7a2-4df3-90e8-6e9f936507XX",
```

```
        "operationType": "CREATE",
        "status": "FAILED"
    }
  ]
}
```

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 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 >cloudtrail_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 permettent ensuite de 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 en configurant une boucle.

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-identifiant
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-identifiant 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/4B3H0ULNU0L2AXXX"
    }
  ]
}
```

Étape 2. Obtenez les informations

```
aws --region us-west-1 controltower get-landing-zone --landing-zone-identifiant
arn:aws:controltower:us-west-1:123456789012:landingzone/4B3H0ULNU0L2AXXX
```

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

```
{
  "landingZone": {
    "arn": "arn:aws:controltower:us-
west-1:123456789012:landingzone/4B3H0ULNU0L2AXXX",
    "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"
}
}
```

Étape 6. (Facultatif) Appelez l'**ListLandingZoneOperationsAPI** pour consulter le statut de toute opération modifiant votre zone d'atterrissage.

Pour suivre l'état de toute opération de zone d'atterrissage, vous pouvez appeler [l'ListLandingZoneOperationsAPI](#).

Lancez une zone d'atterrissage en utilisant 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 de APIs through AWS CloudFormation.

Rubriques

- [Conditions préalables au lancement d'une zone d'atterrissage à l'aide de AWS CloudFormation](#)
- [Créez une nouvelle zone d'atterrissage à l'aide de AWS CloudFormation](#)
- [Gérez une zone d'atterrissage existante à l'aide de AWS CloudFormation](#)

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

1. À partir de AWS CLI, utilisez le 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 `AWSControlTowerAdmin`, `AWSControlTowerCloudTrailRole`, `AWSControlTowerConfigAggregatorRoleForOrganizations`, et `AWSControlTowerStackSetRole` de service.

Pour plus d'informations sur la manière dont AWS Control Tower utilise ces rôles pour effectuer des API appels 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 d'atterrissage à l'aide de 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 corriger la dérive dans une zone d'atterrissage](#), vous pouvez utiliser la console AWS Control Tower, le AWS CLI, ou le [ResetLandingZoneAPI](#).


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 la configuration de groupes, de rôles et de 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 garantie [Validation 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, consultez [Résolution 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, consultez [Limites de contrôle](#).

Le guide de référence sur les commandes

Les informations détaillées sur les commandes de AWS Control Tower ont été transférées dans [le guide de référence de AWS Control Tower Controls](#).

Limitations connues de AWS Control Tower

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

- AWSControl Tower a 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 unAPI. 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 que ces modifications apparaissent dans la console AWS Control Tower.
- Une limite de cinq (5) SCPs par unité d'organisation s'applique OUs à la zone d'atterrissage AWS de votre Control Tower.
- AWSControl Tower prend en charge jusqu'à 10 000 comptes dans l'organisation de votre zone d'atterrissage, répartis entre tous les vôtresOUs.

- Les comptes existants OUs avec plus de 1 000 comptes directement imbriqués ne peuvent pas être enregistrés ou réenregistrés dans AWS Control Tower. Pour plus d'informations sur les limites liées à l'enregistrement OUs, consultez [Limitations basées sur les AWS services sous-jacents](#).
- Les personnalisations pour AWS Control Tower (CfCT) ne sont pas disponibles dans ces environnements Régions AWS, car certaines dépendances ne le sont pas :
 - Région Europe (Zurich), eu-central-2
 - Région Europe (Espagne), eu-south-2
 - Canada Ouest (Calgary)

Vous pouvez déployer et gérer des ressources dans ces régions avec CfCT, si vous déployez CfCT dans la région d'origine de votre AWS Control Tower, mais vous ne pouvez pas créer de CfCT dans ces régions.

- AWSControl Tower Account Factory for Terraform (AFT) n'est pas disponible dans les versions suivantes Régions AWS, car certaines dépendances ne le sont pas :
 - Région Europe (Zurich), eu-central-2
 - Région Europe (Espagne), eu-south-2
 - Canada Ouest (Calgary)
- AWSControl Tower Account Factory for Terraform (AFT) ne peut pas être déployé par de nouveaux AFT clients dans les régions suivantes, car AWS CodeStar Connections n'est pas disponible pour se connecter à un système de contrôle de version tiers () VCS :
 - Asie-Pacifique (Hong Kong), Afrique (Le Cap), Moyen-Orient (Bahreïn), Europe (Zurich), Asie-Pacifique (Jakarta), Asie-Pacifique (Hyderabad), Asie-Pacifique (Osaka), Asie-Pacifique (Melbourne), Israël (Tel Aviv), Europe (Espagne) et Moyen-Orient () UAE
- Les régions suivantes ne prennent pas en charge IAM Identity Center.
 - Région du Moyen-Orient (UAE), 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 de AWS Control Tower dans les régions non prises en charge AWS Service Catalog, consultez [AWSControl Tower disponible en AWS Canada Ouest \(Calgary\)](#).

- Lorsque vous appelez une commande API pour activer ou désactiver une commande, la limite pour les `DisableControl` mises à jour `EnableControl` et les mises à jour dans AWS Control Tower sont 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 AWS de 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 [Limitations basées sur les AWS services sous-jacents](#) la documentation AWS de Control Tower. Par défaut : 1000, non réglable.
- Opérations simultanées pour les unités organisationnelles (OUs) : nombre maximum d'opérations simultanées liées aux unités d'organisation 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 de la 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 peut prendre SCPs plus de temps qu'avec trois SCPs.

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 de AWS Control Tower.

Vous pouvez également contacter le [AWS Support](#) pour demander une augmentation du quota pour certaines ressources de 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

AWSControl Tower vous aide à maintenir un environnement multi-comptes sécurisé au AWS moyen de contrôles mis en œuvre sous différentes formes, tels que des politiques de contrôle des services (SCPs), des AWS Config règles et des AWS CloudFormation hooks.

Le guide de référence sur les commandes

Les informations détaillées sur les commandes de AWS Control Tower ont été transférées dans [le guide de référence de AWS Control Tower Controls](#).

Si vous modifiez les ressources de la AWS Control Tower, telles qu'une ressource 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 commandes 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 SCPs des commandes préventives lors de la mise à jour de votre zone d'atterrissage. Les modifications que vous avez éventuellement apportées SCPs sont remplacées par la version standard du contrôle, par conception.

Limitations par région

Certaines commandes de AWS Control Tower ne fonctionnent pas dans certaines régions AWS où AWS Control Tower est disponible, car ces régions ne prennent pas en charge les fonctionnalités sous-jacentes requises. Par conséquent, lorsque vous déployez ce contrôle, il se peut qu'il ne fonctionne pas dans toutes les régions que vous gouvernez avec AWS Control Tower. Cette limitation concerne certains contrôles de détection, certains contrôles proactifs et certains contrôles du Security Hub Service-managed Standard : AWS Control Tower. Pour plus d'informations sur la disponibilité régionale, consultez les [contrôles du Security Hub](#). Consultez également 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 de plus amples informations, veuillez consulter [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, consultez [Considérations relatives à l'activation des AWS régions optionnelles](#).

Note

Pour obtenir les informations les plus récentes sur les contrôles et le support régional, nous vous recommandons d'appeler les [ListControls](#) API opérations [GetControl](#)et.

Trouvez les commandes et les régions disponibles

Vous pouvez consulter les régions disponibles pour chaque contrôle dans la console AWS Control Tower. Vous pouvez afficher les régions disponibles par programmation à l'aide du catalogue de AWS contrôle [GetControl](#)et [ListControls](#)APIsà partir de celui-ci.

Consultez également le tableau de référence des commandes AWS Control Tower et des régions prises en charge, ainsi que [la disponibilité des commandes par région](#), dans le guide de référence de AWS Control Tower Controls.

Non compatible Régions AWS avec AWS Security Hub Service-Managed Standard : Control Tower AWS

Pour plus d'informations sur les AWS Security Hub contrôles du Service-Managed Standard : AWS Control Tower qui ne sont pas pris en charge dans certaines régions Régions AWS, consultez la section « Régions non prises en charge » dans le standard [Security](#) Hub.

Les régions suivantes Régions AWS, en tant que région d'origine, ne prennent pas en charge le déploiement de contrôles proactifs. Vous pouvez déployer des contrôles proactifs pour gouverner ces régions si vous déployez les contrôles depuis une autre région d'origine qui prend 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 déployables
CT.DAX.PR.2	ca-west-1, us-west-1

Identifiant de contrôle	Régions non déployables
CT.REDSHIFT.PR.5	ap-southeast-2, ap-southeast-3, ap-southeast-4, ca-ouest-1, eu-central-2, eu-sud-2, il-central-1, il-central-1

Le tableau suivant indique les commandes de détection AWS de la Control Tower qui ne sont pas prises en charge dans certains cas Régions AWS.

Identifiant de contrôle	Régions non déployables
AWS-GR_AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED	ap-northeast-3, ap-southeast-3, ap-southeast-4, ca-ouest-1, il-central-1
AWS-GR_DMS_REPLICATION_NOT_PUBLIC	af-south-1, ap-southeast-2, ap-southeast-3, ap-southeast-4, ca-ouest-1, eu-central-2, eu-sud-1, eu-centre-2, eu-sud-2, il-central-1, eu-central-1, eu-central-1 me-central-1
AWS-GR_EBS_OPTIMIZED_INSTANCE	ca-west-1
AWS-GR_EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK	eu-south-2
AWS-GR_EC2_INSTANCE_NO_PUBLIC_IP	ap-northeast-3
AWS-GR_EC2_VOLUME_INUSE_CHECK	ca-west-1
AWS-GR_EKS_ENDPOINT_NO_PUBLIC_ACCESS	ca-west-1
AWS-GR_ELASTICSEARCH_IN_VPC_ONLY	ap-southeast-2, ap-southeast-3, ap-southeast-4, ca-ouest-1, eu-central-2, eu-sud-2, il-central-1
AWS-GR_EMR_MASTER_NO_PUBLIC_IP	af-south-1, ap-northeast-3, ap-southeast-2, ap-southeast-3, ap-southeast-4, ca-ouest-1, eu-central-2, eu-sud-1 2, il-central-1, me-central-1

Identifiant de contrôle	Régions non déployables
AWS-GR_ENCRYPTED_VOLUMES	af-south-1, ap-northeast-3, eu-south-1, il-central-1
AWS-GR_IAM_USER_MFA_ENABLED	ap-southeast-2, ap-southeast-4, ca-ouest-1, eu-central-2, eu-sud-2, il-central-1, me-central-1
AWS-GR_LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED	eu-south-2
AWS-GR_MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS	ap-southeast-2, ap-southeast-4, ca-ouest-1, eu-central-2, eu-sud-2, il-central-1, me-central-1
AWS-GR_NO_UNRESTRICTED_ROUTE_TO_IGW	ap-northeast-3, ap-southeast-2, ap-southeast-3, ca-ouest-1, eu-south-2
AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK	ap-south-2, eu-south-2
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_RDS_STORAGE_ENCRYPTED	eu-central-2, eu-south-2
AWS-GR_REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK	ap-south-2, ap-southeast-3, ca-ouest-1, eu-sud-2
AWS-GR_RESTRICTED_SSH	af-south-1, eu-south-1
AWS-GR_ROOT_ACCOUNT_MFA_ENABLED	ca-west-1, il-central-1, me-central-1
AWS-GR_S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC	eu-central-2, eu-sud-2, il-central-1
AWS-GR_SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS	af-south-1, ap-northeast-3, ap-southeast-2, ap-southeast-3, ap-southeast-4, ca-ouest-1, eu-central-2, eu-sud-1 2, il-central-1, me-central-1
AWS-GR_SSM_DOCUMENT_NOT_PUBLIC	ca-west-1, il-central-1

Identifiant de contrôle	Régions non déployables
AWS-GR_SUBNET_AUTO_ASSIGN_P UBLIC_IP_DISABLED	ap-northeast-3

Limitations basées sur les AWS services sous-jacents

Cette page décrit les limitations que vous pouvez rencontrer en raison des limitations d'autres AWS services, ainsi que la manière dont AWS Control Tower fonctionne avec ces services.

Directives générales

En règle générale, nous nous attendons à ce que le nombre de comptes pris en charge lors de l'enregistrement d'une unité d'organisation diminue à mesure que vous augmentez le nombre de régions régies et le nombre de contrôles activés pour cette unité d'organisation. Ces directives générales supposent que 15 contrôles facultatifs sont activés. Si plus ou moins de contrôles sont activés sur votre unité d'organisation, les limites de comptes par unité d'organisation seront différentes lors de l'enregistrement.

- Avec 15 régions gouvernées, OUs jusqu'à 1 000 comptes sont pris en charge.
- Avec 16 à 21 régions gouvernées, la taille maximale de l'unité d'organisation prise en charge est comprise entre 600 et 1 000 comptes.
- Avec 22 régions gouvernées, OUs jusqu'à 680 comptes sont pris en charge.
- Avec 23 régions gouvernées ou plus, la taille maximale de l'unité d'organisation prise en charge est inférieure à 680 comptes.

En cas d'erreur

Si l'enregistrement échoue, vous pouvez essayer de réenregistrer l'unité d'organisation. Vous pouvez également réduire la taille de l'UO en utilisant une UO imbriquée ou en déplaçant des comptes vers une autre UO.

Note

Les contrôles obligatoires que AWS Control Tower applique toujours ne sont pas pris en compte dans le nombre de contrôles que vous avez activés sur une unité d'organisation, aux fins de l'enregistrement.

AWS CloudFormation limites des ensembles de piles

Si vous envisagez d'enregistrer un grand nombre de comptes répartis sur plusieurs comptes Régions AWS, vous risquez de rencontrer des limites imposées par AWS CloudFormation des ensembles de comptes 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 \leq 150 000

Cette limitation apparaît au cours du processus d'enregistrement de l'UO. Par exemple, si 15 régions sont gouvernées et que 15 contrôles facultatifs sont activés, la limite d'enregistrement de l'unité d'organisation est de 1 000 comptes. Toutefois, si vous devez vous inscrire OUs avec plus de 1 000 comptes, ou si un grand nombre de contrôles facultatifs sont activés, vous devez réduire le nombre de régions gouvernées à moins de 15. Cette réduction est due aux limites du stack set.

AWS Config limites

Si vous prévoyez de vous enregistrer OUs avec un grand nombre de comptes, vous pouvez rencontrer des limites quant [au nombre maximum de comptes pouvant AWS Config être créés ou supprimés chaque semaine](#), tous agrégateurs confondus. Les comptes inscrits ne sont pas pris en compte dans cette limite : vous pouvez inscrire jusqu'à 1 000 nouveaux comptes dans AWS Control Tower chaque semaine.

Limitations relatives à la première utilisation des comptes et des régions d'inscription

Si vous prévoyez de vous inscrire pour la première fois OUs auprès d'un grand nombre de comptes répartis dans plusieurs régions participantes, vous risquez de rencontrer des limites en raison des [quotas de gestion des comptes](#), ce qui peut entraîner une latence prolongée. Des erreurs peuvent survenir lors de l'enregistrement de l'unité d'organisation en raison de la latence.

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 AWS de 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 de 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 de 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 access advisor** — L'outil access advisor AWS Identity and Access Management (IAM) vous permet de déterminer les autorisations dont disposent vos développeurs en analysant le dernier horodatage auquel une IAM entité, telle qu'un utilisateur, un rôle ou un groupe, a appelé un AWS service. 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](#).
- **IAM simulateur de politiques** : avec le simulateur de IAM politiques, vous pouvez tester et résoudre les problèmes liés aux politiques IAM basées sur les ressources. Pour plus d'informations, voir [Tester des IAM politiques avec le simulateur IAM de politiques](#).
- **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 de 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 la 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 règles en utilisant des politiques de contrôle des services (SCPs).

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 OUs 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'un des contrôles applicables OUs pour lesquels 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 des informations détaillées sur les commandes et leurs fonctions, voir [À propos des commandes dans AWS Control Tower](#).

Planifiez la zone d'atterrissage de votre AWS Control Tower

Au cours du processus de configuration, AWS Control Tower lance une ressource clé associée à votre compte, appelée landing zone, 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, consultez [AWS stratégie multi-comptes pour votre zone de landing AWS zone de Control Tower](#).

Méthodes de configuration de la 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.
- [Lancez AWS Control Tower dans une nouvelle organisation](#): Cette section est destinée aux clients n'ayant pas OUs de compte existant AWS Organizations.

Note

Si vous disposez déjà d'une zone d' AWS Organizations atterrissage, vous pouvez étendre la gouvernance de la AWS Control Tower de la zone d'atterrissage existante à tout ou partie de vos comptes OUs 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 de AWS Control Tower à une organisation existante ou l'extension de la gouvernance de AWS Control Tower aux comptes OUs 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 une 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 de 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 comptes OUs et au sein de votre organisation existante.

À propos de l'extension de la gouvernance : l'extension de la gouvernance s'applique à des comptes spécifiques OUs au sein d'une même organisation déjà enregistrée auprès de 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 de la AWS Control Tower sont étendus de telle sorte que leurs contraintes s'appliquent OUs aux comptes spécifiques 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 [solution AWS Landing Zone \(ALZ\)](#) pour AWS Organizations, contactez votre architecte de AWS solutions avant d'essayer d'activer AWS Control Tower dans votre organisation. AWSControl 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 d'atterrissage. 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 [Si le compte ne répond pas aux prérequis](#)

Lancer AWS Control Tower dans une organisation existante

En configurant une zone d'atterrissage AWS Control Tower dans une organisation existante, vous pouvez commencer à travailler immédiatement, en parallèle avec votre AWS Organizations environnement existant. Vos autres OUs créations AWS Organizations sont inchangées, car elles ne sont pas enregistrées auprès AWS de Control Tower. Vous pouvez continuer à les utiliser OUs ainsi que les comptes tels qu'ils sont.

AWSControl 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 AWS de 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 de votre zone de landing AWS Control Tower.

Lorsque vous configurez votre zone d'atterrissage, 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 AWS de 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 AWS de votre zone d'atterrissage Control Tower dans une AWS Organizations organisation existante ne vous permet pas d'étendre AWS la gouvernance de cette organisation à d'autres OUs ou à des comptes qui ne sont pas enregistrés auprès de AWS Control Tower.

Pour lancer AWS Control Tower dans votre organisation existante, suivez le processus décrit dans [Commencer à utiliser AWS Control Tower](#).

Pour plus d'informations sur la manière dont AWS Control Tower interagit avec les AWS Organizations organisations existantes, consultez [Gérez les organisations et les comptes avec AWS Control Tower](#).

Lancez AWS Control Tower dans une nouvelle organisation

Si vous utilisez AWS Control Tower pour la première fois et que vous n'avez jamais travaillé avec AWS Organizations lui, le meilleur point de départ est de consulter notre [Configuration](#) document.

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

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

AWSLes clients de 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 d'atterrissage de la AWS Control Tower.

AWSControl 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 Organizations Une fois votre zone de landing zone configurée, AWS Control Tower continue de vous aider à appliquer les politiques et les pratiques de sécurité de votre entreprise 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 (OUs) et de comptes augmente dans votre zone d'atterrissage de 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, par conséquent, gérer plusieurs charges de travail et environnements.

AWSControl Tower met en place un environnement bien conçu. Il s'appuie 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.

AWSControl 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 de landing zone, 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
- Unités organisationnelles multiples (OUs)
- Une structure bien planifiée

Utiliser plusieurs AWS comptes

Un seul compte ne suffit pas pour configurer un environnement bien conçu. En utilisant plusieurs comptes, vous pouvez mieux répondre à vos objectifs de sécurité et à 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 (GDPR).
- **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

AWSControl Tower et d'autres structures 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 (OUs), à des fins de gouvernance et de contrôle. OUs sont conçus 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 mise en scène peuvent être créés et gérés séparément OUs, et facturés sous forme de comptes distincts. En outre, vous souhaitez peut-être configurer une unité d'organisation Sandbox pour tester le code.

Utilisez une structure bien planifiée pour votre OUs zone d'atterrissage

AWSControl Tower en configure certaines automatiquement OUs 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 votre unité OUs après avoir configuré votre zone d'atterrissage en sélectionnant Modifier sur la page détaillée de l'UO.

Recommandations

Une fois que AWS Control Tower a configuré la première unité d'organisation requise pour vous, l'unité d'organisation de sécurité, nous vous recommandons d'en créer une autre OUs 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. AWSControl Tower peut configurer l'unité d'organisation Sandbox pour vous lors de la création de la zone d'atterrissage, si vous la sélectionnez.

OUsVous pouvez en configurer vous-même deux autres : 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 des charges de travail. Vous pouvez en ajouter d'autres OUs dans votre zone de landing zone via la console AWS Control Tower sur la page Organizational units.

OUsRecommandé en plus de ceux configurés automatiquement

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

Note

AWSControl 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

AWSControl 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

AWSControl Tower ne configure pas l'unité d'organisation Workloads pour vous.

Pour plus d'informations, voir [Organisation du démarrage de la production avec AWS Control Tower](#).

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

AWSControl 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'exemples OUs dans un environnement AWS Control Tower étendu et plat avec des instructions AWS multicomptes, voir [Exemple : charges de travail dans une structure d'unité d'organisation plate](#).
- Pour plus d'informations sur le fonctionnement AWS de Control Tower avec des structures d'unité d'organisation imbriquées, consultez [UO imbriquées dans AWS Control Tower](#).
- Pour plus d'informations sur la manière dont AWS Control Tower s'aligne sur les AWS recommandations, consultez le AWS white paper, [Organizing Your AWS Environment Using Multiple Accounts](#).

Le diagramme sur la page liée montre que davantage de fondamentaux OUs et d'autres supplémentaires OUs ont été créés. Ils OUs répondent aux besoins supplémentaires d'un déploiement de plus grande envergure.

Dans la OUs colonne Foundational, deux OUs ont été ajoutés 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 dédiée aux pare-feux.
- OU d'infrastructure — Vous souhaitez peut-être séparer l'unité d'organisation d'infrastructure, recommandée précédemment, en deux OUs, Infrastructure_Test (pour l'infrastructure de pré-production) et Infrastructure_Prod (pour l'infrastructure de production).

Dans la OUs zone supplémentaire, plusieurs autres OUs ont été ajoutés à la structure de base. Voici les prochaines recommandations OUs à créer au fur et à mesure que votre environnement se développe :

- UO des charges de travail : l'unité d'organisation des charges de travail, recommandée précédemment mais facultative, a été séparée en deux OUs, 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 et pour tous les OUs comptes de votre organisation. Conceptuellement, la racine contient tous les OUs. 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 votre OUs. Pour un schéma utile, consultez [la AWS Organizations documentation](#).

Conseils administratifs pour la configuration de la zone d'atterrissage

Voici quelques conseils pour configurer et configurer votre 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 buckets 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 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.
- AWSControl Tower prend en charge le balisage uniquement pour les commandes activées. Pour de plus amples informations, veuillez consulter [AWSControl Tower prend en charge le balisage pour les commandes activées](#).
- Nous recommandons d'activer l'authentification multifactorielle (MFA) pour chaque compte géré par AWS Control Tower.

Considérations relatives à VPCs

- La VPC version créée par AWS Control Tower est limitée à la Régions AWS version dans laquelle 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 compte Account Factory créé avec votre compte Account Factory. Ils peuvent préférer en créer un nouveau à VPC l'aide du portefeuille Service Catalog ou créer une version personnalisée VPC qui ne s'exécute que dans les régions requises.

- La valeur VPC créée par AWS Control Tower n'est pas la même que la valeur par défaut VPC créée pour tous Comptes AWS. Dans les régions où AWS Control Tower est prise en charge, AWS Control Tower supprime la valeur par défaut VPC lors de la création de la AWS Control TowerVPC.
- Si vous supprimez votre option par défaut VPC dans votre AWS région d'origine, il est préférable de la supprimer dans toutes les autres AWS régions.

Recommandations pour la configuration de groupes, de rôles et de 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, consultez [Gestion des identités et des accès dans AWS Control Tower](#).

Restrictions recommandées

Vous pouvez restreindre l'étendue de l'accès administratif à vos organisations en définissant un IAM rôle ou une politique permettant aux administrateurs de gérer uniquement les actions de la AWS Control Tower. L'approche recommandée consiste à utiliser la IAM politique `arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy`. 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 un accès à SCPs 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 `AWSecurityAuditors` 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 dans les 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 la création et la modification des ressources AWS de la 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 :

- Conservez 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 AWS Identity and Access Management (IAM) rôles 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 enregistrer ces comptes auprès de AWS Control Tower, ni enregistrer leur parent OUs immédiat.
- N'en interdisez pas l'utilisation par les Régions AWS biais de l'un SCPs ou de l'autre 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 de la 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 de

la capacité de [refus de contrôle de la région de contrôle appliquée à l'unité d'organisation](#), qui fonctionne au niveau de l'unité d'organisation pour restreindre l'accès aux régions.

- AWS Organizations FullAWSAccessSCP doit être appliqué et ne doit pas être fusionné avec un autre SCPs. Toute modification apportée à ce SCP paramètre n'est pas signalée comme une dérive ; toutefois, certaines modifications peuvent affecter AWS le fonctionnement de la Control Tower de manière imprévisible, si l'accès à certaines ressources est refusé. Par exemple, s'il 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 le 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 de la 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_DisableAWSServiceAccess dans la AWS Organizations API référence](#).
- 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 :

- AWSControl Tower permet des actions simultanées pour déployer des contrôles optionnels. Pour plus d'informations, voir [Déploiement simultané pour les contrôles facultatifs](#).
- AWSControl 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, consultez [Quels sont les comptes partagés ?](#).

Conseils sur les comptes et OUs

- Nous vous recommandons de limiter chaque unité d'organisation enregistrée à un maximum de 1 000 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 680, même si la limite est de 1 000 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 680 comptes peut avoir besoin de 2 heures pour s'enregistrer et activer les contrôles, et d'une 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 de plus amples informations, veuillez consulter [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 IAM autorisations 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 de 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

AWSControl Tower est étroitement associée à AWS Organizations. Voici quelques conseils spécifiques sur la meilleure façon de travailler ensemble pour protéger votre AWS environnement.

- 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 (SCPs) associées à une unité d'organisation enregistrée auprès AWS de 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 le modifier, vous pouvez en créer de nouveaux SCPs et les OUs joindre à ceux SCPs que AWS Control Tower a créés.

- 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. Consultez [Types de dérive de gouvernance](#).
- Si vous créez, invitez ou déplacez des comptes au sein d'une organisation enregistrée auprès de AWS Control Tower, ces comptes ne sont pas enregistrés par AWS Control Tower et ces modifications ne sont pas enregistrées. AWS Organizations Si vous devez accéder à ces comptes par le biais SSO de la section [Accès aux comptes des membres](#).
- 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.
- AWSControl 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 tous OUs dans la console AWS Control Tower, même s'ils ne sont pas autorisés à récupérer ces noms et parents directement auprès de AWS Organizations ces derniers.
- AWSControl 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 AWS de Control Tower sont censés disposer de toutes les autorisations nécessaires.
- AWS Organizations FullAWSAccessSCP doit être appliqué et ne doit pas être fusionné avec un autre SCPs. Toute modification apportée à ce SCP paramètre n'est pas signalée comme une dérive ; toutefois, certaines modifications peuvent affecter AWS le fonctionnement de la Control Tower de manière imprévisible, si l'accès à certaines ressources est refusé. Par exemple, s'il 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 le 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 de la 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_DisableAWSServiceAccess dans la AWS Organizations API référence](#).

IAMConseils relatifs au centre d'identité

AWSControl 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 configurez IAM Identity Center 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.

Note

SSOest une abréviation utilisée dans le secteur des technologies pour désigner l'authentification unique. En termes généraux, SSO il s'agit d'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 Management, et abrégé en IAMIAMIdentity Center.

Par défaut, AWS Control Tower configure AWS IAM Identity Center pour votre zone de landing zone, conformément 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. Cliquez ensuite sur 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, Control AWS Tower crée uniquement les rôles et les politiques nécessaires à la gestion de Control AWS Tower, tels que `AWSControlTowerAdmin` et `AWSControlTowerAdminPolicy`. Pour les zones d'atterrissage qui s'autogèrent, AWS Control Tower ne crée plus de IAM rôles ni de groupements destinés à un usage spécifique du 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 de 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 d'atterrissage.

- 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 AWS IAM Identity Center aux 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 de 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 de AWS Control Tower et 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 de AWS Control Tower.

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

Si vous êtes authentifié en tant qu'IAMutilisateur ou utilisateur d'IAMIdentity Center lors de la création d'un nouveau compte dans Account Factory ou lorsque vous utilisez la fonctionnalité AWS Control Tower d'inscription à un compte, 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, reportez-vous [Erreur Aucun chemin de lancement trouvé](#) à la section [Dépannage](#) du guide de l'utilisateur de AWS Control Tower.

Note

Jusqu'à cinq comptes peuvent être provisionnés à la fois.

Conseils pour s'abonner à Topics SNS

Abonnez-vous aux SNS rubriques pour obtenir des informations sur votre environnement AWS Control Tower.

- Le `aws-controltower-AllConfigNotifications` SNS sujet reçoit tous les événements publiés par AWS Config, y compris les notifications de conformité et les notifications CloudWatch d'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 `aws-controltower-AllConfigNotifications` SNS sur le sujet.

- Pour recevoir des notifications de conformité détaillées, nous vous recommandons de vous abonner à la `aws-controltower-AllConfigNotifications` SNS rubrique. 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 dans l'ensemble, nous vous recommandons de vous abonner à la `aws-controltower-AggregateSecurityNotifications` SNS rubrique.
- Pour recevoir des notifications concernant les erreurs de AWS Control Tower Account Factory for Terraform (AFT), vous pouvez vous abonner à un SNS sujet intitulé [aft_failure_notifications](#), affiché dans le AFT référentiel. Par exemple :

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

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

Pour plus d'informations sur SNS les sujets et la conformité, consultez [la section Prévention et notification](#).

Conseils pour les KMS clés

AWSControl 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 KMS clé à chaque fois que vous mettez à jour votre zone de landing zone. Comme bonne pratique, nous vous recommandons d'utiliser vos propres KMS clés et de les changer de temps à autre.

AWS KMS vous permet de créer des clés multirégionales et KMS des clés asymétriques. Cependant, AWS Control Tower ne prend pas en charge les clés multirégionales ni les clés asymétriques. AWSControl 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 de Control Tower.

Pour les clients qui exploitent un HSM cluster AWS Cloud : créez un magasin de clés personnalisé associé à votre HSM cluster Cloud. Vous pouvez ensuite créer une KMS clé, qui se trouve dans le

magasin de clés HSM personnalisé Cloud que vous avez créé. Vous pouvez ajouter cette KMS clé à AWS Control Tower.

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

Bonnes pratiques pour les mises à jour des zones d'atterrissage

Cette section présente certaines considérations et bonnes pratiques à prendre en compte lorsque vous envisagez une mise à niveau de votre version de zone d'atterrissage dans AWS Control Tower. Le passage de la série de versions de zone d'atterrissage 2.0 à la série de versions de zone d'atterrissage 3.0 est particulièrement important. Lorsque vous améliorez votre zone de landing zone, AWS Control Tower vous déplace automatiquement vers la dernière version disponible.

Note

Il est recommandé de passer à la dernière version de la zone d'atterrissage.

Résumé des meilleures pratiques expliquées dans cette section

- Bonne pratique : pour des raisons de sécurité et d'audit, nous vous recommandons vivement d'activer la journalisation à tous les niveaux, pour tous les comptes, et d'envoyer les informations de journalisation à un emplacement centralisé. Dans AWS Control Tower, cet emplacement centralisé est le compte d'archivage des journaux, qui fournit un compartiment de journalisation Amazon S3.
- Bonne pratique : si vous choisissez de ne pas suivre le CloudTrail parcours au niveau de l'organisation dans AWS Control Tower, configurez et gérez vos propres sentiers.
- Bonne pratique : Lorsque vous exploitez votre environnement AWS Control Tower, configurez un environnement de test.

Avantages du passage des versions de zone d'atterrissage 2.x aux versions de zone d'atterrissage 3.x

- Enregistrez AWS Config les ressources uniquement dans la région d'origine, ce qui permet de réaliser des économies lorsque vous gérez des ressources mondiales

- Chiffrez votre AWS CloudTrail parcours avec votre propre clé KMS
- Personnalisez le délai de conservation de vos journaux
- Contrôles obligatoires renforcés
- Nombre accru de commandes disponibles
- Intégré à AWS Security Hub
- Mises à jour du runtime Python

Mises en garde concernant le passage des versions de zone d'atterrissage 2.x aux versions de zone d'atterrissage 3.x

- Avec la landing zone 3.0 et les versions ultérieures, AWS Control Tower ne prend plus en charge les AWS CloudTrail traces de gestion au niveau du compte. AWS
- Vous avez la possibilité de choisir un sentier géré par AWS Control Tower au niveau de l'organisation ou de ne pas en faire partie et de gérer vos propres CloudTrail sentiers.
- Il existe un risque de double coût, en particulier si certains comptes au sein d'une unité d'organisation ne sont pas inscrits à AWS Control Tower et ont leurs propres traces au niveau du compte que vous souhaitez conserver.

Considérations relatives au choix des parcours au niveau de l'organisation CloudTrail

- Lorsque vous effectuez une mise à niveau vers la version 3.0 ou une version ultérieure, AWS Control Tower supprime les traces au niveau du compte créées à l'origine, au bout de 24 heures.
- Aucune donnée provenant de ces pistes n'est perdue. Vos journaux existants sont préservés même lorsque les sentiers sont supprimés.
- AWSControl Tower crée un nouveau chemin dans le même compartiment Amazon S3 pour les pistes, afin de différencier les pistes au niveau du compte des pistes au niveau de l'organisation.
 - Le chemin du journal de suivi d'un compte se présente sous la forme suivante : `/orgId/AWSLogs/...`
 - Le chemin du journal de suivi d'une organisation se présente sous la forme suivante : `/orgId/AWSLogs/orgId/...`
- CloudTrail Les pistes supplémentaires que vous avez déployées, celles qui n'ont pas été déployées par AWS Control Tower, ne sont pas touchées.

- Tous les comptes sont inclus dans le suivi au niveau de l'organisation, y compris les comptes non inscrits à AWS Control Tower, si les comptes non inscrits font partie d'une unité d'organisation enregistrée.
- CloudWatch Les alarmes Amazon dans les comptes associés ne sont pas déclenchées.
- Si vous vous désabonnez d'un suivi au niveau de l'organisation, AWS Control Tower crée toujours le journal, mais définit son statut sur Off.
- À titre de bonne pratique, si vous choisissez de ne pas suivre le parcours au niveau de l'organisation dans AWS Control Tower, vous devez créer et gérer vos propres CloudTrail sentiers,

Avantages des parcours au niveau de l'organisation

- Le suivi de l'organisation fonctionne sur tous les comptes de l'unité d'organisation.
- Les éléments enregistrés sont standardisés et ne peuvent pas être modifiés par les utilisateurs du compte.

Envisagez un environnement de test

Lorsque vous améliorez votre zone d'atterrissage, AWS Control Tower apporte des modifications uniquement aux comptes partagés et à l'unité d'organisation de base. Il n'apporte aucune modification à vos comptes de charge de travail ou OUs. Cependant, comme bonne pratique, lorsque vous exploitez votre environnement AWS Control Tower, nous vous recommandons de configurer un environnement de test. Dans l'environnement de test isolé, vous pouvez tester les mises à niveau de la zone d'atterrissage de la AWS Control Tower, ainsi que les modifications que vous pourriez apporter aux politiques de contrôle des services (SCPs), et vous pouvez tester les contrôles que vous souhaitez appliquer à l'environnement. Cette recommandation est particulièrement utile si vous opérez dans un secteur réglementé,

Services basés sur l'IA et AWS Control Tower

Vous pouvez créer des politiques de contrôle des services (SCPs) qui vous permettent de refuser que vos données soient stockées par des services basés sur l'IA sur AWS. Ces SCP politiques 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 SCP politiques de désactivation de 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'intelligence artificielle](#), 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 d'atterrissage garantit que 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 d'atterrissage de 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	2-09-2023	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 les régions que vous gérez
- Vous pouvez modifier votre politique de conservation des journaux
- Vous pouvez ajouter ou supprimer le refus de contrôle de la région
- Vous pouvez appliquer des clés AWS KMS de chiffrement
- 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 de 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 d'atterrissage. Il se peut que votre zone d'atterrissage soit dans un état indéterminé. Si tel est le cas, contactez AWS le support. Pour plus d'informations sur la résolution d'un échec de mise à jour, consultez [Impossible de mettre à jour la zone d'atterrissage](#).

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

Des mises à jour sont nécessaires pour corriger une dérive en matière de gouvernance ou pour passer à une nouvelle version de AWS Control Tower. Pour effectuer une mise à jour complète de AWS Control Tower, vous devez d'abord mettre à jour votre zone d'atterrissage, 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 les nouvelles versions de AWS Control Tower telles 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.

Mettez à jour votre zone de landing zone

Le moyen le plus simple de mettre à jour la zone d'atterrissage de votre 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 le menu de navigation de gauche du tableau de bord de la 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.

Procédure de mise à jour standard

La procédure suivante explique les étapes d'une mise à jour complète de AWS Control Tower depuis la console. Pour mettre à jour un compte individuel, consultez [Mettre à jour le compte dans la console](#).

Pour mettre à jour votre zone de landing zone, quel que soit le 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 vos comptes de membres (cette procédure doit être suivie pour une unité d'organisation contenant plus de 1 000 comptes).
4. Dans le volet de navigation de gauche, sélectionnez Organisation.
5. Pour mettre à jour chaque compte, suivez les étapes indiquées dans [Mettre à jour le compte dans la console](#).

i Réenregistrez éventuellement l'unité d'organisation pour mettre à jour les comptes

Pour les AWS Control Tower enregistrées OUs avec moins de 300 comptes, vous pouvez accéder à la page de l'unité d'organisation dans le tableau de bord et sélectionner Ré-enregistrer l'unité d'organisation pour mettre à jour les comptes de cette unité d'organisation.

Sélectionnez une version de zone d'atterrissage

Si vous utilisez la version 3.1 ou supérieure de AWS Control Tower landing zone, vous pouvez choisir de conserver la version actuelle ou de passer à une version plus récente lorsque vous effectuez une opération de mise à jour ou de réinitialisation sur les configurations de votre zone d'atterrissage. L'opération de réinitialisation est le meilleur moyen de réparer la dérive, dans la plupart des cas.

Vous pouvez choisir une version de zone d'atterrissage dans la console AWS Control Tower ou via la AWS Control Tower APIs.

i Note

Si vous choisissez de déployer une version de zone d'atterrissage qui ignore une version intermédiaire, par exemple si vous passez de la version 3.1 à la version 3.3, AWS Control Tower déploie automatiquement la version intermédiaire dans le cadre de l'opération de mise à jour.

Dans les conversations, le passage à une version plus récente est souvent considéré comme une mise à niveau, et non comme une simple mise à jour. Ces deux concepts sont distincts, car vous pouvez mettre à jour les paramètres de votre zone d'atterrissage sans passer à une nouvelle version, par exemple en modifiant les régions que vous gérez. Dans la console, le bouton Mettre à jour effectue une mise à jour sur place ou une opération de mise à niveau, en fonction de la version actuelle de votre zone d'atterrissage et de celle que vous sélectionnez pour le déploiement.

Choisissez la version de votre zone d'atterrissage — procédure sur console

1. Depuis la console AWS Control Tower, accédez à la page des paramètres de la zone d'atterrissage. Dans le tableau des zones d'atterrissage disponibles, sélectionnez la nouvelle version. N'oubliez pas que vous pouvez sélectionner les versions 3.1 ou ultérieures. Les versions antérieures à 3.1 ne sont pas compatibles avec cette fonctionnalité.
2. Lorsque vous sélectionnez une version dans le tableau, vous pouvez voir les actions disponibles. La mise à jour est disponible si votre version actuelle est antérieure à la version sélectionnée. La réinitialisation est disponible si votre version actuelle est 3.1 ou plus récente.
3. Après avoir choisi la version, sélectionnez le bouton Mettre à jour ou le bouton Réinitialiser, dans le coin supérieur droit de l'écran.
4. Vous verrez un écran de confirmation indiquant la version de la zone d'atterrissage que vous avez sélectionnée pour le déploiement. Pour continuer, choisissez Next en bas à droite. L'opération de mise à jour peut prendre quelques minutes ou plus.
5. Une fois la zone d'atterrissage mise à jour, vous devrez peut-être mettre à jour vos comptes. Le moyen le plus simple de mettre à jour votre compte est de procéder à un processus de réenregistrement de l'unité d'organisation pour chacun de vos inscritsOUs.

Mises à jour du compte, versions de la zone d'atterrissage et données de référence

AWS Les zones d'atterrissage de la Control Tower sont AWS des ressources qui correspondent à un ensemble de configurations de base. Il n'existe pas de one-to-one cartographie des versions des lignes de base et des zones d'atterrissage. Vous pouvez consulter un tableau qui montre [Compatibilité des versions de base de l'UO et de la zone d'atterrissage](#).

Lorsque vous passez à une version de référence, vous devez mettre à jour les comptes après la mise à jour de votre zone de landing zone. Par exemple, lors de la mise à niveau de la version 3.1 vers la version 3.2, vous n'avez pas besoin de mettre à jour vos comptes, car ces versions de zone d'atterrissage partagent la même base de référence.

En revanche, si vous passez de la version 3.1 à la version 3.3, vous devrez mettre à jour les comptes, car la version de base est la version 4.0, qui englobe les versions 3.2 à 3.3.

Pour plus d'informations sur la relation entre les versions de zone d'atterrissage et les lignes de base, consultez [Compatibilité des versions de base de l'UO et de la zone d'atterrissage](#).

Schémas des zones d'atterrissage

Une zone d'atterrissage est une AWS ressource créée au moyen de schémas. Chaque version de la zone de landing zone de AWS Control Tower possède un schéma unique.

Les schémas des zones d'atterrissage de AWS Control Tower, versions 3.0 et ultérieures, sont publiés dans cette section de référence afin de vous aider à choisir une version compatible.

Note

Un problème connu concernant la journalisation des accès inutiles est présent dans la version 3.0 de la zone d'atterrissage. Ce problème est résolu dans la version 3.1 de la zone d'atterrissage. Pour plus d'informations sur les modifications, consultez [AWSZone d'atterrissage de la Control Tower, version 3.1](#).

Schéma de la zone d'atterrissage 3.1

```
{
  "type": "object",
  "required": [
    "centralizedLogging",
    "organizationStructure",
    "securityRoles"
  ],
  "properties": {
    "accessManagement": {
      "$ref": "#/definitions/AccessManagement"
    },
    "centralizedLogging": {
      "$ref": "#/definitions/CentralizedLogging"
    },
    "governedRegions": {
      "type": "array",
      "items": {
        "type": "string",
        "maxLength": 24,
        "minLength": 1,
        "pattern": "^[a-z]{2}-[a-z\\-]*-[0-9]{1}$",
        "additionalProperties": false
      },
      "additionalProperties": false
    }
  }
}
```



```
    },
    "organizationStructure": {
      "$ref": "#/definitions/OrganizationStructure"
    },
  },
  "securityRoles": {
    "$ref": "#/definitions/SecurityRoles"
  }
},
"additionalProperties": false,
"definitions": {
  "AccessManagement": {
    "type": "object",
    "required": [
      "enabled"
    ],
    "properties": {
      "enabled": {
        "type": "boolean",
        "additionalProperties": false,
        "default": true
      }
    }
  },
  "additionalProperties": false
},
"CentralizedLogging": {
  "type": "object",
  "required": [
    "accountId"
  ],
  "properties": {
    "accountId": {
      "type": "string",
      "maxLength": 12,
      "minLength": 12,
      "pattern": "^\\d{12}$",
      "additionalProperties": false
    },
    "configurations": {
      "$ref": "#/definitions/LoggingConfigurations"
    },
    "enabled": {
      "type": "boolean",
      "additionalProperties": false,
      "default": true
    }
  }
}
```

```
    }
  },
  "additionalProperties": false
},
"LoggingConfigurations": {
  "type": "object",
  "properties": {
    "accessLoggingBucket": {
      "$ref": "#/definitions/S3BucketConfiguration"
    },
    "kmsKeyArn": {
      "type": "string",
      "maxLength": 2048,
      "minLength": 1,
      "additionalProperties": false
    },
    "loggingBucket": {
      "$ref": "#/definitions/S3BucketConfiguration"
    }
  },
  "additionalProperties": false
},
"OrganizationalUnit": {
  "type": "object",
  "required": [
    "name"
  ],
  "properties": {
    "name": {
      "type": "string",
      "maxLength": 120,
      "minLength": 1,
      "pattern": "^[\\s\\S]*$",
      "additionalProperties": false
    }
  },
  "additionalProperties": false
},
"OrganizationStructure": {
  "type": "object",
  "required": [
    "security"
  ],
  "properties": {
```

```

        "sandbox": {
            "$ref": "#/definitions/OrganizationalUnit"
        },
        "security": {
            "$ref": "#/definitions/OrganizationalUnit"
        }
    },
    "additionalProperties": false
},
"S3BucketConfiguration": {
    "type": "object",
    "properties": {
        "retentionDays": {
            "type": "number",
            "minimum": 1,
            "additionalProperties": false
        }
    },
    "additionalProperties": false
},
"SecurityRoles": {
    "type": "object",
    "required": [
        "accountId"
    ],
    "properties": {
        "accountId": {
            "type": "string",
            "maxLength": 12,
            "minLength": 12,
            "pattern": "^\\d{12}$",
            "additionalProperties": false
        }
    },
    "additionalProperties": false
}
}
}

```

Schéma de la zone d'atterrissage 3.2

```

{
    "type": "object",

```

```

"required": [
  "centralizedLogging",
  "organizationStructure",
  "securityRoles"
],
"properties": {
  "accessManagement": {
    "$ref": "#/definitions/AccessManagement"
  },
  "centralizedLogging": {
    "$ref": "#/definitions/CentralizedLogging"
  },
  "governedRegions": {
    "type": "array",
    "items": {
      "type": "string",
      "maxLength": 24,
      "minLength": 1,
      "pattern": "^[a-z]{2}-[a-z\\-]*-[0-9]{1}$",
      "additionalProperties": false
    },
    "additionalProperties": false
  },
  "organizationStructure": {
    "$ref": "#/definitions/OrganizationStructure"
  },
  "securityRoles": {
    "$ref": "#/definitions/SecurityRoles"
  }
},
"additionalProperties": false,
"definitions": {
  "AccessManagement": {
    "type": "object",
    "required": [
      "enabled"
    ],
    "properties": {
      "enabled": {
        "type": "boolean",
        "additionalProperties": false,
        "default": true
      }
    }
  },

```

```

    "additionalProperties": false
  },
  "CentralizedLogging": {
    "type": "object",
    "required": [
      "accountId"
    ],
    "properties": {
      "accountId": {
        "type": "string",
        "maxLength": 12,
        "minLength": 12,
        "pattern": "^\\d{12}$",
        "additionalProperties": false
      },
      "configurations": {
        "$ref": "#/definitions/LoggingConfigurations"
      },
      "enabled": {
        "type": "boolean",
        "additionalProperties": false,
        "default": true
      }
    }
  },
  "additionalProperties": false
},
"LoggingConfigurations": {
  "type": "object",
  "properties": {
    "accessLoggingBucket": {
      "$ref": "#/definitions/S3BucketConfiguration"
    },
    "kmsKeyArn": {
      "type": "string",
      "maxLength": 2048,
      "minLength": 1,
      "additionalProperties": false
    },
    "loggingBucket": {
      "$ref": "#/definitions/S3BucketConfiguration"
    }
  }
},
"additionalProperties": false
},

```

```
"OrganizationalUnit": {
  "type": "object",
  "required": [
    "name"
  ],
  "properties": {
    "name": {
      "type": "string",
      "maxLength": 120,
      "minLength": 1,
      "pattern": "^[\\s\\S]*$",
      "additionalProperties": false
    }
  },
  "additionalProperties": false
},
"OrganizationStructure": {
  "type": "object",
  "required": [
    "security"
  ],
  "properties": {
    "sandbox": {
      "$ref": "#/definitions/OrganizationalUnit"
    },
    "security": {
      "$ref": "#/definitions/OrganizationalUnit"
    }
  },
  "additionalProperties": false
},
"S3BucketConfiguration": {
  "type": "object",
  "properties": {
    "retentionDays": {
      "type": "number",
      "minimum": 1,
      "additionalProperties": false
    }
  },
  "additionalProperties": false
},
"SecurityRoles": {
  "type": "object",
```

```

    "required": [
      "accountId"
    ],
    "properties": {
      "accountId": {
        "type": "string",
        "maxLength": 12,
        "minLength": 12,
        "pattern": "^\\d{12}$",
        "additionalProperties": false
      }
    },
    "additionalProperties": false
  }
}

```

Schéma de la zone d'atterrissage 3.3

```

{
  "type": "object",
  "required": [
    "centralizedLogging",
    "organizationStructure",
    "securityRoles"
  ],
  "properties": {
    "accessManagement": {
      "$ref": "#/definitions/AccessManagement"
    },
    "centralizedLogging": {
      "$ref": "#/definitions/CentralizedLogging"
    },
    "governedRegions": {
      "type": "array",
      "items": {
        "type": "string",
        "maxLength": 24,
        "minLength": 1,
        "pattern": "^([a-z]{2}-[a-z\\-])*-[0-9]{1}$",
        "additionalProperties": false
      }
    },
    "additionalProperties": false
  }
}

```

```
    },
    "organizationStructure": {
      "$ref": "#/definitions/OrganizationStructure"
    },
  },
  "securityRoles": {
    "$ref": "#/definitions/SecurityRoles"
  }
},
"additionalProperties": false,
"definitions": {
  "AccessManagement": {
    "type": "object",
    "required": [
      "enabled"
    ],
    "properties": {
      "enabled": {
        "type": "boolean",
        "additionalProperties": false,
        "default": true
      }
    }
  },
  "additionalProperties": false
},
"CentralizedLogging": {
  "type": "object",
  "required": [
    "accountId"
  ],
  "properties": {
    "accountId": {
      "type": "string",
      "maxLength": 12,
      "minLength": 12,
      "pattern": "^\\d{12}$",
      "additionalProperties": false
    },
    "configurations": {
      "$ref": "#/definitions/LoggingConfigurations"
    },
    "enabled": {
      "type": "boolean",
      "additionalProperties": false,
      "default": true
    }
  }
}
```



```

    }
  },
  "additionalProperties": false
},
"LoggingConfigurations": {
  "type": "object",
  "properties": {
    "accessLoggingBucket": {
      "$ref": "#/definitions/S3BucketConfiguration"
    },
    "kmsKeyArn": {
      "type": "string",
      "maxLength": 2048,
      "minLength": 1,
      "additionalProperties": false
    },
    "loggingBucket": {
      "$ref": "#/definitions/S3BucketConfiguration"
    }
  },
  "additionalProperties": false
},
"OrganizationalUnit": {
  "type": "object",
  "required": [
    "name"
  ],
  "properties": {
    "name": {
      "type": "string",
      "maxLength": 120,
      "minLength": 1,
      "pattern": "^[\\s\\S]*$",
      "additionalProperties": false
    }
  },
  "additionalProperties": false
},
"OrganizationStructure": {
  "type": "object",
  "required": [
    "security"
  ],
  "properties": {

```

```
        "sandbox": {
            "$ref": "#/definitions/OrganizationalUnit"
        },
        "security": {
            "$ref": "#/definitions/OrganizationalUnit"
        }
    },
    "additionalProperties": false
},
"S3BucketConfiguration": {
    "type": "object",
    "properties": {
        "retentionDays": {
            "type": "number",
            "minimum": 1,
            "additionalProperties": false
        }
    },
    "additionalProperties": false
},
"SecurityRoles": {
    "type": "object",
    "required": [
        "accountId"
    ],
    "properties": {
        "accountId": {
            "type": "string",
            "maxLength": 12,
            "minLength": 12,
            "pattern": "^\\d{12}$",
            "additionalProperties": false
        }
    },
    "additionalProperties": false
}
}
```


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 SCPs données 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 et [Déterminez 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 intitulée Types 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 de la 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 approvisionner et personnaliser des comptes avec AWSControl Tower Account Factory for Terraform (AFT). Pour de plus amples informations, veuillez consulter [Présentation de AWS Control Tower Account Factory pour Terraform \(AFT\)](#).

- Vous pouvez mettre à jour les comptes avec Customizations for AWS Control Tower (CfCT). Pour de plus amples informations, veuillez consulter [Présentation des personnalisations pour AWS Control Tower \(CfCT\)](#).
- Automatisation des scripts : si vous préférez utiliser une API approche, vous pouvez mettre à jour les comptes à l'aide du [APIframework](#) de Service Catalog et les mettre AWS CLI à jour par lots. Vous devez appeler le [UpdateProvisionedProduct](#) API Service Catalog pour chaque compte. Vous pouvez écrire un script pour mettre à jour les comptes, un par un, avec cela 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 procédure](#) Il 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 le [UpdateProvisionedProduct](#) API au lieu du [ProvisionProduct](#) API.

Une autre étape de l'automatisation par script consiste à vérifier le statut Succeed de l'événement du [UpdateLandingZone](#) cycle de vie de la 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 :

- [AWS CloudShell À utiliser 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 supplémentaires et liens](#) 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 de 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](#).

AWS CloudShell À utiliser pour travailler avec AWS Control Tower

AWS CloudShell est un AWS service qui facilite le travail dans le AWS CLI. Il s'agit d'un shell pré-authentifié basé sur un navigateur que vous pouvez lancer directement depuis le AWS Management Console. Il 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 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

Obtenir IAM des autorisations 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 IAM utilisateurs 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 par AWS](#) est une politique autonome qui est créée et gérée par AWS. La politique AWS gérée suivante pour CloudShell peut être attachée aux IAM identités :

- `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 IAM utilisateur ou un utilisateur d'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 à l'aide de IAM politiques](#) dans le Guide de AWS CloudShell l'utilisateur.

Note

Votre IAM identité 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](#).

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.

Interagissez avec AWS Control Tower via 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.

AWS CloudShell À utiliser pour aider à 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 du centre d'IAMidentité ou IAM en tant qu'utilisateur disposant des autorisations administratives pour le compte de gestion qui contient votre zone d'atterrissage.

1. Voici comment vous pouvez utiliser AWS Config CLI les commandes 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.

Exemple : Vérifiez votre AWS Config statut

Commandes d'affichage :


- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-records`
- La réponse normale est quelque chose comme "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 :

Exemple : gestion de 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 AWS Config documentation

- [Gestion de l'enregistreur de configuration \(AWS CLI\)](#)

-

[Gestion du canal de distribution](#)

3. Cet exemple montre AWS CLI les commandes AWS CloudShell à partir desquelles vous devez entrer pour activer ou désactiver l'accès sécurisé pour 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

Exemple : activer ou désactiver l'accès aux services sécurisés

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

Exemple : créer un compartiment Amazon S3 avec AWS CloudShell

Dans l'exemple suivant, vous pouvez AWS CloudShell créer un compartiment Amazon S3, puis utiliser la PutObject méthode 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 :

```
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:wad4a567d8bfd9a1234ebee56\""
}
```

ETagIl 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](#).

Créez AWS Control Tower des 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 dans JSON ouYAML. Ces modèles décrivent les ressources que vous souhaitez mettre à disposition dans vos AWS CloudFormation piles. Si vous ne connaissez pas JSON ouYAML, 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 JSON et des YAML modèles pour ces types de ressources, consultez [AWS Control Tower](#)le guide de AWS CloudFormation l'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 voir des AWS Control Tower exemples relatifs à la console CLI et à la console, voir [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](#)
- [AWS CloudFormation API Référence](#)
- [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, consultez [Limites 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-codé de 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-sample](#) référentiel.
- Des exemples de code supplémentaires concernant CfCT sont disponibles dans le cadre de l'architecture de référence de AWS sécurité, dans le [aws-sample](#) 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)

Customizations for AWS Control Tower (CfCT) vous aide 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 (SCPs).

Cette fonctionnalité CfCT est intégrée aux événements du cycle de vie de la AWS Control Tower, afin que vos déploiements de ressources restent synchronisés avec votre zone d'atterrissage. 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 (OUs) 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 présente les considérations architecturales et les étapes de configuration pour le déploiement de Customizations for AWS Control Tower (CfCT). Il inclut un lien vers le [AWS CloudFormation](#) modèle 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](#) du référentiel. GitHub

Présentation de l'architecture

Le déploiement de CfCT crée l'environnement suivant dans le AWS cloud, avec un compartiment Amazon S3 comme source de configuration.

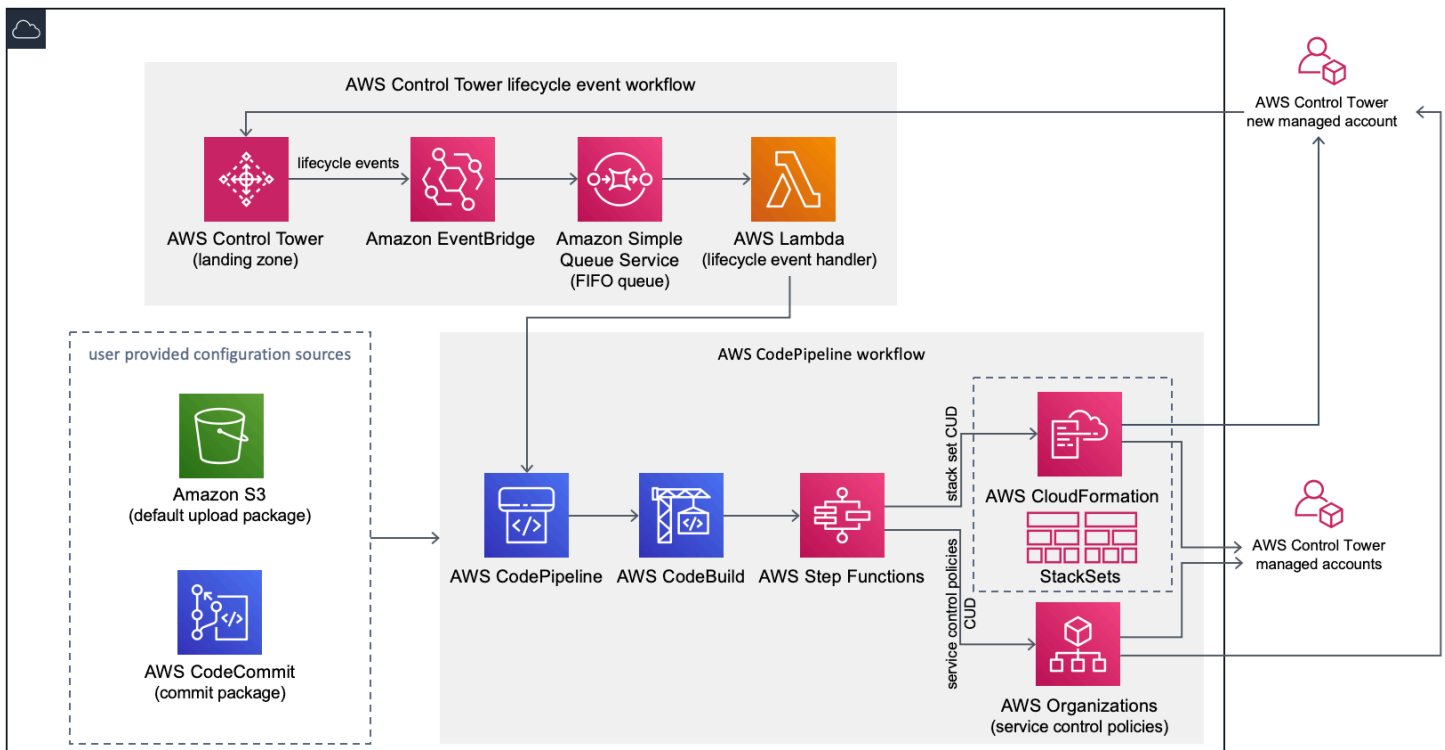


Figure 1 : Personnalisations de l'architecture AWS Control Tower

CfCT inclut un AWS CloudFormation modèle que vous pouvez déployer 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 la zone d'atterrissage de votre AWS Control Tower.

i Remarque

Le CfCT doit être déployé dans la région d'origine de la AWS Control Tower et dans le compte de gestion de la AWS Control Tower, car c'est là que votre zone d'atterrissage de la AWS Control Tower est déployée. Pour plus d'informations sur la configuration d'une zone d'atterrissage de la AWS Control Tower, reportez-vous à [Premiers 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 invoque automatiquement la machine d'état des politiques de contrôle des services (SCPs) et la machine d'[AWS CloudFormation StackSets](#) état pour les déployer SCPs au niveau de l'unité d'organisation ou pour déployer des instances de pile au niveau de l'unité d'organisation ou du compte.

i Remarque

Par défaut, CfCT crée un compartiment Amazon S3 pour stocker la source du pipeline. Si vous avez un AWS CodeCommit dépôt existant, vous pouvez le remplacer par un [CodeCommit](#)dépôt. Pour plus d'informations, consultez [Configurer Amazon S3 comme source de configuration](#).

CfCT déploie deux flux de travail :

- un [AWS CodePipeline](#)flux de travail
- et un flux de travail relatif aux événements liés au cycle de vie de la AWS Control Tower.

Le AWS CodePipeline flux de travail

Le AWS CodePipeline flux de travail configure AWS CodePipeline, [AWS CodeBuild](#)projet et [AWS Step Functions](#)orchestre la gestion de AWS CloudFormation StackSets et au sein de votre SCPs 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 AWS CodeBuild de.
- SCPÉtape — invoque la machine d'état de la politique de contrôle des services, qui appelle le AWS Organizations API pour créerSCPs.
- AWS CloudFormation Étape : invoque la machine d'état Stack Set pour déployer les ressources spécifiées dans la liste des comptes ou OUs que vous avez fournies 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 personnalisés et SCPs vers les comptes individuels ciblés, ou vers une unité organisationnelle complète.

i Remarque

Pour obtenir des informations détaillées sur la personnalisation du package de configuration, reportez-vous à [Guide de personnalisation du CfCT](#).

Le flux de travail événementiel relatif au cycle de vie de la 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' EventBridge événement [Amazon](#), une [file d'attente « premier entré, premier sorti » \(SQS\) Amazon Simple Queue Service](#) (AmazonFIFO) et une [AWS Lambda](#) fonction.

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

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) AWS CodeCommit et les ressources du référentiel 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). Reportez-vous à [Amazon S3](#) et à la [AWS CodeCommittarification](#) pour plus de détails.

Services relatifs aux composants

Les AWS services suivants font partie de Customizations for AWS Control Tower (CfCT).

AWS CodeCommit

Si vous avez un AWS CodeCommit référentiel existant, vous pouvez le configurer comme source pour votre pipeline, comme alternative à Amazon S3.

Sur la base de vos entrées dans le AWS CloudFormation modèle, CfCT peut créer un [AWS CodeCommit](#) référentiel 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](#).

Note

Si vous ne l'utilisez pas déjà CodeCommit, votre seule option est de configurer le compartiment Amazon S3 comme emplacement de stockage pour votre package de configuration. CodeCommit n'est pas disponible si vous déployez CfCT pour la première fois.

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 le contrôle de la source de configuration, 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 SQS file d'attente Amazon et des paramètres sensibles du magasin de paramètres AWS Systems 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 FIFO file d'attente ou aux SecureString valeurs du magasin de paramètres, les 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 appeler les composants de l'installation lors de l'installation et du déploiement initiaux AWS CloudFormation StackSets ou AWS Organizations SCPs lors d'un événement du cycle de vie AWS de la Control Tower.

Amazon Simple Notification Service

CfCT peut publier des notifications, telles que l'approbation du pipeline sur des sujets [Amazon Simple Notification Service](#) (AmazonSNS) 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 la zone d'atterrissage AWS de votre Control Tower. L'exemple de manifeste identifie les configurations requises pour les ensembles de piles et les politiques de contrôle des services (SCPs) 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, consultez [Guide de personnalisation du CfCT](#).

Amazon Simple Queue Service

CfCT utilise une file d'attente Amazon Simple Queue Service (AmazonSQS) FIFO pour capturer les événements du cycle de vie d'Amazon EventBridge. Il déclenche une AWS Lambda fonction, qui invoque AWS CodePipeline pour déployer AWS CloudFormation StackSets ou SCPs. Pour plus d'informations sur SCPs, voir [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 dans lesquels 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 de 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](#).

N'oubliez pas de supprimer le trait de soulignement

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

Si vous disposez d'un référentiel AWS CodeCommit Git existant, vous pouvez modifier l'emplacement de stockage du package de configuration en remplaçant le compartiment Amazon S3 par un référentiel AWS CodeCommit Git. Pour ce faire, sélectionnez l'`CodeCommit` option dans le AWS CloudFormation paramètre.

Compresser ou ne pas compresser ?

Lorsque vous utilisez le compartiment S3 par défaut, assurez-vous que le package de configuration est disponible sous forme de .zip fichier. Si vous utilisez le AWS CodeCommit référentiel, veillez à placer le package de configuration dans le référentiel sans compresser les fichiers. Pour plus d'informations sur la création et le stockage du package de configuration dans AWS CodeCommit, consultez [Guide 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.

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 de AWS Control Tower, puis 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 de la configuration de la 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 AWS de la 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 sur votre compte de gestion AWS Control Tower et dans votre AWS région d'origine. Si aucune zone d'atterrissage n'est configurée, consultez [Premiers 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.
- Vérifiez 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 présenté dans cette section déploie Customizations for 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 de landing AWS Control Tower, à savoir votre région d'origine.

3. Sur la page Créer une pile, vérifiez que le bon modèle URL apparaît dans la zone de URLtexte 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 "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.
AWS CodePipelineLa source	Amazon S3	La source pour vous aider AWS CodePipeline à sélectionner où stocker et configurer les personnalisations CfCT.

AWS CodeCommit Configuration		
Paramètre	Par défaut	Description
CodeCommitRéférentiel existant ?	No	Choisissez si vous souhaitez utiliser un dépôt CodeCommit Git existant. Si vous le souhaitezYes, vous devez définir le paramètre CodePipeline Source surAWS CodeCommit .
CodeCommit Nom du référentiel	custom-control-tower-configuration	Si vous fournissez le nom d'un dépôt Git existant, vous devez définir le CodeCommit référentiel existant ? paramètre Yes et entrez le nom exact de ce dépôt.
CodeCommit Nom de la succursale	main	Branche Git dans laquelle le package de personnalisation est stocké. Pour utiliser ce paramètre, vous devez définir le paramètre CodePipeline Source surAWS CodeCommit .

AWS CloudFormation StackSets Configuration		
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 .

AWS CloudFormation StackSets Configuration

Paramètre	Par défaut	Description
Pourcentage de tolérance aux défaillances	10	Pourcentage de comptes, par région, pour lesquels cette opération de pile peut échouer avant d'AWS CloudFormation arrêter 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 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 créera AWS Identity and Access Management (IAM) des ressources.
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 ajouter des personnalisations à votre zone d'atterrissage AWS Control Tower et à vos politiques de contrôle des services (SCPs) en personnalisant le package de configuration inclus. Pour obtenir des instructions détaillées sur la création d'un package personnalisé, reportez-vous au [Guide de personnalisation du CfCT](#).

i 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 Customizations for 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 [console AWS CloudFormation](#).
2. Sélectionnez votre CloudFormation stack Customizations for AWS Control Tower (CfCT) existant, puis sélectionnez Update.
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 Amazon S3 URL, entrez le modèle URL du modèle que vous avez précédemment chargé sur Amazon S3, puis choisissez Next. GitHub
 - c. Vérifiez que le modèle URL est correct. 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 plus de détails sur les paramètres.
6. Choisissez 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 peut créer AWS Identity and Access Management (IAM) des ressources.

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, les ALLressources 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 [console AWS 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, consultez [the 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 JSON fichiers pour décrire et implémenter les personnalisations AWS de votre environnement 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. La plupart des clients conservent cette valeur par défaut. Si vous avez un AWS CodeCommit dépôt existant, vous pouvez modifier l'emplacement de la source pour le placer AWS CodeCommit dans votre dépôt. 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 JSON les autres fichiers

- 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

N'oubliez pas le soulignement

Le nom du fichier d'exemple de package de configuration commence par un trait de soulignement (_) afin qu'il ne 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 etcfn_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 à appeler AWS Organizations APIs pour créer des politiques de contrôle des services (SCPs).

5. AWS CloudFormation étape de la ressource

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 (OUs), que vous avez fournies 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. Pour spécifier une dépendance aux ressources, organisez l'ordre dans lequel les ressources sont spécifiées dans le fichier manifeste. L'ordre des ressources dans le fichier manifeste est le seul moyen de spécifier une dépendance.

Définition d'une configuration personnalisée

Vous allez définir votre configuration AWS Control Tower personnalisée à l'aide du fichier manifeste, du jeu de modèles qui l'accompagne et d'autres JSON fichiers. 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
- politiques/                                [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 de AWS Control Tower. Cette valeur doit être un nom de AWS région valide (tel que `us-east-1`, `eu-west-1`, `ouap-southeast-1`). La région d'origine de la AWS Control Tower est la région par défaut lorsque vous créez des ressources AWS Control Tower personnalisées (telles que 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 à [Mises 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 indique le AWS CloudFormation StackSets ou AWS Organizations SCPs que CfCT déploie automatiquement via le pipeline de code. Vous pouvez créer des listes OUs, des comptes et des 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. SCPs sont déployés au niveau de l'OU. 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, un Amazon S3 URI ou s'URLil pointe vers un AWS CloudFormation modèle ou une politique de contrôle des AWS Organizations services JSON pour la création AWS CloudFormation de ressources ou. SCPs

- 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 en tant qu'Amazon S3 URI

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

3. L'exemple suivant montre le fichier de ressources fourni en tant qu'Amazon S3 HTTPS URL

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

Note

Si vous fournissez un Amazon S3URL, vérifiez que la politique du bucket autorise l'accès en lecture au compte de gestion AWS Control Tower à partir duquel vous déployez CfCT. Si vous fournissez un Amazon S3 HTTPSURL, 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 endroit où 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 le *AccountId* variable illustrée dans l'exemple avec 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 `stack_setoption` de déploiement des ressources via AWS CloudFormation StackSets, ou de `scption` si vous déployez. SCPs

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

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

 Note

Si vous souhaitez déployer une 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 `OU_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 `OU_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 touches de SSM paramètres vous permettent de stocker les sorties du modèle dans le magasin de SSM paramètres. 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 SSM paramètres et la valeur contient la value chaîne du paramètre.
- Valeurs valides : n'importe quelle 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 SSM paramètre 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 (OU) `organizational_units` dans la version V2 du manifeste (2021-03-15).

- Si vous choisissez la méthode de scp déploiement suivante : lorsque vous ajoutez Root `underorganizational_units`, AWS Control Tower applique les politiques à tous les éléments OUs Under the 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 meilleures pratiques de 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 de la Control Tower.

Conformément aux directives relatives aux meilleures pratiques, le déploiement de 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 `AWSControlTowerExecution` rôle 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 IAM les rôles 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'`organizational_units` organisation ci-dessous, n'en ajoutez aucune autre OUs.

UO imbriquée

CfCT prend en charge la liste d'un ou plusieurs éléments imbriqués OUs sous le `organizational_units` mot clé dans la version V2 du manifeste (2021-03-15).

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 deux OUs. Pour ce qui est de la méthode de déploiements `cp`, AWS Control Tower déploie l'unité SCPs d'organisation jusqu'à la dernière unité organisationnelle dans le chemin d'unité d'organisation imbriqué. Pour ce qui est de la méthode de déploiements `tack_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 ensembles SCPs to `OUname3` et `stack` uniquement sur tous les comptes situés directement sous `OUname3`.

```
---
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 de contrôle des services (SCPs) et AWS CloudFormation des ressources. Pour les ressources qui doivent être déployées, vous pouvez ajouter ou supprimer des comptes et OUs. 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 (SCPs). 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 une personnalisation SCP dans le exemple-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 un Amazon S3 URL pour le fichier de ressources et si vous utilisez des paramètres avec des paires clé/valeur.

Vous devez inclure une SCP politique dans le JSON format permettant de prendre en charge le manifeste, car le fichier manifeste fait référence au JSON fichier. Assurez-vous que les chemins des fichiers correspondent aux informations de chemin fournies dans le fichier manifeste.

- Un JSON fichier de politique contient le fichier SCPs vers lequel le déploiement doit être effectué.

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 qui a été affiché précédemment pour configurer un package de configuration. SCPs 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 ressources détails. L'ordre de ressources détermine l'ordre d'exécution pour créer des ressources 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 et les fichiers de SCP politique pris en charge qui se trouvent 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 OUs 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 SSM paramètres](#) définie dans le AWS CloudFormation modèle. À l'aide de l'assistant Alfred, vous pouvez utiliser des valeurs stockées dans le SSM Parameter Store 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: ${alfred_ssm_/stack_1/subnet/id}
  - parameter_key: AvailabilityZones # Type: CommaDelimitedList
    parameter_value:
  - "${alfred_ssm_/availability_zone_1}"
  - "${alfred_ssm_/availability_zone_2}"
```

JSONschéma du package de personnalisation

Le JSON schéma 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 le service associé. AWS APIs Le schéma du manifeste permet à un seul fichier `manifest.yaml` de gérer les ressources prises en charge (AWS CloudFormation modèles et SCPs) 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 SCPs 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 du JSON fichier de paramètres 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 VPCs](#)
- 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'à /16 à 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

AWSControl Tower utilise des IAM rôles pour aider à 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 IAM les groupes 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, voir [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, voir [Créer des rôles et attribuer des 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 \(IAMpolitiques\) pour AWS Control Tower](#) et [Politiques gérées pour AWS Control Tower](#).
- Pour plus d'informations sur AWS Control Tower et AWS Config rôles, voir [AWSControl Tower ConfigRecorderRole](#).
- Pour plus d'informations sur les rôles utilisés par AWS Control Tower pour agréger AWS Config informations relatives à vos comptes, voir [How AWS Control Tower Aggregates AWS Config règles dans les comptes](#) non gérés OUs et.
- Pour plus d'informations sur la façon de protéger vos ressources lorsque vous attribuez des rôles et des autorisations, voir [Conditions facultatives pour les relations d'approbation de vos rôles](#), Configuration [facultative AWS KMS clés](#), et [Empêchez l'usurpation d'identité entre services](#).
- Pour des informations spécifiques sur le provisionnement automatique des comptes dans AWS Control Tower avec IAM des rôles, consultez la section [Provisionnement automatique des comptes avec des IAM rôles](#).

- Pour consulter la politique qui protège AWS Config SNSsujet, voir [The AWS Config SNSpolitique thématique](#).

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 obtenir des informations générales sur IAM les rôles dans AWS, consultez [la rubrique sur IAM les rôles dans le AWS IAM Guide de l'utilisateur](#).

Rôles et création de comptes

AWSControl Tower crée le compte d'un client en appelant CreateAccount API le AWS Organizations. Quand AWS Organizations crée ce compte, elle crée un rôle au sein de ce compte, que AWS Control Tower nomme en transmettant un paramètre auAPI. Le nom du rôle est `AWSControlTowerExecution`.

AWSControl 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. AWSLes bases de référence de Control Tower sont contenues dans les rôles que vous appliquez à chaque compte inscrit.

Pour plus d'informations sur les comptes et les ressources, consultez [À propos Comptes AWS de in 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 Audit et Log Archive.

Le `AWSControlTowerExecution` rôle peut être ajouté à un compte de différentes manières, comme suit :

- Pour les comptes de l'unité d'organisation Security (parfois appelés comptes principaux), AWS Control Tower crée le rôle au moment de la configuration initiale de 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 de créer un compte individuel dans AWS Control Tower. Tout d'abord, vous devez ajouter le `AWSControlTowerExecution` rôle à ce compte. Pour savoir comment ajouter le rôle, consultez [Ajoutez manuellement le IAM rôle requis à un rôle existant](#) [Compte AWS et inscrivez-le](#).

Fonctionnement du `AWSControlTowerExecution` rôle avec OUs :

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, dans 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 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 la section [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 dans les 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 de 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'intégralité ARN de la ressource, ou si vous spécifiez plusieurs ressources, vous pouvez utiliser la `aws:SourceArn` condition avec des caractères génériques (*) pour les parties inconnues du ARN. Par exemple, `arn:aws:controltower:*:123456789012:*` fonctionne si vous ne souhaitez pas spécifier de région.

L'exemple suivant illustre l'utilisation de la `aws:SourceArn` IAM condition avec vos politiques de confiance IAM dans les rôles. Ajoutez cette condition à votre relation de confiance pour le `AWSControlTowerAdmin` rôle, car le responsable du service AWS Control Tower interagit avec celui-ci.

Comme indiqué dans l'exemple, le format de la source ARN est le 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, la source ARN désignée comme `arn:aws:controltower:us-west-2:012345678901:*` étant la seule ARN autorisée 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 de plus amples informations, veuillez consulter [Empêchez l'usurpation d'identité entre services](#).

Pour des informations générales sur les politiques d'autorisation dans AWS Control Tower, voir [Gérez 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 AWS services. Pour plus d'informations, consultez l'exemple de `AWSControlTowerAdmin`, présenté précédemment dans cette section. Pour AWS Config rôle d'enregistreur, nous vous recommandons d'ajouter la `aws:SourceArn` condition, en spécifiant l'enregistreur Config ARN comme source autoriséeARN.

Pour les rôles tels que `AWSControlTowerExecution` les [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 dans le bon sens 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 AWS de Control Tower soit réinitialisé dans certaines circonstances. Il est recommandé de vérifier régulièrement les rôles, si vous les avez personnalisés.

Comment AWS Control Tower agrège AWS Config règles relatives aux comptes non gérés OUs

Le compte de gestion AWS Control Tower crée un agrégateur au niveau de l'organisation, qui aide à détecter les éléments externes AWS Config règles, afin que AWS Control Tower n'ait pas besoin d'accéder à des comptes non gérés. La console AWS Control Tower vous indique le nombre de créations externes AWS Config règles que vous avez 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 `avecconfig.amazonaws.com`.

Voici la IAM politique (JSONartefact) associée 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 gérée `AWSControlTowerServiceRolePolicy`, qui est utilisée par le `AWSControlTowerAdmin` rôle lorsqu'il crée le 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 UO. 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 AWS Config console où vous pouvez consulter les détails de chaque règle externe de votre compte. Utilisez les informations contenues dans AWS Config console et console AWS Control Tower pour déterminer si les commandes appropriées sont activées pour le compte.

Rôles programmatiques et relations de confiance pour le compte d'audit AWS de la 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 accordés à AWS Fonctions Lambda uniquement. 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.

La pile AWS Control Tower `StackSet-AWSControlTowerBP-BASELINE-ROLES` crée ces IAM rôles inter-comptes uniquement programmatiques dans le compte d'audit :

- `aws-control tower- AdministratorExecutionRole`
- `aws-control tower- ReadOnlyExecutionRole`

La pile AWS Control Tower `StackSet-AWSControlTowerSecurityResources` crée ces IAM rôles inter-comptes uniquement programmatiques dans le compte d'audit :

- `aws-control tower- AuditAdministratorRole`
- `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 `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 assumé par AWS Service Lambda uniquement
- 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`— AWS politique 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 `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 assumé par AWS Service Lambda uniquement
- 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`— AWS politique 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"
    }
  ]
}
```

Approvisionnement automatique 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 `AWSControlTowerExecution` rôle](#) 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 ce travail 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:ProvisionApplicationInstanceForAWSAccount`, `sso:ProvisionApplicationProfileForA` et `sso:ProvisionSAMLProvide` sont requises par AWS Control Tower Account Factory pour interagir avec AWS IAM Centre d'identité.

Ressources de AWS Control Tower

- Pour des informations générales sur la propriété des ressources dans AWS Control Tower, consultez [Présentation de la gestion des autorisations d'accès aux ressources AWS de votre Control Tower](#).
- Pour plus d'informations sur les ressources créées par AWS Control Tower dans les comptes partagés, consultez [À propos des comptes partagés](#).
- Pour plus d'informations sur les ressources créées par AWS Control Tower lorsqu'elle approvisionne un compte via Account Factory, consultez [Considérations relatives aux ressources pour Account Factory](#).
- Pour obtenir des informations détaillées sur les types de AWS ressources définis par AWS Control Tower et destinés à être utilisés avec [la AWS Control Tower APIs](#), reportez-vous à la [référence des types de ressources AWS Control Tower](#) dans le guide de AWS CloudFormation l'utilisateur.

Comment AWS les régions travaillent avec AWS Control Tower

AWSControl Tower est actuellement prise 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 (UAE)
- 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 OUs 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 compatible. Pour plus d'informations sur le comportement des commandes lorsque vous activez AWS Control Tower dans une nouvelle région, consultez [Configurez les régions AWS de votre Control Tower](#).

Configurez les régions AWS de votre Control Tower

Cette section décrit le comportement auquel vous pouvez vous attendre lorsque vous étendez la zone d'atterrissage de votre AWS Control Tower dans une nouvelle AWS région ou que vous supprimez une région de la configuration de votre zone d'atterrissage. Généralement, cette action est effectuée via la fonction Update de la console AWS Control Tower.

Note

Nous vous recommandons d'éviter d'étendre la zone d'atterrissage de votre AWS Control Tower à AWS des 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 de 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 de vos unités organisationnelles (OUs) gérés par AWS Control Tower ne sont pas mis à jour dans le cadre de ce processus de mise à jour de la zone d'atterrissage. Par conséquent, vous devez mettre à jour vos comptes en réenregistrant votre OUs.

Lorsque vous configurez les régions de votre 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 de AWS Control Tower.

Lorsque vous configurez votre zone d'atterrissage pour de nouvelles régions, les commandes de détection de AWS Control Tower respectent les règles suivantes :

- Le comportement reste le même pour les éléments existants. Les comportements de contrôle, qu'ils soient détectifs ou préventifs, restent inchangés pour les comptes existants OUs, dans les régions existantes.
- Vous ne pouvez pas appliquer de nouveaux contrôles de détection à OUs des comptes contenant existants qui ne sont pas mis à jour. Lorsque vous avez configuré votre zone d'atterrissage de AWS Control Tower dans une nouvelle région (en mettant à jour votre zone d'atterrissage), vous devez mettre à jour les comptes existants OUs avant de pouvoir activer de nouveaux contrôles de détection sur ces derniers OUs et sur les 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 la zone d'atterrissage de votre 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.

Configurer les régions AWS de 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 de 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-la OUs pour mettre à jour les comptes dans vos nouvelles régions. Pour de plus amples informations, veuillez consulter [Quand mettre à jour AWS Control Tower OUs et ses comptes](#).

[Une autre méthode pour approvisionner ou mettre à jour des comptes individuels après avoir configuré de nouvelles régions consiste à utiliser le API framework de Service Catalog et AWS CLI à mettre à jour les comptes par lots.](#) Pour de plus amples informations, veuillez consulter [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 de la AWS Control Tower à une nouvelle Région AWS entité et après avoir supprimé la gouvernance de la 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 une fois que AWS Control Tower a étendu la gouvernance à une nouvelle Région AWS entité ou 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 d'atterrissage. 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 EnregistréOUs, pour les comptes qui ne sont pas encore mis à jour.

Note

AWSControl 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 systématiquement 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, l'EnableControlAPIopération sur l'unité d'organisation échoue pour les contrôles détectifs et proactifs. Vous recevrez un message d'FAILED_TO_ENABLEerreur, 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 relevant du Security Hub Service Managed Standard : AWS Control Tower ne peuvent pas signaler de conformité avec précision dans les régions où il existe un décalage entre la configuration de la zone d'atterrissage et les comptes qui ne sont pas mis à jour.
- La gouvernance mixte ne modifie pas le comportement des contrôles SCP basés (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, s'ils OUs ont moins de 1 000 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 de IAM données par le biais de comptes actifs dans les régions optionnelles. Toutes les données gérées par le biais du IAM service 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 opt-in 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 (UAE), 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

AWSCertaines commandes de Control Tower fonctionnent différemment dans les régions optionnelles par rapport aux régions commerciales. Pour de plus amples informations, veuillez consulter [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. AWSControl 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 SDK
- Lorsque AWS Control Tower étend la gouvernance à une région optionnelle, elle active (opts-in) la région dans tous les comptes membres. Lorsque vous retirez 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 AWS console de facturation ou. AWS SDK 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 d'atterrissage est mise hors service, AWS Control Tower nettoie les ressources de 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 accédez au service AWS Control Tower depuis la AWS console d'une autre région, la console ne vous redirige pas automatiquement vers la région d'origine.

- Le sous-jacent API comporte des limites de capacité, qui peuvent faire passer 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 pour la gouvernance et les comptes

- Si 16 régions commerciales ou plus dans lesquelles AWS Control Tower est disponible sont régies, y compris les régions optionnelles, la limite supérieure du nombre de comptes par unité organisationnelle (UO) est réduite lors de l'enregistrement d'une UO. Pour plus d'informations, consultez la section [Limitations basées sur les AWS services sous-jacents](#).

Configurer le contrôle de refus des régions

AWSControl 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 éléments spécifiques OUs 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](#).

Considérations relatives à la région : refus de contrôler la zone d'atterrissage

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 tous les inscrits OUs.
- Ce contrôle ne peut pas être configuré pour un individu OUs.

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.

Lorsque vous activez le contrôle, il s'applique à tous les niveaux supérieurs OUs enregistrés de votre hiérarchie, et il est hérité par le niveau OUs inférieur de la chaîne. Lorsque vous supprimez le contrôle, il est supprimé pour toutes les régions enregistrées OUs, toutes les régions non gouvernées de AWS Control Tower conservent le statut Non gouvernées et vous pouvez déployer des ressources dans des régions où la AWS Control Tower n'est pas disponible.

Exceptions

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](#).

- Nom du contrôle complet : refuser l'accès AWS en fonction de la AWS région demandée
- Description du contrôle : 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 de refus de contrôle de la région SCP, voir [Refuser l'accès en AWS fonction de ce qui est demandé Région AWS](#) dans la référence AWS Control Tower Control. La AWS Control Tower SCP est similaire à [SCP la forme AWS Organizations](#), mais 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'OU

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](#).

Vous pouvez également consulter [Configurer le contrôle des refus par région](#).

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 AWS Control Tower.

Il inclut également un aperçu 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, consultez [À propos Comptes AWS de in AWS Control Tower](#). Pour plus d'informations sur l'inscription de plusieurs comptes dans AWS Control Tower, consultez [Enregistrer une unité organisationnelle existante auprès AWS de 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 d'approvisionnement

AWSControl 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 d'atterrissage 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 approvisionner des comptes de base en vous basant sur les paramètres par défaut de AWS Control Tower. Vous pouvez également créer des comptes personnalisés répondant aux exigences des cas d'utilisation spécialisés.

Account Factory Customization (AFC) permet de configurer des comptes personnalisés depuis 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 de plus amples informations, veuillez consulter [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 fonction « Enroll account » AWS de Control Tower, si votre zone d'atterrissage n'est pas en état de dérive. Consultez [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 en même temps.

Méthodes automatisées :

- Code Lambda : depuis le compte de gestion de votre zone d'atterrissage AWS Control Tower, en utilisant le code Lambda et les rôles appropriés. IAM Consultez la section [Approvisionnement automatique des comptes avec des IAM rôles](#).
- Terraform : De la AWS Control Tower Account Factory pour Terraform (AFT), qui s'appuie sur Account Factory et un GitOps modèle permettant d'automatiser le provisionnement et la mise à jour des comptes. Consultez [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 provisionnement futur 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 approvisionnés par une interaction entre AWS Control Tower, AWS Organizations, et AWS Service Catalog. Pour connaître les étapes à suivre pour inscrire une personne existante Compte AWS à l'aide de la console AWS Control Tower, reportez-vous [Inscrire un compte existant](#) à.

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 le Service Catalog ProvisionProductAPI.
2. AWS Service Catalog appelle AWS Control Tower.
3. AWSControl Tower lance un flux de travail qui, dans un premier temps, appelle le AWS Organizations CreateAccountAPI.
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 provisionnement 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 depuis la console AWS Control Tower avec Account Factory, vous devez être connecté à un compte 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. IAM

Pour des informations générales sur les autorisations requises dans AWS Control Tower, consultez [Utilisation 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](#)

À propos Comptes AWS de in AWS Control Tower

Un Compte AWS est le conteneur pour toutes vos propres ressources. Ces ressources incluent les AWS Identity and Access Management (IAM) identités acceptées par le compte, qui déterminent qui a accès à ce compte. IAM les identités peuvent inclure des utilisateurs, des groupes, des rôles, etc. Pour plus d'informations sur l'utilisation 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

Lorsque AWS Control Tower crée ou inscrit un compte, elle déploie la configuration de ressources minimale nécessaire pour le compte, y compris des ressources sous forme de [modèles Account Factory](#) et d'autres ressources dans votre zone de landing zone. Ces ressources peuvent inclure IAM des rôles, des AWS CloudTrail pistes, des [produits fournis par Service Catalog](#) et des utilisateurs

IAM d'Identity Center. AWSControl 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.

AWSControl 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, consultez [Conseils pour la création et la modification des ressources AWS de la Control Tower](#).

Considérations relatives à l'ajout de comptes de sécurité ou de journalisation existants

Avant d'accepter un Compte AWS compte de sécurité ou de connexion, AWS Control Tower vérifie si le compte contient des ressources qui ne répondent pas aux exigences AWS de Control Tower. Par exemple, vous pouvez avoir un bucket de journalisation portant le même nom que celui requis par AWS Control Tower. AWSControl 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 que AWS Control Tower est autorisée à fournir des ressources au sein du compte.

AWSControl 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 tous les comptes OUs et comptes de votre organisation, quel que soit l'unité organisationnelle ou le statut d'inscription dans AWS Control Tower. Vous pouvez consulter et inscrire les comptes des 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 géré 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 de plus amples informations, veuillez consulter [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 que AWS Control Tower crée dans les comptes partagés lorsque vous configurez votre zone de landing zone.

Pour plus d'informations sur les ressources relatives aux comptes de membres, consultez [Considérations 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.


AWSservice	Type de ressource	Nom de la ressource
AWS Organizations	Comptes	audit

AWSservice	Type de ressource	Nom de la ressource
		log archive
AWS Organizations	OUs	Security Sandbox
AWS Organizations	Politiques de contrôle de service	aws-guardrails-*
AWS CloudFormation	Piles	AWSControlTowerBP-BASELINE-CLOUDTRAIL-MASTER AWSControlTowerBP-BASELINE-CONFIG-MASTER(dans les versions 2.6 et ultérieures)

AWSservice	Type de ressource	Nom de la ressource
AWS CloudFormation	StackSets	<p>AWSControlTowerBP-BASELINE-CLOUDTRAIL(Non déployé dans la version 3.0 et versions ultérieures)</p> <p>AWSControlTowerBP_BASELINE_SERVICE_LINKED_ROLE (Deployed in 3.2 and later)</p> <p>AWSControlTowerBP-BASELINE-CLOUDWATCH</p> <p>AWSControlTowerBP-BASELINE-CONFIG</p> <p>AWSControlTowerBP-BASELINE-ROLES</p> <p>AWSControlTowerBP-BASELINE-SERVICE-ROLES</p> <p>AWSControlTowerBP-SECURITY-TOPICS</p> <p>AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED</p> <p>AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED</p> <p>AWSControlTowerLoggingResources</p>

AWSservice	Type de ressource	Nom de la ressource
		AWSControlTowerSecurityResources AWSControlTowerExecutionRole
AWS Service Catalog	Produit (langue française non garantie)	AWSControl 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
AWS Identity and Access Management	Rôles	AWSControlTowerAdmin AWSControlTowerStackSetRole AWSControlTowerCloudTrailRolePolicy
AWS Identity and Access Management	Politiques	AWSControlTowerServiceRolePolicy AWSControlTowerAdminPolicy AWSControlTowerCloudTrailRolePolicy AWSControlTowerStackSetRolePolicy

AWSservice	Type de ressource	Nom de la ressource
AWS IAM Identity Center	Groupes d'annuaires	AWSAccountFactory
		AWSAuditAccountAdmins
		AWSControlTowerAdmins
		AWSLogArchiveAdmins
		AWSLogArchiveViewers
		AWSSecurityAuditors
		AWSSecurityAuditPowerUsers
		AWSServiceCatalogAdmins
AWS IAM Identity Center	Jeux d'autorisations	AWSAdministratorAccess
		AWSPowerUserAccess
		AWSServiceCatalogAdminFullAccess
		AWSServiceCatalogEndpointUserAccess
		AWSReadOnlyAccess
		AWSOrganizationsFullAccess

 Note

AWS CloudFormation StackSet BP_BASELINE_CLOUDTRAILII 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.

AWSservice	Type de ressource	Nom de la ressource
AWS CloudFormation	Piles	StackSet-AWSContro ITowerGuardrailAWS-GR- AUDIT-BUCKET-PUBLIC- READ-PROHIBITED-
		StackSet-AWSContro ITowerGuardrailAWS-GR- AUDIT-BUCKET-PUBLIC-WRI TE-PROHIBITED
		StackSet-AWSContro ITowerBP-BASELINE- CLOUDWATCH-
		StackSet-AWSContro ITowerBP-BASELINE- CONFIG-
		StackSet-AWSContro ITowerBP-BASELINE- CLOUDTRAIL-
		StackSet-AWSContro ITowerBP-BASELINE- SERVICE-ROLES-
		StackSet-AWSContro ITowerBP-BASELINE- SERVICE-LINKED-ROLE-(In 3.2 and later)

AWSservice	Type de ressource	Nom de la ressource
		StackSet-AWSContro ITowerBP-BASELINE-ROLES-
		StackSet-AWSContro ITowerLoggingResources-
AWS Config	AWS Config Rules	AWSControlTower_AW S-GR_AUDIT_BUCKET_ PUBLIC_READ_PROHIBITED AWSControlTower_AW S-GR_AUDIT_BUCKET_ PUBLIC_WRITE_PROHIBIT
AWS CloudTrail	Journaux de suivi	aws-controltower-BaselineCl oudTrail
Amazon CloudWatch	CloudWatch Règles de l'événement	aws-controltower-ConfigComp lianceChangeEventRule
Amazon CloudWatch	CloudWatch Journaux	/aws/lambda/aws-controltowe r-NotificationForwarder

AWSservice	Type de ressource	Nom de la ressource
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
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.

AWSservice	Type de ressource	Nom de la ressource
AWS CloudFormation	Piles	StackSet-AWSContro ITowerGuardrailAWS-GR- AUDIT-BUCKET-PUBLIC- READ-PROHIBITED-
		StackSet-AWSContro ITowerGuardrailAWS-GR- AUDIT-BUCKET-PUBLIC-WRI TE-PROHIBITED-
		StackSet-AWSContro ITowerBP-BASELINE- CLOUDWATCH-
		StackSet-AWSContro ITowerBP-BASELINE- CONFIG-
		StackSet-AWSContro ITowerBP-BASELINE- CLOUDTRAIL-
		StackSet-AWSContro ITowerBP-BASELINE- SERVICE-ROLES-
		StackSet-AWSContro ITowerBP-BASELINE- SERVICE-LINKED-ROLE-(In 3.2 and later)

AWSservice	Type de ressource	Nom de la ressource
		StackSet-AWSContro ITowerBP-SECURITY- TOPICS- StackSet-AWSContro ITowerBP-BASELINE-ROLES- StackSet-AWSContro ITowerSecurityResources-*
AWS Config	Agrégateur	aws-controltower-Guardrails ComplianceAggregator
AWS Config	AWS Config Rules	AWSControlTower_AW S-GR_AUDIT_BUCKET_ PUBLIC_READ_PROHIBITED AWSControlTower_AW S-GR_AUDIT_BUCKET_ PUBLIC_WRITE_PROHI BITED
AWS CloudTrail	Journal d'activité	aws-controltower-BaselineCl oudTrail
Amazon CloudWatch	CloudWatch Règles de l'événement	aws-controltower-ConfigComp lianceChangeEventRule
Amazon CloudWatch	CloudWatch Journaux	/aws/lambda/aws-controltowe r-NotificationForwarder

AWSservice	Type de ressource	Nom de la ressource
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
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, voir [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 d'atterrissage. 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, consultez [Ressources 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'IAMutilisateur ou l'utilisateur IAM administrateur 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 IAM administrateur pour ce compte.

Pour plus d'informations sur les rôles et les ressources disponibles dans le compte de gestion, consultez [Ressources 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 pour 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 les versions 3.3 et ultérieures de AWS Control Tower landing zone, les comptes doivent remplir une `aws:SourceOrgID` condition pour toute autorisation d'écriture sur votre compartiment d'audit. Cette condition garantit que CloudTrail seuls les comptes de votre organisation peuvent écrire des journaux dans votre compartiment S3 ; elle empêche les CloudTrail journaux extérieurs à votre organisation d'écrire dans votre compartiment AWS Control Tower S3. Pour de plus amples informations, veuillez consulter [AWSZone d'atterrissage de la 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 (AmazonSNS). 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 OUs, utilisateurs et SCPs dans votre zone de landing zone. Pour plus d'informations sur la dérive, voir [Déterminez 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 SNS rubrique Amazon 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, consultez [Ressources du compte d'audit](#).

Pour plus d'informations sur l'audit programmatique, voir [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 envoyé par 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 IAM d'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 de 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 à AWS Control Tower ou désenregistrés. Les contrôles s'appliquent différemment aux comptes inscrits et non inscrits, et des contrôles peuvent s'appliquer aux comptes imbriqués en OUs fonction 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 de la AWS Control Tower à un individu, existant Compte AWS lorsque vous l'inscrivez dans une unité organisationnelle (UO) déjà gouvernée par AWS Control Tower. Les comptes éligibles existent dans des comptes non enregistrés OUs qui font partie de la même AWS Organizations organisation que la AWS Control Tower OU.

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 gérer 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. AWSControl 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 et AWS CloudFormation StackSets, voir [AWS CloudFormation StackSets et 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 tout SCPs ce qui est appliqué dans l'unité d'organisation actuelle, afin que votre posture de sécurité reste cohérente.
- Applique les contrôles obligatoires au compte au moyen de ceux SCPs 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 AWS contrôles de détective de la 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 créez un compte dans AWS Control Tower, celui-ci est régi par l'historique AWS CloudTrail de la nouvelle organisation. Si vous avez déjà déployé un CloudTrail trail, vous risquez de voir des frais dupliqués, sauf si vous supprimez le trail existant pour le compte avant de l'inscrire à 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 souhaitez peut-être supprimer toute trace restante 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 VPCs

AWSControl Tower se comporte VPCs différemment lorsque vous créez un nouveau compte dans Account Factory et lorsque vous enregistrez un compte existant.

- Lorsque vous créez un nouveau compte, AWS Control Tower supprime automatiquement le compte AWS par défaut VPC et en crée un nouveau VPC pour ce compte.
- Lorsque vous enregistrez un compte existant, AWS Control Tower n'en crée pas de nouveau VPC pour ce compte.
- Lorsque vous enregistrez un compte existant, AWS Control Tower ne supprime aucun compte existant VPC ou AWS par défaut VPC associé au compte.

Tip

Vous pouvez modifier le comportement par défaut des nouveaux comptes en configurant Account Factory, afin qu'il n'en configure pas VPC par défaut pour les comptes de votre organisation sous AWS Control Tower. Pour de plus amples informations, veuillez consulter [Créer un compte dans AWS Control Tower sans VPC](#).

Conditions préalables à l'inscription

Les conditions 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 la section [Créer 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 par le biais du formulaire « 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 de 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 de Control Tower. Le compte existant ne peut être inscrit que dans la même organisation que le compte de gestion de AWS Control Tower, dans une unité d'organisation déjà enregistrée auprès de 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 l'historique AWS CloudTrail de l'organisation AWS Control Tower. Si vous avez déjà déployé un CloudTrail trail, vous risquez de voir des frais dupliqués, sauf si vous supprimez le trail existant pour le compte avant de l'inscrire à AWS Control Tower.

Inscrire un compte existant

La fonction d'inscription du compte est disponible dans la console AWS Control Tower, permettant d'inscrire les utilisateurs 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 la fabrique 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 AWS de la 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, voir [Ajoutez manuellement le IAM rôle 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.
- AWSControl Tower entame 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.
- Il se peut que votre IAM principal ne dispose pas des autorisations nécessaires pour créer 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 obtenir des instructions sur la façon d'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 [Interagissez avec AWS Control Tower via AWS CloudShell](#).

- Si le compte appartient à une autre unité d'organisation dotée d'un compte de gestion, y compris une autre AWS unité organisationnelle de 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 unités d'organisation de votre destination SCPs ne vous permettent pas de créer toutes les ressources requises pour ce compte. Par exemple, une unité SCP d'organisation de votre 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 OUs n'est concerné 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 meilleures 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 certaines commandes de la AWS Control Tower. Pour déterminer dans quelle mesure l'inscription à AWS Control Tower peut affecter vos comptes, consultez [Étendre la gouvernance de 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 créer une zone d'atterrissage pour la 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 se trouvent dans un espace OUs enregistré 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.

Si le compte ne répond pas aux prérequis

N'oubliez pas que, comme condition préalable, les comptes éligibles à l'adhésion à la gouvernance de 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 que AWS Control Tower.

Étapes préparatoires pour ouvrir un compte dans la même organisation que 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 dans la même organisation que AWS Control Tower. et établit SCPs et consolide la facturation.

i 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 la valeur par défaut `VPC`. (Cette partie est facultative. AWS Control Tower ne modifie pas votre valeur par défaut existante `VPC`.)
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 AWS Config CLI commandes pour l'état des ressources](#) et [Inscrire des comptes disposant de ressources existantes AWS Config](#)

Une fois ces étapes préparatoires terminées, vous pouvez enregistrer le compte dans AWS Control Tower. Pour de plus amples informations, veuillez consulter [Étapes pour créer un compte](#). Cette étape place le compte dans la gouvernance complète AWS de 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 approvisionné de 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 indiquées [Désinscrire 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 AWS Config CLI commandes pour l'état des ressources

Voici quelques exemples de AWS Config CLI commandes 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 IAM rôle requis à un rôle existant Compte AWS et inscrivez-le

Si vous avez déjà configuré la zone d'atterrissage de votre AWS Control Tower, vous pouvez commencer à inscrire les comptes de votre organisation dans une unité d'organisation enregistrée auprès de AWS Control Tower. Si vous n'avez pas configuré votre zone d'atterrissage, suivez les étapes décrites dans le guide de l'utilisateur de 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 de 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 AWS de 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 IAM rôle multicompte 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 l'identifiant du compte que vous avez copié.
 - Sous Rôle, entrez le nom du IAM rôle 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 *ID du compte de gestion* avec 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 de 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 article 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 YAML modèle 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, consultez [Exemples de AWS Config CLI commandes 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

Réviser le AWS CloudFormation modèle de manière à ce que le IncludeGlobalResourcesTypesparamètre ait la valeur voulue dans votre région d'origineGLOBAL_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 de AWS Control Tower avec Account Factory.

Autorisations pour configurer et approvisionner des comptes

La 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 IAM d'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 approvisionner des comptes par programme, avec 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, consultez [Personnalisez les comptes avec Account Factory Customization \(AFC\)](#).

Pour approvisionner des comptes individuellement dans Account Factory, en tant qu'utilisateur

1. Connectez-vous depuis votre portail utilisateur URL.
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 AWSControl Tower Account Factory, puis cliquez sur le bouton Launch product. Cette action lance l'assistant pour le provisionnement d'un nouveau compte.
9. Renseignez les informations et gardez à l'esprit les points suivants :


- Il SSOUserEmail peut s'agir d'une nouvelle adresse e-mail ou de l'adresse e-mail associée à un utilisateur existant de IAM Identity Center. Quel que soit votre choix, cet utilisateur aura un accès administratif au compte que vous mettez en service.
 - AccountEmail 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 SSOUserEmail, 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, désinscrire et fermer les comptes que vous avez créés et approvisionnés 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 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 est d'utiliser la console AWS Control Tower. Les mises à jour de compte individuelles sont utiles pour résoudre les problèmes de dérive, tels que [Déplacement 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 OUs

Lorsque vous déplacez un compte entre les deux OUs, les commandes de l'unité d'organisation de destination sont appliquées au compte. Toutefois, les contrôles appliqués au compte depuis l'ancienne unité d'organisation ne sont pas supprimés. Le comportement exact des commandes est spécifique à la mise en œuvre des 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 SCPs : Les contrôles SCP basés sur l'unité d'organisation précédente sont supprimés. Les contrôles SCP basés sur l'unité d'organisation 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 supprimées 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 comptes OUs et, 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, en tant qu'utilisateur d'IAMIdentity Center dans un AWSAccountFactory ou AWSServiceCatalogAdmins plusieurs 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 redirigé 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 :
 - SSOUserEmail(Disponible dans les détails du produit approvisionné)

- AccountEmail(Disponible dans les détails du produit approvisionné)
 - SSOUserFirstName(Disponible dans IAM Identity Center)
 - SSOUserLastName(Disponible dans IAM Identity Center)
 - AccountName(Disponible dans IAM Identity Center)
- 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 cloud central 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.

Vous pouvez également mettre à jour l'adresse e-mail d'un compte Account Factory ou d'un autre compte membre depuis la AWS Organizations console sans vous connecter en tant qu'utilisateur root. Pour plus d'informations, consultez [la section Mise à jour de l'adresse e-mail de l'utilisateur root pour un compte de membre AWS Organizations](#) 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. AWSControl 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 voir la liste des unités organisationnelles (OUs) et leur statut dans la liste d'autorisation. Par défaut, tous OUs figurent sur la liste des comptes autorisés, ce qui signifie que les comptes peuvent être provisionnés en vertu de ces listes. Vous pouvez désactiver certains OUs pour le provisionnement du compte via AWS Service Catalog.

Vous pouvez consulter les options VPC de configuration Amazon disponibles pour vos utilisateurs finaux lorsqu'ils fournissent de nouveaux comptes.

Pour configurer les VPC paramètres Amazon dans Account Factory

1. En tant qu'administrateur cloud central, 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 VPC de configuration 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 AmazonVPC. Par défaut, le sous-réseau est accessible sur Internet.

Note

Si vous définissez la VPC configuration d'usine du compte de telle sorte que les sous-réseaux publics soient activés lors de la mise en service d'un nouveau compte, Account Factory configure VPC Amazon pour créer NAT une passerelle. Votre utilisation vous sera facturée par AmazonVPC. Consultez la section [VPCTarifcation](#) pour plus d'informations.

- Choisissez le nombre maximum de sous-réseaux privés dans Amazon dans VPC 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 IP pour créer votre compteVPCs. La valeur doit prendre la forme d'un bloc de routage inter-domaines (CIDR) sans classe (par exemple, la valeur par défaut est 172.31.0.0/16). Ce CIDR bloc fournit la gamme globale d'adresses IP de sous-réseau pour VPC celles créées par Account Factory pour votre compte. Au sein de votreVPC, les sous-réseaux sont attribués automatiquement à partir de la plage que vous spécifiez, et ils sont de taille égale. Par défaut, les sous-réseaux de votre site VPC ne se chevauchent pas. Cependant, les plages d'adresses IP de sous-réseau VPCs de tous vos comptes provisionnés peuvent se chevaucher.
- Choisissez une région ou toutes les régions pour créer un compte VPC lorsqu'un compte est approvisionné. Par défaut, toutes les régions disponibles sont sélectionnées.
- Dans la liste, choisissez le nombre de zones de disponibilité pour lesquelles configurer des sous-réseaux dans chacune VPC d'elles. Le nombre par défaut et recommandé est de trois.
- Choisissez Save (Enregistrer).

Vous pouvez configurer ces options de configuration pour créer de nouveaux comptes qui n'incluent pas unVPC. Consultez la [procédure](#).

Désinscrire 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 désinscrire le compte depuis la console AWS Control Tower.


Lorsque vous désinscrivez un compte AWS Control Tower, toutes les ressources fournies par AWS Control Tower sont supprimées, y compris les plans. Le compte est déplacé de n'importe quelle AWS

unité d'organisation de Control Tower vers la zone racine. Le compte ne fait plus partie d'une unité d'organisation enregistrée et n'est plus soumis à AWS Control Tower SCPs. Vous pouvez fermer le compte via AWS Organizations.

La désinscription d'un compte peut également être effectuée dans la console Service Catalog par un utilisateur d'IAM Identity Center du AWS Account Factory groupe, en mettant fin au produit provisionné. Pour plus d'informations sur les utilisateurs ou les groupes IAM d'Identity Center, voir [Gérer les utilisateurs et l'accès via AWS IAM Identity Center](#). La procédure suivante décrit comment désinscrire un compte membre dans Service Catalog.

Pour désinscrire un compte enregistré

1. Ouvrez la console Service Catalog dans votre navigateur Web à l'adresse <https://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 AWS Control Tower ne doit plus gérer.
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 a été désinscrit, 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 désinscrivez un compte personnalisé, AWS Control Tower supprime les ressources déployées dans le plan, ainsi que toutes les autres ressources créées par AWS Control Tower dans le compte. Après avoir désinscrit le compte, vous pouvez le fermer via. AWS Organizations

Note

Un compte non inscrit n'est ni fermé ni supprimé. Lorsque le compte a été désinscrit, 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 de plus amples informations, veuillez consulter [Mettez à jour et déplacez les comptes Account Factory avec AWS Control Tower ou avec AWS Service Catalog](#).

Vidéo de démonstration

Cette vidéo (3:25) explique comment supprimer un compte de AWS Control Tower, obtenir un accès root au compte et enfin fermer le Compte AWS. Vous pouvez également fermer un compte avec [un 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 de 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

La fermeture d'un compte n' Compte AWS est pas la même chose que la désinscription d'un compte auprès de AWS Control Tower : il s'agit d'actions distinctes. Vous devez désinscrire le compte avant de le fermer.

Fermez le compte d'un membre de AWS Control Tower via AWS Organizations

Vous pouvez fermer vos comptes de membre de AWS Control Tower depuis le compte de gestion de votre organisation sans avoir à vous connecter à chaque compte membre individuellement avec les 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 le AWS Organizations [CloseAccount API](#), ou fermez un compte dans la AWS Organizations console, le compte du membre est isolé pendant 90 jours, comme tout Compte AWS 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 du délai de 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 désinscrire 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 affiche 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 d'organisation 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 ne désinscrivez pas le 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 le [CloseAccount API](#).

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
Amazon CloudWatch	CloudWatch Règles de l'événement	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch Journaux	aws-controltower/CloudTrail Logs
		/aws/lambda/aws-controltower-NotificationForwarder

AWS service	Type de ressource	Nom de la ressource
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

- [Configuration pour la personnalisation](#)
- [Créez un compte personnalisé à partir d'un plan](#)
- [Inscrivez et personnalisez des comptes](#)
- [Ajouter un plan à un compte AWS Control Tower](#)
- [Mettre à jour un plan](#)
- [Supprimer un plan d'un compte](#)
- [Les plans des partenaires](#)
- [Considérations relatives aux personnalisations d'Account Factory \(AFC\)](#)
- [En cas d'erreur de plan](#)
- [Personnalisation de votre document de politique pour les plans de l'AFC sur la base de CloudFormation](#)
- [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 `AWSControlTowerBlueprintAccess` rôle 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, consultez [Personnalisez 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-customizations` référentiel.

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 et [Limites 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-request` référentiel. 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
- SS0UserEmail
- SS0UserFirstName
- SS0UserLastName

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-request` référentiel incluent `OUName` et `OUName (OU-ID)`.

- `account_tagscapture` 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_fieldscapture` 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-customizations` référentiel. 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-request` référentiel 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-request` référentiel.

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 est destinée 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 pour Terraform (AFT) avec un nouveau compte de AFT gestion dédié.

Note

Un module Terraform se déploie. AFT Ce module est disponible dans le [AFT référentiel](#) le GitHub, et l'ensemble du AFT référentiel est considéré comme le module. Nous vous recommandons de vous référer aux AFT modules au GitHub lieu de cloner le AFT référentiel. De cette façon, vous pouvez contrôler et utiliser les mises à jour des modules dès qu'elles sont disponibles.

Pour plus de détails 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 AFT environnement, vous devez disposer des éléments suivants :

- Une zone d'atterrissage de la AWS Control Tower. Pour plus d'informations, consultez [Planifier la zone d'atterrissage AWS de votre Control Tower](#).

- Une région d'accueil pour la zone d'atterrissage AWS de votre Control Tower. Pour plus d'informations, consultez [How Régions AWS work with AWS Control Tower](#).
- Une version et une distribution de Terraform. Pour plus d'informations, consultez [Terraform et AFT ses versions](#).
- Un VCS fournisseur 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 déployez AFT pour la première fois et que vous n'avez pas de CodeCommit référentiel existant, vous devez choisir un VCS fournisseur externe, tel que GitHub ou BitBucket. Pour plus d'informations, 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 s'installe. AFT
- AFToptions de fonctionnalités. Pour plus d'informations, consultez la section [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 AFT en suivant l'[introduction au AFT](#) laboratoire sur le site Web de AWS Workshop Studio.

Étape 1 : Lancez la zone d'atterrissage AWS de votre Control Tower

Suivez les étapes décrites dans [Getting started with AWS Control Tower](#). C'est ici que vous créez le compte de gestion AWS de la Control Tower et que vous configurez votre zone de landing zone de 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 :

- [IAMidentités \(utilisateurs, groupes d'utilisateurs et rôles\)](#) dans le guide de AWS Identity and Access Management l'utilisateur

- [AdministratorAccess](#) dans le Guide de référence des politiques AWS gérées

Étape 2 : Création d'une nouvelle unité organisationnelle pour AFT (recommandé)

Nous vous recommandons de créer une unité d'organisation distincte dans votre AWS organisation. C'est ici que vous déployez le compte AFT de gestion. Créez la nouvelle unité d'organisation avec votre compte de gestion AWS Control Tower. Pour plus d'informations, voir [Création d'une nouvelle unité d'organisation](#).

Étape 3 : provisionner le compte AFT de gestion

AFT exige que vous fournissiez un AWS compte dédié aux opérations AFT de gestion. Le compte de gestion AWS Control Tower, qui est associé à votre zone d'atterrissage AWS Control Tower, vend le compte AFT de gestion. 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 AFT de gestion.

Le provisionnement complet du compte de AFT gestion 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 1.6.0 ou ultérieure.

Étape 5 : Appelez le module Account Factory for Terraform pour le déployer AFT

Appelez le AFT module avec le rôle que vous avez créé pour le compte de gestion AWS Control Tower doté d'AdministratorAccess informations d'identification. AWSControl Tower fournit un module

Terraform via le compte de gestion AWS Control Tower, qui établit toute l'infrastructure requise pour orchestrer les demandes de AWS Control Tower Account Factory.

Vous pouvez consulter le AFT module dans le [AFT référentiel](#) sur GitHub. L'ensemble du GitHub référentiel est considéré comme le AFT module. Reportez-vous au [README fichier](#) pour obtenir des informations sur les entrées requises pour exécuter le AFT module et le déployer AFT. Vous pouvez également consulter le AFT module dans le registre [Terraform](#).

Le AFT module inclut un `aft_enable_vpc` paramètre qui indique si AWS Control Tower fournit les ressources du compte dans un cloud privé virtuel (VPC) dans le compte AFT de gestion central. Par défaut, le paramètre est défini sur `true`. Si vous définissez ce paramètre sur `false`, AWS Control Tower se déploie AFT sans utiliser de ressources réseau privées, telles que VPC des NAT passerelles ou VPC des points de terminaison. La désactivation `aft_enable_vpc` peut contribuer à réduire les coûts d'exploitation AFT de 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 AFT module à votre flux de travail existant. Sinon, exécutez le AFT module 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 d'expiration 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 IAM dans](#) le Guide de AWS Identity and Access Management l'utilisateur.

Note

Vous pouvez attendre jusqu'à 30 minutes AFT pour terminer le déploiement via le module Terraform.

Étape 6 : Gérer le fichier d'état Terraform

Un fichier d'état Terraform est généré lors du déploiement. AFT Cet artefact décrit l'état des ressources créées par Terraform. Si vous prévoyez de mettre à jour la AFT version, assurez-vous de conserver le fichier d'état Terraform ou de configurer un backend Terraform à l'aide d'Amazon S3 et DynamoDB. Le AFT module ne gère pas l'état d'un backend Terraform.

Note

Vous êtes responsable de la protection du fichier d'état de 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'AFT infrastructure terminé, suivez ces étapes supplémentaires pour terminer le processus de configuration et vous préparer à provisionner des comptes.

Étape 1 : Complétez CodeConnections avec le VCS fournisseur de votre choix

Si vous choisissez un VCS fournisseur tiers, il les AFT 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 selon vos préférencesVCS.

L'étape initiale d'établissement de la AWS CodeStar connexion est accomplie parAFT. Vous devez confirmer la connexion.

Étape 2 : remplir chaque référentiel

AFTnécessite que vous gériez [quatre référentiels](#) :

1. Demandes de compte — Ce référentiel gère le placement ou la mise à jour des demandes de compte. [Des exemples sont disponibles](#). Pour plus d'informations sur les demandes de AFT compte, consultez[Création d'un nouveau compte auprès de l'AFT](#).
2. AFTpersonnalisations du provisionnement des comptes : ce référentiel gère les personnalisations appliquées à tous les comptes créés et gérés avecAFT, avant de commencer la phase de personnalisation globale. [Des exemples sont disponibles](#). Pour créer des personnalisations de provisionnement de AFT comptes, 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 [Des exemples sont disponibles](#). Pour créer des personnalisations AFT globales, voir [Appliquer des personnalisations globales](#).
4. Personnalisations de compte : ce référentiel gère les personnalisations appliquées uniquement à des comptes spécifiques créés par et gérés avec. AFT [Des exemples sont disponibles](#). Pour créer des personnalisations de AFT compte, voir [Appliquer les personnalisations de compte](#).

AFTs'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 github](#). [AFT](#)

Présentation de AWS Control Tower Account Factory pour Terraform () AFT

Account Factory for Terraform (AFT) met en place un pipeline Terraform pour vous aider à approvisionner et à personnaliser des comptes dans Control Tower. AWS AFT vous offre l'avantage du provisionnement de comptes basé sur Terraform tout en vous permettant de gérer vos comptes avec Control Tower. AWS

Avec AFT vous, créez un fichier Terraform de demande de compte pour obtenir les informations qui déclenchent le AFT flux de travail pour le provisionnement du compte. Une fois l'étape de provisionnement du compte terminée, exécute AFT 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 AFT comptes](#).

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 la gouvernance de 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, elle AFT génère un jeton de suivi unique qui passe par une machine d' AWS Step Functions état de AFT personnalisation, 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 AFT flux de travail. 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 services [Services relatifs aux composants](#), comme, pour créer un framework, avec des pipelines qui déploient Terraform Infrastructure as Code (IaC). AFT vous permet d'effectuer les opérations suivantes :

- 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 AFT gestion, pour déployer AFT les fonctionnalités. Avant de procéder à la configuration AFT, vous devez disposer d'une zone d'atterrissage AWS Control Tower existante. Le compte AFT de gestion n'est pas le même que le compte de gestion AWS Control Tower.

AFT offre de la flexibilité

- Flexibilité pour votre plateforme : AFT prend en charge n'importe quelle distribution Terraform pour le déploiement initial et le fonctionnement continu : Community Edition, Cloud et Enterprise.
- Flexibilité pour votre système de contrôle de version : AFT supports AWS CodeCommit et sources de contrôle de version alternatives via AWS 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 la AWS valeur par défaut VPC pour les comptes
- Inscription de comptes provisionnés dans le plan de AWS Support aux entreprises

Note

Le AFT pipeline n'est pas destiné à être utilisé pour déployer des ressources, telles que EC2 des instances Amazon, 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 pour 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.](#)

AFTArchitecture

Ordre des opérations

Vous exécutez AFT des opérations dans le compte AFT de gestion. 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 de 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.

AWSControl Tower Account Factory pour Terraform : flux de travail de provisionnement des comptes

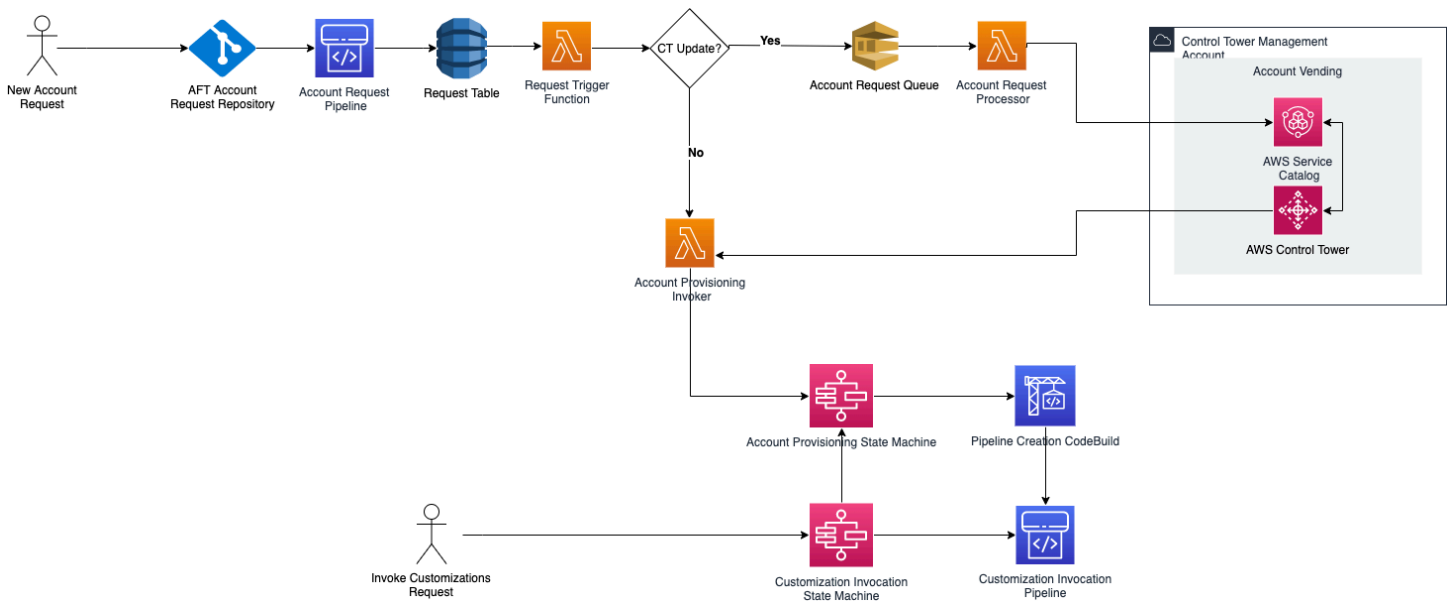


Figure 1 : AWS Control Tower Account Factory pour Terraform

Coût

Il n'existe aucun frais supplémentaire pour 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 AFT environnement.

La AFT configuration par défaut inclut l'allocation de AWS PrivateLink points de terminaison, pour une protection et une sécurité accrues des données, ainsi qu'une NAT passerelle requise pour le support AWS CodeBuild. Pour plus de détails sur la tarification de cette infrastructure, consultez les [AWS PrivateLink tarifs](#) et les [VPCtarifs Amazon pour la NAT passerelle](#). 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. 1.6.0 Vous devez fournir une version Terraform comme paramètre d'entrée pour le processus de déploiement AFT, comme indiqué dans l'exemple suivant.

```
terraform_version = "1.6.0"
```


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, consultez [Déployez 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 Enterprise

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'AFT](#) Pour 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 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-cust omizations
		aws-ct-aft-trigger-baseline

AWS web	Type de ressource	Nom de la ressource
		aws-ct-aft-features
VPC	VPC	aws-ct-aft-vpc
Amazon SNS	Rubriques	aws-ct-aft-notifications aws-ct-aft-failure-notifications
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 web	Type de ressource	Nom de la ressource
		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 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'utilisateur AWS 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": [  
    {  
      "Action": "sts:AssumeRole",  
      "Effect": "Allow",  
      "Resource": "arn:aws:iam::012345678901:role/AWSAFTExecutionRole",  
      "Condition": {"Bool": {"op": "NotEquals", "value": "true", "variable": "aws:PrincipalTag:AccountType"}},  
      "Sid": "AllowAssumeRole" } ]
```

```
{
  "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

Lors du déploiement 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 approvisionner les comptes.
- [Amazon DynamoDB](#) : crée des tables AFT Amazon DynamoDB dans le compte de gestion, qui stockent les demandes de compte, AFT l'historique des audits des mises à jour du compte, les métadonnées du compte et les événements du cycle de vie de la Control Tower. AWS AFT crée également des déclencheurs DynamoDB Lambda pour lancer des processus en aval, tels que AFT le démarrage du flux de travail de provisionnement des comptes.
- [Amazon Simple Storage Service](#) : AFT crée des compartiments Amazon Simple Storage Service (S3) dans AFT le compte de gestion et le compte d'archivage des journaux de la Control AWS Tower, qui stockent les journaux générés par les services requis par AWS le pipeline. AFT crée également un compartiment S3 principal Terraform, dans les AWS régions 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 AFT gestion, qui stocke les notifications de réussite et d'échec après le traitement de chaque demande de AFT compte. Vous pouvez recevoir ces messages en utilisant le protocole de votre choix.
- [Amazon Simple Queuing Service](#) : AFT crée une FIFO file d'attente Amazon Simple Queuing Service (AmazonSQS) 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 AWS CodeBuild construction dans le compte de AFT gestion pour initialiser, compiler, tester et appliquer les plans Terraform pour le code AFT source à différentes étapes de construction.
- [AWS CodePipeline](#)— AFT crée des AWS CodePipeline pipelines dans le compte AFT de gestion pour les intégrer au fournisseur de AWS CodeStar connexions pris en charge que vous avez sélectionné pour le code AFT source et pour déclencher des tâches de création AWS CodeBuild.
- [AWS Lambda](#) : crée des fonctions et des couches AFT AWS Lambda dans le compte de AFT gestion pour effectuer des étapes lors des processus de demande de compte, de provisionnement du AFT compte et de personnalisation du compte.

- [AWSSystems Manager Parameter Store](#) : AFT configure le AWS Systems Manager Parameter Store dans le compte de AFT gestion, afin de stocker les paramètres de configuration requis pour les processus du AFT pipeline.
- [Amazon CloudWatch](#) — AFT crée des groupes de CloudWatch journaux Amazon dans le compte AFT de gestion pour stocker les journaux générés par AWS les services utilisés par le AFT pipeline. 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 AFT de gestion dans un environnement réseau distinct, afin d'améliorer la sécurité.
- [AWSKMS](#) — AFT utilise le AWS Key Management Service (KMS) dans le compte de AFT gestion et dans le compte d'archivage des journaux de 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 AWS ressources et les services sont déployés par AFT. KMS la rotation annuelle AFT des clés créées par 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 AFT gestion, dans les comptes AWS Control Tower et dans les comptes AFT provisionnés, selon les besoins, afin d'effectuer les actions requises pendant le flux de travail du AFT pipeline.
- [AWS Step Functions](#) — AFT crée des machines d'état AWS Step Functions dans le compte AFT de gestion. Ces machines d'état orchestrent et automatisent le processus et les étapes du cadre de provisionnement des AFT comptes et des personnalisations.
- [Amazon EventBridge](#) — AFT crée un bus d'EventBridge événements Amazon dans le compte de gestion AFT and AWS Control Tower afin de capturer et de stocker les événements du cycle de vie de AWS Control Tower à long terme dans la table DynamoDB du compte de AFT gestion. AFT crée des règles relatives aux CloudWatch événements Amazon dans les comptes AFT de gestion et de gestion de AWS Control Tower, qui déclenchent plusieurs étapes requises lors de l'exécution du flux de travail du AFT pipeline
- [AWS CloudTrail \(Facultatif\)](#) — Lorsque cette fonctionnalité est activée, elle AFT crée un journal AWS CloudTrail organisationnel dans le compte de gestion de 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'archive des journaux de AWS Control Tower.

- [AWS Support \(facultatif\)](#) : lorsque cette fonctionnalité est activée, AFT active le plan de support aux AWS entreprises pour les comptes fournis par AFT. Par défaut, les AWS comptes sont créés avec le plan Support AWS de base 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 compte](#) étape.

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 compte](#) étape (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, voir [Réinvoquer 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, consultez [Configurez et lancez votre AWS Control Tower Account Factory pour Terraform](#).
- gitRéférentiels 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 réinvoque 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/](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 un système AWS CodeCommit de contrôle de version du code source (VCS), et il en autorise d'autres [CodeConnections](#) qui répondent aux exigences de votre entreprise ou à votre architecture existante.

Si vous déployez AFT pour la première fois et que vous n'avez pas de CodeCommit référentiel existant, vous devez spécifier un VCS fournisseur externe, dans le cadre des conditions préalables au AFT déploiement. Pour plus d'informations, consultez la section [Alternatives pour le contrôle de version du code source dans AFT](#).

AFT prend en charge les alternatives de contrôle du code source suivantes :

- GitHub
- GitHub Serveur d'entreprise
- BitBucket

Note

Si vous spécifiez AWS CodeCommit le VCS, aucune étape supplémentaire n'est requise. 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.

Configurez un autre système de contrôle de version du code source (personnalisé VCS) avec AFT

Pour configurer un autre système de contrôle de version du code source pour votre AFT déploiement, procédez comme suit.

Étape 1 : créer des `git` référentiels dans un système de contrôle de version tiers pris en charge (VCS).

Si vous n'en utilisez pas AWS CodeCommit, vous devez créer des `git` référentiels dans votre environnement de VCS fournisseur tiers AFT pris en charge pour les éléments suivants.

- AFT demandes de compte. [Exemple de code disponible](#). Pour plus d'informations sur les demandes de AFT compte, consultez [Création d'un nouveau compte auprès de l'AFT](#).

- AFT personnalisations du provisionnement des comptes. [Exemple de code disponible](#). Pour plus d'informations sur les personnalisations du provisionnement des AFT comptes, consultez [Créez votre compte AFT, provisionnement, personnalisation, machine à états](#)
- AFT personnalisations globales. [Exemple de code disponible](#). Pour plus d'informations sur les personnalisations AFT globales, consultez [Personnaliser le compte](#).
- AFT personnalisations de compte. [Exemple de code disponible](#). Pour plus d'informations sur les personnalisations de AFT compte, consultez [Personnaliser le compte](#).

Étape 2 : Spécifier les paramètres VCS de configuration requis pour AFT le déploiement

Les paramètres d'entrée suivants sont nécessaires pour configurer votre VCS fournisseur dans le cadre du AFT déploiement.

- `vcs_provider` : Si vous ne l'utilisez pas AWS CodeCommit, spécifiez le VCS fournisseur en tant que `"bitbucket"`, ou `"github"`/`"githubenterprise"`, en fonction de votre cas d'utilisation.
- `github_enterprise_url` : pour les clients GitHub Enterprise uniquement, spécifiez le. GitHub URL
- `account_request_repo_name` : pour les AWS CodeCommit utilisateurs, cette valeur est définie sur. `aft-account-request` Dans un environnement de VCS fournisseur tiers AFT pris en charge, 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` : pour les AWS CodeCommit utilisateurs, cette valeur est définie sur. `aft-account-customizations` Dans un environnement de VCS fournisseur tiers AFT pris en charge, 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` : pour les utilisateurs, cette valeur est définie sur. AWS CodeCommit `aft-account-provisioning-customizations` Dans un environnement de VCS fournisseur tiers AFT pris en charge, 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` : pour les AWS CodeCommit utilisateurs, cette valeur est définie sur. `aft-global-customizations` Dans un environnement de VCS fournisseur tiers AFT pris en charge, 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 existe main par défaut, mais la valeur peut être remplacée.

Par défaut, les AFT sources 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 README fichier du module [AFTTerraform](#).

Pour les AWS CodeCommit clients existants

Si vous créez un CodeCommit référentiel sous un nouveau nom pour AFT, vous pouvez mettre à jour le nom du référentiel en mettant à jour les valeurs de ces paramètres d'entrée.

Étape 3 : terminer la AWS CodeStar connexion pour les VCS fournisseurs tiers

Lorsque votre déploiement s'exécute, AFT il crée les AWS CodeCommit référentiels requis ou une AWS CodeStar connexion pour le VCS fournisseur tiers que vous avez choisi. Dans ce dernier cas, vous devez vous connecter manuellement à la console du compte de AFT gestion 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 AWS consultez 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 de AWS 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 S3aft-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 AWS. Nous 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    = "xxxxxxxxxxxx"
  log_archive_account_id     = "xxxxxxxxxxxx"
  audit_account_id           = "xxxxxxxxxxxx"
  aft_management_account_id  = "xxxxxxxxxxxx"
  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 font partie des tâches opérationnelles habituelles des administrateurs de comptes de gestion de 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 (OUs), comptes et 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

AWSControl Tower détecte automatiquement la dérive. Pour détecter la dérive, le `AWSControlTowerAdmin` rôle nécessite un accès permanent à votre compte de gestion afin que AWS Control Tower puisse passer des API appels en lecture seule. AWS Organizations Ces API appels apparaissent sous forme d' AWS CloudTrail événements.

La dérive apparaît dans les notifications Amazon Simple Notification Service (AmazonSNS) qui sont agrégées dans le compte d'audit. Les notifications de chaque compte membre envoient des alertes à une SNS rubrique Amazon locale et à une fonction Lambda.

Pour les contrôles faisant partie du AWS Security Hub Service-Managed Standard : AWS Control Tower, la dérive est indiquée sur les pages du compte et des détails du compte de la console AWS Control Tower, ainsi que par le biais d'une notification AmazonSNS.

Les administrateurs des comptes des membres peuvent (et c'est la meilleure pratique, ils devraient) s'abonner aux notifications de SNS dérive pour des comptes spécifiques. Par exemple, la `aws-controltower-AggregateSecurityNotifications` SNS rubrique 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 SNS sujets relatifs à la détection et à la notification de [la dérive, voir 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 SNS notification 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 et la SCP dérive des comptes sont gérées de la manière suivante

- Si vous modifiez le même gestionnaire à SCP plusieurs reprises, vous recevez une notification lorsque vous le modifiez pour la première fois.
- Si vous modifiez un objet géréSCP, puis que vous corrigez une dérive, puis que vous le modifiez à nouveau, vous recevrez deux notifications.
- Si un compte est déplacé OUs plusieurs fois entre la même source et la même destination, sans que la dérive soit réparée au préalable, une seule notification est envoyée, même si le compte a été transféré de l'une à l'autre à OUs plusieurs reprises.

Types de dérive des comptes

- Le compte a été transféré entre OUs
- 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 SCPs et AWS Config les règles doivent toujours être supprimés manuellement lorsqu'un compte changeOUs.

Types de dérive politique


- SCPmis à jour
- SCPattaché à l'OU
- SCPdétaché de l'OU
- SCPattaché 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 1 000 comptes, vous pouvez résoudre le problème de dérive dans les comptes provisionnés par Account Factory, ou de SCP dérive, 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 de plus amples informations, veuillez consulter [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 de la 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 SCP scans

AWSControl Tower scanne SCPs quotidiennement votre appareil géré pour vérifier que les commandes correspondantes sont correctement appliquées et qu'elles n'ont pas dérivé. Pour les récupérer SCPs et les vérifier, AWS Control Tower appelle en votre AWS Organizations nom, en utilisant un rôle dans votre compte de gestion.

Si un scan AWS de la Control Tower détecte une dérive, vous recevrez une notification. AWSControl 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 objet de dérive ne soit trouvé.

AWS Organizations limite la fréquence à laquelle chacun d'entre eux APIs peut être appelé. Cette limite est exprimée en transactions par seconde (TPS) et est connue sous le nom de TPSlimite, de taux de limitation ou de taux de API demandes. Lorsque AWS Control Tower effectue un audit de vos appels AWS Organizations, les API appels passés SCPs par AWS Control Tower sont pris en compte dans le calcul de votre TPS limite, 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 la même personne APIs 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 le même appel AWS Organizations APIs au même moment (dans un délai d'une seconde) et que les TPS limites 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 API demandes est dépassé

- Si AWS Control Tower atteint la limite et est limitée, nous interrompons 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 SCP scan quotidien consiste en

1. Récupération de votre activité OUs récente.
2. Pour chaque unité d'organisation enregistrée, récupération de toutes les unités SCPs gérées par AWS Control Tower qui sont rattachées à l'unité d'organisation. SCPsLes personnes gérées ont des identifiants qui commencent `aws-guardrails` par.
3. Pour chaque contrôle préventif activé sur l'unité d'organisation, vérifier que l'énoncé de politique du contrôle est présent dans l'unité d'organisation gérée SCPs.

Une unité d'organisation peut en avoir une ou plusieurs gérées SCPs.

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 d'atterrissage de la AWS Control Tower. Voici quelques exemples de dérives majeures que vous souhaitez 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 que certains AWS Identity and Access Management (IAM) rôles ne sont pas déviés lorsque vous vous connectez à IAM la console. 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`, `AWSControlTowerCloudTrailRole`, `AWSControlTowerStackSetRole`.

Pour plus d'informations sur ces rôles, consultez [Autorisations requises pour utiliser la console AWS Control Tower](#).

- Ne supprimez pas tous les éléments supplémentaires OUs : si vous supprimez l'unité organisationnelle initialement nommée Sandbox lors de la configuration de la zone d'atterrissage par AWS Control Tower, votre zone d'atterrissage sera en état de dérive, mais vous pourrez toujours utiliser AWS Control Tower. Au moins une unité d'organisation supplémentaire est requise pour que AWS Control Tower fonctionne, mais il n'est pas nécessaire que ce soit l'unité d'organisation Sandbox.
- Ne supprimez pas les comptes partagés : si vous supprimez des comptes partagés de FoundationalOUs, par exemple si vous supprimez le compte de connexion de l'unité d'organisation de sécurité, votre zone de landing sera en état de dérive. La zone d'atterrissage 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 de la AWS Control Tower, bien qu'elles puissent entraîner une dérive résoluble. 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.
- Changez le nom des comptes des membres dans Non-FoundationalOUs.
- 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 d'OUsun compte à un autre 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 fonction d'inscription du compte dans AWS Control Tower ne fonctionnera pas. Dans ce cas, vous devez créer de nouveaux comptes via AWS Service Catalog. Pour obtenir des instructions, consultez [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, telles que 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 OUsSCPs, et les comptes des membres sont modifiés ou mis à jour. Les types de dérive de gouvernance qui peuvent être détectés dans AWS Control Tower sont les suivants :

- [Déplacement du compte membre](#)
- [Suppression de compte membre](#)
- [Mise à jour imprévue vers Managed SCP](#)
- [SCPAttaché au compte du membre](#)
- [SCP Rattaché à l'unité d'organisation gérée](#)
- [SCP Détaché de l'unité d'exploitation 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 IAM rôles, ou à tout type de dérive organisationnelle qui affecte spécifiquement les comptes fondamentaux OUs et 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 ainsi que 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 du AWS Security Hub Service-managed Standard : 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 de 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 SNS notification Amazon 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 1000 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 1 000 comptes, vous pouvez y remédier en :

- Accédez à la page Organisation de 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 de 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 de plus amples informations, veuillez consulter [Enregistrer une unité organisationnelle existante auprès AWS de Control Tower](#).
- Mettre à jour le produit provisionné dans Account Factory. Pour de plus amples informations, veuillez consulter [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 1 000 comptes, la résolution de la dérive peut dépendre du type de compte qui a été déplacé, comme expliqué dans les paragraphes suivants. Pour de plus amples informations, veuillez consulter [Mettez à jour votre zone de landing zone](#).
- Si un compte approvisionné par Account Factory est déplacé : dans une unité d'organisation comptant moins de 1 000 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 1 000 comptes, vous devez résoudre le problème en mettant à jour chaque compte déplacé, soit par le biais de la console AWS Control Tower, soit par le biais du produit provisionné, car le fait de réenregistrer l'unité d'organisation n'effectuera pas la mise à jour. Pour de plus amples informations, veuillez consulter [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 de plus amples informations, veuillez consulter [Mettez à jour votre zone de landing zone](#).

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 de AWS Control Tower. L'exemple suivant montre la SNS notification Amazon 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 de plus amples informations, veuillez consulter [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 plus d'informations sur la résolution de la dérive pour les comptes OUs, voir [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 imprévue vers Managed SCP

Ce type de dérive peut se produire lorsqu'un SCP contrôle est mis à jour dans la AWS Organizations console ou par programmation à l'aide du AWS CLI ou de l'un des AWS SDKs. Voici un exemple de SNS notification Amazon 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 comportant jusqu'à 1 000 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 de plus amples informations, veuillez consulter [Enregistrer une unité organisationnelle existante auprès AWS de Control Tower](#).
- Mise à jour de votre zone d'atterrissage (option plus lente). Pour de plus amples informations, veuillez consulter [Mettez à jour votre zone de landing zone](#).

Lorsque ce type de dérive se produit dans une unité d'organisation comportant plus de 1 000 comptes, corrigez-le en mettant à jour votre zone de landing zone. Pour de plus amples informations, veuillez consulter [Mettez à jour votre zone de landing zone](#).

SCPRattaché à l'unité d'organisation gérée

Ce type de dérive peut se produire lorsqu'un SCP contrôle est attaché à une autre unité d'organisation. Ce problème est particulièrement fréquent lorsque vous travaillez sur votre console OUs depuis l'extérieur de la console AWS Control Tower. Voici un exemple de SNS notification Amazon 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 comportant jusqu'à 1 000 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 de plus amples informations, veuillez consulter [Enregistrer une unité organisationnelle existante auprès AWS de Control Tower](#).
- Mise à jour de votre zone d'atterrissage (option plus lente). Pour de plus amples informations, veuillez consulter [Mettez à jour votre zone de landing zone](#).

Lorsque ce type de dérive se produit dans une unité d'organisation comportant plus de 1 000 comptes, corrigez-le en mettant à jour votre zone de landing zone. Pour de plus amples informations, veuillez consulter [Mettez à jour votre zone de landing zone](#).

SCP Détaché de l'unité d'exploitation gérée

Ce type de dérive peut se produire lorsqu'un SCP contrôle a été détaché d'une UO gérée par AWS Control Tower. Ce problème est particulièrement fréquent lorsque vous travaillez en dehors de la console AWS Control Tower. Voici un exemple de SNS notification Amazon 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 comportant jusqu'à 1 000 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 de plus amples informations, veuillez consulter [Enregistrer une unité organisationnelle existante auprès AWS de 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, consultez [Mettez à jour votre zone de landing zone](#).

Lorsque ce type de dérive se produit dans une unité d'organisation comportant plus de 1 000 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, consultez [Mettez à jour votre zone de landing zone](#).

SCP Attaché au compte du membre

Ce type de dérive peut se produire lorsqu'un SCP contrôle est associé à un compte dans la console Organizations. Les garde-corps et leurs accessoires SCPs peuvent être activés OUs (et donc appliqués à tous les comptes inscrits d'une unité d'organisation) via la console AWS Control Tower. Voici un exemple de SNS notification Amazon 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 de plus amples informations, veuillez consulter [Mettez à jour votre zone de landing zone](#).

Lorsque ce type de dérive se produit dans une unité d'organisation non fondamentale comptant jusqu'à 1 000 comptes, vous pouvez y remédier en :

- Détacher la AWS Control Tower SCP 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 de plus amples informations, veuillez consulter [Enregistrer une unité organisationnelle existante auprès AWS de Control Tower](#).

Lorsque ce type de dérive se produit dans une unité d'organisation comportant plus de 1 000 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 de plus amples informations, veuillez consulter [Mettez à jour votre zone de landing zone](#).

UO de base supprimée

Ce type de dérive s'applique uniquement à AWS Control Tower FoundationalOUs, tel que l'unité d'organisation Security. Cela peut se produire si une UO de base est supprimée en dehors de la console AWS Control Tower. Il est impossible de déplacer Foundational sans créer ce type de dérive, car déplacer une UO revient à la supprimer puis à l'ajouter ailleurs. Lorsque vous corrigez la dérive en mettant à jour votre zone d'atterrissage, AWS Control Tower remplace l'unité d'organisation de base à son emplacement d'origine. L'exemple suivant montre une SNS notification Amazon 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 OUs que pour Foundational, la résolution est de mettre à jour la zone d'atterrissage. Lorsque d'autres types de OUs fichiers sont supprimés, AWS Control Tower est automatiquement mis à jour.

Pour plus d'informations sur la résolution de la dérive pour les comptes OUs, voir [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 du AWS Security Hub Service-Managed Standard : AWS Control Tower signale un état de dérive. Le AWS Security Hub service lui-même ne signale aucun état de dérive pour ces commandes. Au lieu de cela, le service envoie ses résultats à AWS Control Tower.

Une dérive du contrôle du 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 la commande est en dérive. L'exemple suivant montre une SNS notification Amazon 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

Dans le OUs cas de moins de 1 000 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 par le biais de la console ou de la AWS Control Tower APIs, qui réinitialise également le contrôle.

Pour plus d'informations sur la résolution de la dérive pour les comptes OUs, voir [Si vous gérez des ressources en dehors d'AWS Control Tower](#).

Accès sécurisé désactivé

Ce type de dérive s'applique aux zones d'atterrissage AWS de la Control Tower. Cela se produit lorsque vous désactivez l'accès sécurisé à AWS Control Tower AWS Organizations après avoir configuré la zone d'atterrissage AWS de votre 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 OUs. C'est pourquoi il est important de réenregistrer chaque OU chaque fois que vous mettez à jour votre zone de landing zone.

Exemple : SNS notification Amazon

Voici un exemple de la SNS notification Amazon 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

AWSControl 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 AWS de votre 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 » dans [Déterminez 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 [Déterminez 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'adresse <https://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 (OUs) et tous les comptes que vous créez dans AWS Control Tower sont régis automatiquement par AWS Control Tower. De plus, si vous avez des comptes existants OUs et des comptes créés en dehors de AWS Control Tower, vous pouvez les intégrer à la gouvernance AWS de 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, consultez [Inscrire 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 créez un AWS compte dans AWS Control Tower, cela s'appelle l'inscrire.

Consultez vos comptes OUs et vos comptes

Sur la page AWS Control Tower Organization, vous pouvez voir toutes les informations qui se trouvent OUs dans votre compte AWS Organizations, y compris celles OUs qui sont enregistrées auprès de AWS Control Tower et celles qui ne le sont pas. Vous pouvez afficher imbriqué dans OUs 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 dans le OUs, si les comptes répondent aux conditions requises pour l'inscription.

Si vous ne sélectionnez aucun filtre, la page Organisation affiche vos comptes OUs dans une hiérarchie. Il s'agit d'un emplacement central pour surveiller et prendre des mesures sur toutes les

ressources de votre AWS Control Tower. Pour plus d'informations sur la page Organisation, vous pouvez visionner la vidéo de présentation.

Vidéo de démonstration

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 la page Working with the Organization dans AWS Control Tower.](#)

Rubriques

- [Enregistrer une unité organisationnelle existante auprès AWS de Control Tower](#)
- [Inscrire un existant Compte AWS](#)

Étendre la gouvernance à une organisation existante

Vous pouvez ajouter la gouvernance de la AWS Control Tower à une organisation existante en configurant une zone d'atterrissage (LZ), comme indiqué dans le guide de l'utilisateur de la AWS Control Tower présenté à l'[étape 2 de Getting Started](#).

Voici ce à quoi vous pouvez vous attendre lorsque vous configurez votre zone de landing AWS Control Tower dans une organisation existante.

- Vous ne pouvez avoir qu'une seule zone de landing zone par AWS Organizations organisation.
- AWSControl Tower utilise le compte de gestion de votre AWS Organizations organisation existante comme compte de gestion. Aucun nouveau compte de gestion n'est nécessaire.
- AWSControl Tower crée 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 commandes de la 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 en ajouter d'autres OUs dans AWS Control Tower et vous pouvez vous enregistrer déjà OUs.

Pour vérifier les autres conditions requises pour l'enregistrement et l'inscription, consultez [Getting Started with AWS Control Tower](#).

Voici plus de détails sur le fait que les contrôles de la AWS Control Tower ne s'appliquent pas à vous OUs dans AWS les organisations qui n'ont pas configuré de zones d'atterrissage pour la AWS Control Tower :

- Les nouveaux comptes créés en dehors de AWS Control Tower Account Factory ne sont pas soumis aux contrôles de l'unité d'organisation enregistrée.
- Les nouveaux comptes créés dans OUs qui ne sont pas enregistrés auprès de 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 tout compte nouveau OUs ou créé en dehors de AWS Control Tower ne sont pas liés par les contrôles de 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 à des comptes OUs et à des comptes existants, consultez [Enregistrer une unité organisationnelle existante auprès AWS de Control Tower](#).

Pour un aperçu du processus de mise en place d'une zone d'atterrissage 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 est susceptible d'interférer avec le déploiement actuel de votre zone d'atterrissage. Consultez également [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 de la AWS Control Tower doit être identique à la région IAM Identity Center.
- AWS Control Tower ne supprime pas une configuration existante.
- Si IAM Identity Center est déjà activé et si vous utilisez IAM Identity Center Directory, 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 de AWS Control Tower, vous avez toujours accès à tous les AWS services disponibles via AWS Organizations, au moyen de la AWS Organizations console et APIs. 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.

i 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 AWS de 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 permettre à AWS Control Tower de gouverner une UO existante créée avec AWS Organizations et ses comptes, enregistrez l'UO auprès de votre zone d'atterrissage AWS Control Tower. Vous pouvez enregistrer un compte OUs contenant jusqu'à 1 000 comptes. Si une unité d'organisation contient plus de 1 000 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 de AWS Control Tower. Ils sont régis par les contrôles qui s'appliquent à leur unité d'organisation.

i Note

Si vous n'avez pas encore de zone d'atterrissage AWS Control Tower, commencez par créer 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, consultez [Commencer à utiliser AWS Control Tower](#).

Qu'arrive-t-il à mes comptes lorsque j'enregistre mon unité d'organisation ?

AWSControl 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 il se peut que certains comptes ne soient pas enregistrés. 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.

IAMconditions requises par l'utilisateur pour enregistrer une UO

Votre AWS Identity and Access Management (IAM) identité (utilisateur ou rôle) ou l'IAMidentité d'utilisateur d'Identity Center doivent être incluses dans le portefeuille Account Factory approprié lorsque vous effectuez l'opération Register OU, même si vous disposez déjà Admin des 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'IAMutilisateur ou sur l'IAMidentité de l'utilisateur Identity Center lors de l'enregistrement d'une unité d'organisation.

Le portefeuille correspondant est celui créé par AWS Control Tower, appelé AWSControl 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 IAM identité IAM ou celle d'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 de votre organisation OUs et de tous les comptes de votre organisation dans une hiérarchie, y compris ceux OUs qui sont enregistrés auprès de AWS Control Tower et ceux qui ne le sont pas.

En général, les zones non enregistrées OUs ont été créées dans AWS Organizations et ne sont régies par aucune autre zone d'atterrissage. Vous pouvez enregistrer des comptes existants OUs contenant jusqu'à 1 000 comptes. Si une unité d'organisation contient plus de 1 000 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 de la 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 votre compte OUs, 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 par les contrôles 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 [Déterminez et corrigez les dérives dans AWS Control Tower](#).

Note

Une situation inhabituelle peut se produire lorsque AWS Control Tower affiche des écrans OUs 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

Voici comment créer une UO ou une UO imbriquée dans AWS Control Tower.

Pour créer une nouvelle UO 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 le menu déroulant de l'unité d'organisation parent, vous pouvez voir la hiérarchie des unités enregistrées OUs. 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 imbriquées OUs, vous ne verrez pas les unités d'organisation L5 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 Nested OUs in AWS Control Tower, consultez [UO imbriquées dans AWS Control Tower](#).

Causes courantes d'échec lors de l'enregistrement ou du réenregistrement

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.

Si l'enregistrement (ou le réenregistrement) d'une unité d'organisation ou de l'un de ses comptes membres échoue, AWS Control Tower renvoie des messages d'erreur pour les comptes des membres concernés. Vous pouvez consulter les messages d'erreur sur la page des détails de l'unité d'organisation, où un tableau regroupe les prévérifications et les messages d'erreur du compte. Si une opération d'enregistrement de l'unité d'organisation échoue, le tableau affiche tous les messages

d'erreur pour tous les comptes de l'unité d'organisation. Si nécessaire, vous pouvez également consulter les messages d'erreur sur la page des détails du compte pour chaque compte.

Vous pouvez éventuellement télécharger un fichier contenant un rapport détaillé indiquant les prévérifications qui n'ont pas été validées, pour une analyse hors ligne. 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.

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'OU

- Dépasse le nombre maximum de SCPs

Vous avez peut-être dépassé la limite des politiques de contrôle des services (SCPs) par unité d'organisation, ou vous avez peut-être atteint un autre quota. Une limite de 5 SCPs par unité d'organisation s'applique à toutes les personnes OUs présentes dans la zone d'atterrissage de votre AWS Control Tower. Si vous avez SCPs plus que le quota autorisé, vous devez supprimer ou combiner les SCPs.

- En conflit SCPs

L'existant SCPs peut être appliqué à l'unité d'organisation ou au compte, ce qui empêche AWS Control Tower d'enregistrer le compte. Vérifiez la politique appliquée SCPs qui pourrait empêcher AWS Control Tower de fonctionner. Assurez-vous de vérifier ceux SCPs qui sont hérités du OUs niveau supérieur de 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

AWSControl Tower limite chaque UO à 1 000 comptes lors de l'enregistrement.

Erreurs liées au compte

- Contrôles préalables empêchés sur les comptes

Une présence SCP 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-le à jour ou supprimez-le SCP de l'UO.

- 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 de la AWS Control Tower a régi les ressources, avant de pouvoir créer un compte.

- STShandicapé

AWS Security Token Service (AWS STS) peut être désactivé dans le compte. AWS STS les points de terminaison doivent être activés dans les comptes de toutes les régions prises en charge par AWS Control Tower.

- IAMConflit lié au centre d'identité

La région d'origine de la AWS Control Tower n'est pas la même que la région AWS IAM Identity Center (IAM Identity Center). Si IAM Identity Center est déjà configuré, la région d'origine de la AWS Control Tower doit être identique à la région IAM Identity Center.

- SNSSujet contradictoire

Le compte possède un nom de rubrique Amazon Simple Notification Service (Amazon SNS) que AWS Control Tower doit utiliser. AWSControl Tower crée des ressources (telles que SNS des rubriques) portant des noms spécifiques. Si ces noms sont déjà utilisés, la configuration AWS de Control Tower échoue. Cette situation peut se produire si vous réutilisez un compte précédemment inscrit à 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.

- **IAMutilisateur ne figurant 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 à AWS Control Tower. Les instructions pour ajouter un rôle sont disponibles dans [Ajoutez manuellement le IAM rôle 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 à 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 AWS Control Tower OUs et ses comptes

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 effectuer une mise à jour de tous les comptes d'une unité d'organisation à l'aide de l'option Réenregistrement.
- Si vous avez plus d'une unité d'organisation enregistrée dans votre zone de landing, réenregistrez toutes vos unités d'organisation OUs 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. Consultez [Mettre à jour le compte dans la console](#).

Mettre à jour plusieurs comptes dans la même unité d'organisation

Répétez ces étapes pour chaque unité d'organisation de votre organisation AWS Control Tower, si vous devez mettre à jour tous vos comptes etOUs.

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.

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 de la réinscription

Lorsque vous réenregistrez une UO :

- Le champ État indique si le compte est actuellement inscrit auprès de AWS Control Tower (Enrolled), s'il n'a jamais été inscrit (Non inscrit) ou si l'inscription a déjà échoué (Echec 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.
- AWSControl Tower crée un identifiant d'authentification unique (IAMIdentity Center) pour les nouveaux comptes inscrits.
- Les comptes inscrits sont réinscrits dans AWS Control Tower.
- La dérive des contrôles préventifs appliqués à l'unité d'organisation est corrigée, car ils SCPs sont renvoyés à 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 de membres, vous pouvez voir un message d'échec mentionnant le StackSet-`AWSControlTowerExecutionRole`. Cela peut échouer StackSet dans le compte de gestion car le `AWSControlTowerExecutionIAMrôle` 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 les 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, consultez [Mettre 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 [Créez AWS Control Tower des 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 `demanded-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, consultez [Surveillez 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 CloudFormation ou 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 [Déterminez 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 l'approvisionnement de comptes dans Account Factory ou la création de nouvelles unités organisationnelles (OUs) dans la console AWS Control Tower, vous pouvez AWS Identity and Access Management (IAM) ou AWS IAM Identity Center vous demander d'authentifier que vous êtes approuvé AWS utilisateur. Par exemple, si vous utilisez la console AWS Control Tower, vous authentifieriez votre identité en fournissant votre AWS informations d'identification, telles que fournies par votre administrateur.

Après avoir authentifié votre identité, IAM contrôle votre accès à AWS avec un ensemble défini d'autorisations sur un ensemble spécifique d'opérations et de ressources. Si vous êtes administrateur de compte, vous pouvez IAM contrôler l'accès des autres IAM utilisateurs aux ressources associées à votre compte.

Rubriques

- [Authentification](#)
- [Contrôle d'accès](#)
- [Travailler avec AWS IAM Identity Center et AWS Control Tower](#)
- [Présentation de la gestion des autorisations d'accès aux ressources AWS de votre Control Tower](#)
- [Empêchez l'usurpation d'identité entre services](#)
- [Utilisation de politiques basées sur l'identité \(politiques IAM\) pour AWS Control Tower](#)

Authentification

Vous avez accès à AWS sous l'un des types d'identités suivants :

- AWS utilisateur root du compte — Lorsque vous créez pour la première fois un AWS compte, vous commencez avec une identité qui a un accès complet à tous AWS services et ressources du compte. Cette identité s'appelle AWS utilisateur root du 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 IAM utilisateur \(ce n'est pas une bonne pratique dans la plupart des cas\)](#)

[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 de plus amples informations, veuillez consulter [Quand se connecter en tant qu'utilisateur root](#).

- IAMutilisateur — Un [IAMutilisateur](#) est une identité au sein de votre AWS compte doté d'autorisations spécifiques et personnalisées. Vous pouvez utiliser les informations IAM d'identification de l'utilisateur pour vous connecter afin de sécuriser AWS des pages Web telles que AWS Console de gestion, AWS Forums de discussion, ou AWS Centre de support. AWS les meilleures pratiques recommandent de créer un utilisateur IAM Identity Center plutôt qu'un IAM utilisateur, car le risque de sécurité est accru lorsque vous créez un IAM utilisateur doté d'informations d'identification à long terme.

Si vous devez créer un IAM utilisateur dans un certain but, outre les informations de connexion, vous pouvez générer des clés d'accès pour chaque IAM utilisateur. Vous pouvez utiliser ces touches lorsque vous appelez AWS services programmatiquement, soit par le biais de l'un des nombreux services, soit en SDKs utilisant le AWS Interface de ligne de commande (CLI). Les CLI outils SDK et utilisent les clés d'accès pour signer cryptographiquement votre demande. Si vous n'utilisez pas AWS outils, vous devez signer vous-même la demande. AWSControl Tower prend en charge Signature Version 4, un protocole permettant d'authentifier les demandes API entrantes. Pour plus d'informations sur l'authentification des demandes, voir [Processus de signature de la version 4 de Signature](#) dans le AWS Référence générale.

- IAMrôle : un [IAMrôle](#) est une IAM identité que vous pouvez créer dans votre compte et qui dispose d'autorisations spécifiques. Un IAM rôle est similaire à un IAM utilisateur dans la mesure où il s'agit d'un AWS identité, et il dispose de politiques d'autorisation qui déterminent ce que l'identité peut et ne peut pas faire dans AWS. Cependant, au lieu d'être uniquement associé à une seule personne, un rôle est censé être assumé par quiconque 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. IAMles rôles dotés d'informations d'identification temporaires sont utiles dans les situations suivantes :
 - Accès utilisateur fédéré : au lieu de créer un IAM utilisateur, vous pouvez utiliser les identités existantes depuis AWS Directory Service, le répertoire des utilisateurs de votre entreprise ou un fournisseur d'identité Web. Ces derniers 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 la section [Utilisateurs fédérés et rôles du Guide](#) de l'IAMutilisateur.

- **AWS accès au service** — Un rôle de service est un IAM rôle qu'un service assume pour effectuer des actions sur votre compte en votre nom. Lorsque vous configurez certains AWS environnements de 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 accède au AWS les ressources dont elle 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 l'intérieur 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, voir [Création d'un rôle pour déléguer des autorisations à un AWS Service indiqué](#) dans le guide de IAM l'utilisateur.
- **Applications exécutées sur Amazon EC2** : vous pouvez utiliser un IAM rôle pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance Amazon et qui créent AWS CLI ou AWS API demandes. Cela est préférable au stockage des clés d'accès dans l'EC2 instance Amazon. Pour attribuer un AWS pour attribuer un rôle à une EC2 instance Amazon et la rendre disponible pour toutes ses applications, vous créez un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l'EC2 instance Amazon d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez la section [Utiliser un IAM rôle pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon](#) dans le guide de IAM l'utilisateur.
- **IAM L'authentification des utilisateurs d'IAM Identity Center sur le portail utilisateur d'Identity Center** est contrôlée par le répertoire que vous avez connecté à IAM Identity Center. Toutefois, l'autorisation accordée à AWS les comptes accessibles aux utilisateurs finaux depuis le portail utilisateur sont déterminés par deux facteurs :
 - Qui a obtenu l'accès à ces AWS comptes dans le AWS IAM Console Identity Center. Pour plus d'informations, consultez la section [Accès par authentification unique](#) dans le AWS IAM Identity Center Guide de l'utilisateur.
 - Quel niveau d'autorisations a été accordé aux utilisateurs finaux dans le AWS IAM Console Identity Center pour leur permettre l'accès approprié à ces AWS comptes. Pour plus d'informations, consultez la section [Ensembles d'autorisations](#) dans le AWS IAM Identity Center Guide de 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 avez besoin d'autorisations pour effectuer l'opération, et vous avez besoin 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 aux ressources AWS de votre 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, consultez [IAM Conseils relatifs au centre d'identité](#).

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 la configuration de groupes, de rôles et de 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	AWSServiceCatalogE ndUserAccess	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	AWSServiceCatalogA dminFullAccess	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 aux ressources AWS de votre Control Tower

Chaque AWS la ressource est détenue par un Compte AWS, et les autorisations permettant de créer une ressource ou d'y accéder sont régies par des politiques d'autorisation. Un administrateur de compte peut associer des politiques d'autorisation aux IAM identités (c'est-à-dire aux utilisateurs, aux groupes et aux 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 la section [IAM Bonnes pratiques](#) du guide de IAM l'utilisateur.

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 nécessitent des autorisations, ainsi que les actions spécifiques qui doivent être autorisées pour exploiter ces ressources.

Rubriques

- [AWS Ressources et opérations de la 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](#)

AWS Ressources et opérations de la Control Tower

Dans AWS Control Tower, la principale ressource est une zone d'atterrissage. AWS Control Tower prend également en charge un type de ressource supplémentaire, les commandes, parfois appelées glissières de sécurité. Toutefois, pour AWS Control Tower, vous ne pouvez gérer les commandes que dans le contexte d'une zone d'atterrissage existante. Les contrôles peuvent être considérés comme des sous-ressources.

Ressources et sous-ressources dans AWS sont associés à des noms de ressources Amazon (ARNs) uniques, comme illustré dans l'exemple suivant.

AWS Control Tower fournit un ensemble d'API opérations permettant de travailler avec les ressources AWS de la Control Tower. Pour une liste des opérations disponibles, voir AWS Control Tower [the AWS Control Tower API Reference](#).

Pour plus d'informations sur le AWS CloudFormation ressources disponibles dans AWS Control Tower, consultez [le AWS CloudFormation Guide de l'utilisateur](#).

À propos de la propriété des ressources

Le AWS le 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 AWS compte de l'[entité principale](#) (c'est-à-dire le Compte AWS utilisateur root, utilisateur du centre d'IAM identité, IAM utilisateur ou IAM rôle) qui authentifie la demande de création de ressource. Les exemples suivants illustrent comment cela fonctionne :

- Si vous utilisez le plugin AWS informations d'identification de l'utilisateur root de votre compte AWS compte pour configurer une zone d'atterrissage, votre AWS le compte est le propriétaire de la ressource.
- Si vous créez un IAM utilisateur dans votre AWS compte et accorder à cet utilisateur l'autorisation de configurer une zone d'atterrissage, l'utilisateur peut configurer une zone d'atterrissage tant que son compte répond aux conditions préalables. Cependant, votre AWS le compte, auquel appartient l'utilisateur, possède la ressource de la zone d'atterrissage.
- Si vous créez un IAM rôle dans votre AWS compte autorisé à configurer une zone d'atterrissage, toute personne pouvant assumer ce rôle peut configurer une zone d'atterrissage. Votre AWS le 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 traite de l'utilisation IAM dans le contexte de AWS Control Tower. Il ne fournit pas d'informations détaillées sur le IAM service. Pour une IAM documentation complète, voir [Qu'est-ce que c'est IAM ?](#) dans le guide de IAM l'utilisateur. Pour plus d'informations sur IAM la syntaxe et les descriptions des politiques, voir [AWS IAMRéférence](#) à la politique dans le guide de IAM l'utilisateur.

Les politiques associées à une IAM identité sont appelées politiques basées sur l'identité (IAMpolitiques). Les stratégies attachées à une ressource sont appelées stratégies basées sur une ressource.

Note

AWSControl Tower ne prend en charge que les politiques basées sur l'identité (IAMpolitiques).

Rubriques

- [À propos des politiques basées sur l'identité \(politiques\) IAM](#)
- [Création de rôles et attribution d'autorisations](#)
- [Politiques basées sur les ressources](#)

À propos des politiques basées sur l'identité (politiques) IAM

Vous pouvez associer des politiques aux IAM identités. 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.

- Associer une politique d'autorisations à un rôle (accorder des autorisations entre comptes) : vous pouvez associer une politique d'autorisations basée sur l'identité à un IAM rôle pour accorder des autorisations entre comptes. Par exemple, un administrateur pour un AWS le 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 IAM rôle 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 octroyer 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 [section Créer un ensemble d'autorisations](#) dans le AWS IAM Identity Center Guide de l'utilisateur.

- Utilisateurs gérés IAM via un fournisseur d'identité :


Créez un rôle pour la fédération d'identité. Suivez les instructions de la [section Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) dans le guide de IAM l'utilisateur.

- IAMutilisateurs :

- Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la section [Création d'un rôle pour un IAM utilisateur](#) dans le Guide de IAM l'utilisateur.

- (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la [section Ajouter des autorisations à un utilisateur \(console\)](#) dans le guide de IAM l'utilisateur.

Pour plus d'informations sur l'utilisation IAM pour déléguer des autorisations, consultez la section [Gestion des accès](#) dans le guide de IAM l'utilisateur.

 Note


Lors de la configuration d'une zone de landing zone AWS Control Tower, vous aurez besoin d'un utilisateur ou d'un rôle doté de la politique AdministratorAccess gérée. (arn:aws:iam : :aws:policy/) AdministratorAccess

Pour créer un rôle pour un Service AWS (IAMconsole)

1. Connectez-vous au AWS Management Console et ouvrez la IAM console à l'adresse <https://console.aws.amazon.com/iam/>.
2. Dans le volet de navigation de la IAM console, sélectionnez Rôles, puis sélectionnez Créer un rôle.
3. Pour Type d'entité de confiance, sélectionnez 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 associez 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 AWS politiques 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 dans votre Compte AWS, et ne peut pas être rendu unique au cas par cas.

Par exemple, ne créez pas de rôles nommés à la fois **PRODRÔLE** et **prodrole**.

Lorsqu'un nom de rôle est utilisé dans une politique ou dans le cadre d'une politiqueARN, le nom du rôle 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 distingue pas les 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 balisesIAM, consultez les [IAMressources relatives au balisage](#) dans le guide de l'IAMutilisateur.
13. Passez en revue les informations du rôle, puis choisissez Create role (Créer un rôle).

Pour utiliser l'éditeur JSON de stratégie pour créer une stratégie

1. Connectez-vous au AWS Management Console et ouvrez la IAM console à l'adresse <https://console.aws.amazon.com/iam/>.
2. Dans le panneau de navigation de gauche, sélectionnez Politiques (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'JSONoption.
5. Entrez ou collez un document JSON de politique. Pour plus de détails sur le langage IAM de la politique, voir [IAMJSONla référence des politiques](#).
6. Résolez les avertissements de sécurité, les erreurs ou les avertissements généraux générés durant la [validation de la politique](#), puis choisissez Suivant.

 Note

Vous pouvez basculer entre les options Visual et celles de JSONl'éditeur à tout moment. Toutefois, si vous apportez des modifications ou si vous choisissez Suivant dans l'éditeur visuel, vous IAM pouvez restructurer votre politique afin de l'optimiser pour l'éditeur visuel. Pour plus d'informations, consultez la section [Restructuration des politiques](#) dans le guide de IAM l'utilisateur.

7. (Facultatif) Lorsque vous créez ou modifiez une politique dans AWS Management Console, vous pouvez générer un modèle de YAML politique JSON ou de stratégie que vous pouvez utiliser dans AWS CloudFormation modèles.

Pour ce faire, dans l'éditeur de politiques, sélectionnez Actions, puis sélectionnez Générer CloudFormation un modèle. En savoir plus sur AWS CloudFormation, voir [AWS Identity and Access Management référence au type de ressource](#) dans le AWS CloudFormation Guide de 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 balisesIAM, consultez les [IAMressources relatives au balisage](#) dans le guide de l'IAMutilisateur.
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 au AWS Management Console et ouvrez la IAM console à l'adresse <https://console.aws.amazon.com/iam/>.

2. Dans le panneau de navigation de gauche, sélectionnez Politiques (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. Choisissez Create Policy (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 champ de recherche en haut 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). Les [IAMrefus étant par défaut](#), nous vous recommandons, comme bonne pratique de sécurité, de n'autoriser les autorisations que pour les actions et les ressources dont un utilisateur a besoin. Créez une JSON déclaration pour refuser les autorisations uniquement si vous souhaitez annuler 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 ARNs pour spécifier les ressources par leur nom de ressource Amazon (ARN). Vous pouvez utiliser l'ARN éditeur visuel ou la liste ARNs manuellement. Pour plus d'informations sur ARN la syntaxe, consultez [Amazon Resource Names \(ARNs\)](#) dans le guide de IAM l'utilisateur. Pour plus d'informations sur ARNs l'utilisation de l'élément d'une politique, voir [Éléments IAM JSON de stratégie : ressource](#) dans le guide de IAM l'utilisateur.
 - 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. Les conditions limitent l'effet d'une déclaration de JSON politique. 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, voir [Actions, ressources et clés de condition pour 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 IAM JSON de politique : Condition](#) dans le guide de IAM l'utilisateur.

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 entre les options Visual et celles de JSON l'éditeur à tout moment. Toutefois, si vous apportez des modifications ou si vous choisissez Suivant dans l'éditeur visuel, vous IAM pouvez restructurer votre politique afin de l'optimiser pour l'éditeur visuel. Pour plus d'informations, consultez la section [Restructuration des politiques](#) dans le guide de IAM l'utilisateur.

9. (Facultatif) Lorsque vous créez ou modifiez une politique dans AWS Management Console, vous pouvez générer un modèle de YAML politique JSON ou de stratégie que vous pouvez utiliser dans AWS CloudFormation modèles.

Pour ce faire, dans l'éditeur de politiques, sélectionnez Actions, puis sélectionnez Générer CloudFormation un modèle. En savoir plus sur AWS CloudFormation, voir [AWS Identity and Access Management référence au type de ressource](#) dans le AWS CloudFormation Guide de 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 IAM, consultez les [IAM ressources relatives au balisage](#) dans le guide de l'IAM utilisateur.
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 en dehors de l'AWS Management Console. La manière d'accorder un accès programmatique dépend du type d'utilisateur qui accède à 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 au AWS CLI, AWS SDKs, ou AWS APIs.	Suivez les instructions de l'interface que vous souhaitez utiliser. <ul style="list-style-type: none"> • Pour AWS CLI, voir Configuration du AWS CLI à utiliser AWS IAM Identity Center dans le <i>.AWS Command Line Interface Guide de l'utilisateur</i>. • Dans AWS SDKs, des outils et AWS APIs, voir Authentification du centre d'IAM identité dans le <i>AWS SDKset Guide de référence des outils</i>.
IAM	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées au AWS CLI, AWS SDKs, ou AWS APIs.	En suivant les instructions de la section Utilisation d'informations d'identification temporaires avec AWS ressources du guide de IAM l'utilisateur.
IAM	(Non recommandé) Utilisez des informations d'identification à long terme pour signer les demandes programmatiques adressées	Suivez les instructions de l'interface que vous souhaitez utiliser.

Quel utilisateur a besoin d'un accès programmatique ?	Pour	Par
	<p>au AWS CLI, AWS SDKs, ou AWS APIs.</p>	<ul style="list-style-type: none"> • Pour AWS CLI, voir Authentification à l'aide des informations IAM d'identification utilisateur dans le AWS Command Line Interface Guide de l'utilisateur. • Dans AWS SDKset outils, voir Authentification à l'aide d'informations d'identification à long terme dans le AWS SDKset Guide de référence des outils. • Dans AWS APIs, voir Gestion des clés d'accès pour IAM les utilisateurs dans le Guide de IAM l'utilisateur.

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 AWS principes de service, voir [Conditions facultatives relatives à vos relations de confiance](#). 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 également [Spécification 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 plus d'informations sur les utilisateurs, les groupes, les rôles et les autorisations, consultez la section [Identités \(utilisateurs, groupes et rôles\)](#) dans le guide de IAM l'utilisateur.

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. AWSControl 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 par le biais de la console AWS Control Tower ou de [la zone d'atterrissage APIs](#). Pour configurer votre zone de landing zone, vous devez être un IAM utilisateur disposant des autorisations administratives définies dans une IAM politique.

Les éléments suivants sont les plus élémentaires que vous pouvez identifier dans une politique :

- Ressource : dans une politique, vous utilisez un nom de ressource Amazon (ARN) pour identifier la ressource à laquelle la politique s'applique. Pour de plus amples informations, veuillez consulter [AWSRessources et opérations de la 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 (IAMpolitiques), 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). AWSControl Tower ne prend pas en charge les politiques basées sur les ressources.

Pour en savoir plus sur IAM la syntaxe et les descriptions des politiques, voir [AWS IAMRéférence](#) à la politique dans le guide de IAM l'utilisateur.

Spécification de conditions dans une politique

Lorsque vous accordez des autorisations, vous pouvez utiliser le langage de IAM politique pour spécifier les conditions dans lesquelles une politique doit entrer en vigueur. 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, voir [Condition](#) dans le guide de IAM l'utilisateur.

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 AWS-des clés de condition que vous pouvez utiliser le cas échéant. Pour une liste complète des AWS-touches, voir [Clés disponibles pour les conditions](#) dans le guide de IAM l'utilisateur.

Empêchez l'usurpation d'identité entre services

Entrée AWS, l'usurpation d'identité interservices peut créer de la confusion chez les 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 que 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'identifiant du compte, comme celui 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 aux ressources AWS de votre 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 ControlTowerServiceRolePolicy est 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 stacks 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 tableau [Politiques 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. CloudTrail assume 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 être `AWSControlTowerBlueprintAccess`.

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 `AWSServiceCatalogAdminFullAccess` au 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 tableau [Politiques 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	<p>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.</p> <p>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</p>	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	<p>AWS Control Tower a ajouté de nouvelles autorisations qui permettent à AWS Control Tower de passer des appels vers <code>EnableRegionListRegions</code>, et des <code>GetRegionOptStatus</code> 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).</p> <p>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.</p>	6 avril 2023

Modification	Description	Date
AWS ControlTowerServiceRolePolicy – Mise à jour d'une politique existante	<p>AWS Control Tower a ajouté de nouvelles autorisations qui permettent à AWS Control Tower d'assumer le <code>AWSControlTowerBlueprintAccess</code> 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 <code>AWSControlTowerBlueprintAccess</code> 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.</p> <p>Cette modification est nécessaire pour que les clients puissent créer des comptes personnalisés via AWS Control Tower Account Factory.</p>	28 octobre 2022

Modification	Description	Date
AWS ControlTowerServiceRolePolicy – Mise à jour d'une politique existante	<p>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.</p> <p>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.</p>	20 juin 2022

Modification	Description	Date
AWS ControlTowerServiceRolePolicy – Mise à jour d'une politique existante	<p>AWS Control Tower a ajouté de nouvelles autorisations qui permettent aux clients d'utiliser le chiffrement par clé KMS.</p> <p>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.</p>	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 conformité AWS](#). Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Control Tower, consultez [AWS Services in Scope by Compliance Program](#).
- 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 AWS de 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 AWS de votre 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 la section [Confidentialité des données FAQ](#). Pour plus d'informations sur la protection des données en Europe, consultez le [modèle de responsabilité AWS partagée et le billet de GDPR blog sur le blog sur la AWS sécurité](#).

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) pour chaque compte.
- Utilisez SSL/TLS pour communiquer avec les AWS ressources. Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Configuration API et journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section [Utilisation des CloudTrail sentiers](#) dans le guide de AWS CloudTrail l'utilisateur.
- 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 FIPS 140 à 3 modules cryptographiques validés pour accéder AWS via une interface de ligne de commande ou un API, utilisez un point de terminaison. FIPS Pour plus d'informations sur les FIPS points de terminaison disponibles, voir [Federal Information Processing Standard \(FIPS\) 140-3](#).

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 Nom. Cela inclut lorsque vous travaillez avec AWS Control Tower ou un autre utilisateur Services AWS à l'aide de la console API, AWS CLI, ou AWS SDKs. 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 un URL à un serveur externe, nous vous recommandons vivement de ne pas inclure d'informations d'identification dans le URL afin de valider votre demande auprès de ce serveur.

 Note

L'enregistrement des activités des utilisateurs AWS CloudTrail est géré automatiquement dans AWS Control Tower lorsque vous configurez votre zone de landing zone.

Pour plus d'informations sur la protection des données, consultez le [modèle de responsabilitéAWS partagée](#) et le billet de GDPR blog sur le blog sur la AWS sécurité. AWSControl Tower propose les options suivantes que vous pouvez utiliser pour sécuriser le contenu existant dans votre zone de landing zone :

Rubriques

- [Chiffrement au repos](#)
- [Chiffrement en transit](#)
- [Restreindre l'accès au contenu](#)

Chiffrement au repos

AWSControl Tower utilise des compartiments Amazon S3 et des bases de données Amazon DynamoDB qui sont chiffrés au repos à l'aide de SSE clés gérées par Amazon S3 (-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 KMS chiffrement. 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

AWSControl Tower utilise Transport Layer Security (TLS) et le chiffrement côté client pour le chiffrement en transit afin de soutenir votre zone de landing zone. En outre, l'accès à AWS Control Tower nécessite l'utilisation de la console, qui n'est accessible que via un HTTPS point de terminaison. 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 IAM autorisations appropriées ou, dans le cas des utilisateurs d'IAMIdentity Center, qu'ils appartiennent aux bons groupes.

- Pour plus d'informations sur les rôles et les politiques des IAM entités, consultez le [Guide de IAM l'utilisateur](#).

- Pour plus d'informations sur les groupes IAM Identity Center créés lorsque vous configurez votre zone de landing zone, consultez [Groupes de centres d'identité IAM pour AWS Control Tower](#).

Validation de conformité pour AWS Control Tower

AWSControl Tower est un service bien conçu qui peut aider votre entreprise à répondre à ses besoins de conformité grâce à des contrôles et aux meilleures 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 SOC PCI notamment de RAMP la Fed 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 HIPAA sécurité et la conformité sur Amazon Web Services](#) : ce livre blanc décrit comment les entreprises peuvent AWS créer HIPAA des applications conformes.
- [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 une liste des Régions AWS endroits où AWS Control Tower est disponible, consultez [Comment AWS les régions travaillent 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

AWSControl 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 les API appels 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 également prendre en charge les suites de chiffrement parfaitement confidentielles (), telles que Ephemeral Diffie-Hellman (PFS) ou Elliptic Curve Ephemeral Diffie-Hellman (DHE). 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 identifiant de clé d'accès et d'une clé d'accès secrète associés à un IAM principal. 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 les charges de travail de la zone d'atterrissage de la AWS Control Tower. Pour de plus

amples informations, veuillez consulter [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 Activités 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: AWSS3BucketPermissionsCheck
  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: AWSS3BucketDeliveryForConfig
  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: AWSS3BucketDeliveryForOrganizationTrail
  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 CloudTrail capture 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 CloudTrail un 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 de AWS 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 de suivi 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 :

- [Vue d'ensemble 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

- Pour obtenir la liste complète des API publiques d'AWS Control Tower et des informations détaillées sur chacune d'entre elles, consultez [The AWS Control Tower API Reference](#). Les appels à ces API publiques sont enregistrés par AWS CloudTrail.

Autres API

- SetupLandingZone
- UpdateAccountFactoryConfig
- ManageOrganizationalUnit
- CreateManagedAccount
- 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 l'élément [CloudTrail UserIdentity](#).

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 Config à 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, consultez [La 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 considère 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 `UpdateManagedAccount` pour rechercher les événements du cycle de vie `CreateManagedAccount` ainsi 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 nommé `CreateManagedAccount`.

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'Amazon CloudWatch événements.

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 CloudTrail événement 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": "XXXXXXXXXX",
      "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": "00000000-0000-0000-1111-123456789012",
    "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 `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
  "time": "2018-08-30T21:42:18Z", // Event time from
  "region": "us-east-1", // Management account
  "resources": [ ],
  "detail": {
    "eventVersion": "1.05",
    "userIdentity": {
      "accountId": "XXXXXXXXXXXX", // Management-account
      "invokedBy": "AWS Internal"
    },
    "eventTime": "2018-08-30T21:42:18Z", // Timestamp when call
    "eventSource": "controltower.amazonaws.com",
    "eventName": "SetupLandingZone",
    "awsRegion": "us-east-1", // AWS Control Tower
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "eventID": "CloudTrail_event_ID", // This value is
    "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

lerootOrganizationalId, 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.",

```



```
"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" :
          {
```



```
"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 aux AWS 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 Chatbot](#) chat ou par notification push [via l'application mobile pour AWS 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 souhaitez 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](#)
- [Procédure pas à pas : Automatisez le provisionnement des comptes dans AWS Control Tower par les API Service Catalog](#)
- [Procédure pas à pas : configurer AWS Control Tower sans VPC](#)
- [Gérer les ressources d'AWS Control Tower](#)
- [Procédure pas à pas : configurer des groupes de sécurité dans AWS Control Tower avec AWS Firewall Manager](#)
- [Procédure pas à pas : mise hors service d'une zone d'atterrissage d'une AWS Control Tower](#)

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 commande (CLI) de AWS 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'ProvisionProductAPI 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-a8hb8m18)"
},
{
  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](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 `standardOrganizationsFullAccessRole`.
 - 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 nommé `AWSControlTowerBP-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, appelée `AWSControlTowerManagedRule`. 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 dans [Gérer 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 souhaitez 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/](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](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](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/](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/](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/](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 `AWSServiceCatalogEndUserAccess` et 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 `AWSServiceCatalogEndUserAccess`.
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 déléguer 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 souhaitez 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 souhaitez 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, appelée `AWSControlTowerManagedRule`, des comptes partagés et membres de toutes les régions gouvernées. `AWSControlTowerManagedRule` est 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 souhaitez 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 souhaitez 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, appelée `AWSControlTowerManagedRule`, 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, consultez [Comment AWS les régions travaillent 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 `AWSControlTowerAdmins` groupe. 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 VPC AWS 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 VPC AWS 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 si 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-dpqqfywxxx
```

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 [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-xxxxxxx, 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, consultez [Quand mettre à jour AWS Control Tower OUs et ses comptes](#).

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'`EnableBaselineAPI` 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'EnableBaselineAPI 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 `ResetEnabledBaselineAPI`, 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 `ResetEnabledBaselineAPI` 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'`EnableBaselineAPI` 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'`DisableBaselineAPI` 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 `EnableBaselineAPI` 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'UpdateEnabledBaselineAPI 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-identifiant <AWSControlTowerBaseline ARN>
--baseline-version <BASELINE VERSION> --target-identifiant <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-identifiant <AWSControlTowerBaseline ARN>
--baseline-version <BASELINE VERSION> --target-identifiant <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-
identifiant <EnabledBaselineArn>
```

Exemples d'API utilisation de base

Cette section contient des exemples de paramètres d'entrée et de sortie pour la ligne de base de AWS Control Tower APIs.

DisableBaseline

Pour plus d'informations sur cette API opération, consultez [DisableBaseline](#).

DisableBaselineentrée :

```
{
  "enabledBaselineIdentifiant": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789"
}
```

DisableBaselinesortie :

```
{
  "operationIdentifiant": "58f12232-26be-4735-a3e9-dd30d90f021f"
}
```

DisableBaselineCLlexemple :

```
aws controltower disable-baseline \
  --enabled-baseline-identifiant arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789 \
  --region us-west-2
```

EnableBaseline

Pour plus d'informations sur cette API opération, consultez [EnableBaseline](#).

EnableBaselineentrée :

```
{
```

```

    "baselineIdentifiant": "arn:aws:controltower:us-west-2::baseline:17BSJV3IGJ2QSGA2",
    "targetIdentifiant": "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/
XAHCR4CJTISI4W07MZ"
      }
    ]
  }
}

```

EnableBaselinesortie, renvoyant une nouvelle ressource :

```

{
  "operationIdentifiant": "58f12232-26be-4735-a3e9-dd30d90f021f",
  "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAGF7TNOHRD7ES5VV"
}

```

EnableBaselineCLlexemple :

Cet exemple montre l'activation d'une ligne de base pour un AWS Organizations organisation dont la zone d'atterrissage a opté pour AWS IAMAccès à l'Identity Center, géré par AWS Control Tower. Pour récupérer votre EnabledBaseline identifiant Identity Center, vous pouvez appeler le ListEnabledBaselines API filtrage sur la ligne de base Identity Center : (arn:aws:controltower:*Region*::baseline/LN25R72TTG6IGPTQ)

```

aws controltower list-enabled-baselines \
  --filter baselineIdentifiants=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",

```



```

        "baselineIdentifiant": "arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ",
        "targetIdentifiant": "arn:aws:organizations::123456789012:account/o-
aq21sw43de5/123456789012",
        "statusSummary": {
            "status": "SUCCEEDED"
        }
    }
]
}

```

Note

Notez la ARN valeur de la réponse et transmettez-la en tant que paramètre pour activer la ligne de base par défaut.

```

aws controltower enable-baseline \
  --baseline-identifiant arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
  --baseline-version 3.0 \
  --target-identifiant arn:aws:organizations::123456789012:ou/o-aq21sw43de5/ou-po90-
1k87jh65 \
  --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 a choisi de ne pas participer à la gestion d'IAM Identity Center par AWS Control Tower, activez la base de référence sans le paramètre.

```

aws controltower enable-baseline \
  --baseline-identifiant arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
  --baseline-version 3.0 \
  --target-identifiant arn:aws:organizations::123456789012:ou/o-aq21sw43de5/ou-po90-
1k87jh65 \
  --region us-west-2

```

GetBaseline

Pour plus d'informations sur cette API opération, consultez [GetBaseline](#).

GetBaselineentrée :

```
{
  "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2"
}
```

GetBaselinesortie :

```
{
  "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.",
}
```

GetBaselineCLexemple :

```
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 API opération, consultez [GetBaselineOperation](#).

GetBaselineOperationentrée :

```
{
  "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
}
```

GetBaselineOperationsortie :

```
{
  "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"
  }
}
```

GetBaselineOperationCLlexemple :

```
aws controltower get-baseline-operation \
  --operation-identifider 58f12232-26be-4735-a3e9-dd30d90f021f \
  --region us-west-2
```

GetEnabledBaseline

Pour plus d'informations sur cette API opération, consultez [GetEnabledBaseline](#).

GetEnabledBaselineentrée :

```
{
  "enabledBaselineIdentifider": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHCR4CJTISI4W07MZ"
}
```

GetEnabledBaselinesortie :

```
{
  "enabledBaselineDetails": {
    "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTISI4W07MZ",
    "baselineIdentifider": "arn:aws:controltower:us-
west-2::baseline:17BSJV3IGJ2QSGA2",
    "baselineVersion": "3.0",
    "targetIdentifider": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/ou-
r9mj-4j3mzjql",
    "statusSummary": {
      "status": "SUCCEEDED",
      "lastOperationIdentifider": "58f12232-26be-4735-a3e9-dd30d90f021f"
    },
    "parameters": [
      {
        "key": "IdentityCenterEnabledBaselineArn",
        "value": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTISI4W07MZ"
      }
    ]
  }
}
```

```
    }
  ]
}
}
```

GetEnabledBaselineCLlexemple :

```
aws controltower get-enabled-baseline \
  --enabled-baseline-identifiant arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
  --region us-west-2
```

ListBaselines

Pour plus d'informations sur cette API opération, consultez [ListBaselines](#).

ListBaselinesentrée (en utilisant des entrées optionnelles) :

```
{
  "nextToken": "AbCd1234",
  "maxResults": "4"
}
```

ListBaselines sortie :

```
{
  "baselines": [
    {
      "arn": "arn:aws:controltower:us-west-1::baseline/4T4HA1KM010S6311",
      "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."
    }
]
}

```

ListBaselinesCLlexemple :

```

aws controltower list-baselines \
  --region us-west-2

```

ListEnabledBaselines

Pour plus d'informations sur cette API opération, consultez [ListEnabledBaselines](#).

ListEnabledBaselinesentrée (pas de filtres) :

```

{
  "nextToken": "bde7-XX0c6fXXXXXX",
  "maxResults": 5
}

```

ListEnabledBaselinesentrée (baselineIdentifiersfiltre uniquement) :

```

{
  "filter": {
    "baselineIdentifiers": ['arn:aws:controltower:us-
    east-1::baseline/17BSJV3IGJ2QSGA2', 'arn:aws:controltower:us-
    east-1::baseline/12GZU8CKZKVMS2AW']
  },
  "nextToken": "bde7-XX0c6fXXXXXX",
  "maxResults": 5
}

```

ListEnabledBaselinesentrée (targetIdentifiersfiltre 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
}
```

ListEnabledBaselinesentrée (baselineIdentifierset 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
}
```

ListEnabledBaselinessortie :

```
{
  "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-kgj0txdhp/ou-r9mj-4j3mzjq1",
      "statusSummary": {
        "status": "SUCCEEDED",
        "lastOperationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
      }
    },
    {
      "arn": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/XAJ9NKW88AA4W9CLL",

```

```

        "baselineIdentifiant": "arn:aws:controltower:us-
east-1::baseline:17BSJV3IGJ2QSGA2",
        "baselineVersion": "4.0",
        "targetIdentifiant": "arn:aws:organizations::123456789012:ou/o-s9511vn103/
ou-xqj7-fex1u317",
        "statusSummary": {
          "status": "FAILED",
          "lastOperationIdentifiant": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
        }
      }
    ],
    "nextToken": "e2bXXXXX6cab"
  }

```

CLlexemple avec un type de filtre (baselineIdentifiersfiltre) :

```

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

```

CLlexemple d'utilisation de plusieurs filtres (baselineIdentifierset 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 API opération, consultez [ResetEnabledBaseline](#).

ResetEnabledbaselineentrée :

```

{
  "enabledBaselineIdentifiant": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAJ9NKW88AA4W9CLL "
}

```

ResetEnabledBaselinesortie :

```
{
  "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

ResetEnabledBaselineCLlexemple :

```
aws controltower reset-enabled-baseline \
  --enabled-baseline-identifrier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
  --region us-west-2
```

UpdateEnabledBaseline

Pour plus d'informations sur cette API opération, consultez [UpdateEnabledBaseline](#).

UpdateEnabledBaselineentrée :

```
{
  "enabledBaselineIdentifrier": "arn:aws:controltower:us-
east-1:123456789012:enabledbaseline/XAJ9NKW88AA4W9CLL",
  "baselineVersion": "4.0",
  "parameters": [
    {
      "key": "IdentityCenterEnabledBaselineArn",
      "value": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAHCR4CJTISI4W07MZ"
    }
  ]
}
```

UpdateEnabledBaselinesortie :

```
{
  "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

UpdateEnabledBaselineCLlexemple :

```
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 supplémentaires et liens

Cette rubrique inclut des liens vers des articles de blog pertinents, de la documentation technique et des informations connexes qui peuvent vous aider dans votre travail avec AWS Control Tower. Les sources présentent certains cas d'utilisation courants et les meilleures pratiques relatives aux fonctionnalités de AWS Control Tower, ainsi que certaines améliorations supplémentaires.

Tutoriels et ateliers

- [AWSControl Tower lab](#) — Ces ateliers fournissent une vue d'ensemble détaillée des tâches courantes liées à AWS Control Tower.
- Sur le tableau de bord de 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.
- Essayez de consulter [une liste de YouTube vidéos](#) qui expliquent en détail comment utiliser les fonctionnalités AWS de 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 VPCArchitecture 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.
- [Le self-service VPCs dans AWS Control Tower à l'aide de AWS Service Catalog](#) — Ce billet de blog décrit comment configurer Account Factory afin que vous puissiez approvisionner des comptes personnalisésVPCs.
- [Implémentation de 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 AWS de 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

- [Automatiser les AWS Security Hub alertes avec les événements du cycle de vie de la 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 IAM d'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 de AWS Systems Manager et de 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 de AWS 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 enregistrer un AWS compte existant dans AWS Control Tower.
- [Créez un compte auprès AWS de Control Tower](#) — Ce billet de blog explique comment déployer AWS Control Tower dans vos AWS organisations existantes.
- [Étendez la gouvernance de 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 les comptes et les organisations existants à être gérés 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 SNS notifications 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 VPC flux Amazon](#) — Ce billet de blog explique comment automatiser et centraliser Amazon VPC Flow Logs dans un environnement multi-comptes.

- [Automatisez le VPC balisage à l'aide des événements du cycle de vie de AWS Control Tower](#) : ce billet de blog explique comment automatiser le balisage des VPCs ressources 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 des charges de travail.

- [CloudEndure migration](#) — Ce billet de blog explique comment combiner CloudEndure d'autres AWS services avec AWS Control Tower pour faciliter la migration des charges de travail.

Services AWS connexes

AWSControl Tower agit comme une couche d'orchestration pour AWS Organizations. Par conséquent, grâce à la console AWS OrganizationsAPIs, vous avez accès à plus de 20 autres AWS services qui fonctionnent avec AWS Control Tower. Ces services supplémentaires ne sont pas accessibles directement via la console AWS Control Tower.

- Pour une liste complète des services mis à la disposition de AWS Control Tower par le biais de AWS Organizations, consultez [AWSles services que vous pouvez utiliser avec AWS Organizations](#).
- Pour activer les fonctionnalités multi-comptes pour ces AWS services connexes, vous devez activer l'accès sécurisé. Pour plus d'informations, consultez [Using AWS Organizations with other AWS services](#).

Note

N'oubliez pas qu' AWS IAMIdentity Center et qu' AWS CloudTrail ils sont entièrement intégrés dans AWS Control Tower et sont entièrement intégrés. AWS Config II n'est pas nécessaire de modifier vos paramètres d'accès sécurisé ou d'administration déléguée pour ces services.

- Certains AWS services disponibles via 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, [Configurer des groupes de sécurité avec AWS Firewall Manager](#).

AWS Marketplace solutions

Découvrez les solutions de AWS Marketplace.

- [AWSControl 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, les informations de sécurité et la gestion des événements (SIEM).

AWS Notes de mise à jour de Control Tower

Les sections suivantes présentent des informations détaillées sur les versions de AWS Control Tower qui nécessitent une mise à jour pour une zone d'atterrissage de AWS Control Tower, ainsi que sur les versions intégrées automatiquement 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 le [Historique 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 :

- [AWSControl Tower prend en charge jusqu'à 1 000 comptes par unité d'organisation](#)
- [AWSControl Tower ajoute une sélection de versions pour les zones d'atterrissage](#)
- [Contrôle descriptif API disponible, accès étendu aux régions et aux contrôles](#)
- [AWSControl Tower soutient AFT et CfCT dans les régions optionnelles](#)
- [AWSControl Tower ajoute le ListLandingZoneOperations API](#)
- [AWSControl Tower prend en charge jusqu'à 100 opérations de contrôle simultanées](#)
- [AWSControl Tower disponible en AWS Canada Ouest \(Calgary\)](#)
- [AWSControl Tower prend en charge les ajustements de quotas en libre-service](#)
- [AWSControl Tower publie le guide de référence sur les contrôles](#)

- [AWSControl Tower met à jour et renomme deux contrôles proactifs](#)
- [Les contrôles obsolètes ne sont plus disponibles](#)
- [AWSControl Tower prend en charge le balisage des `EnabledControl` ressources dans AWS CloudFormation](#)
- [AWSControl Tower prend en charge APIs l'enregistrement et la configuration des unités d'organisation avec des lignes de base](#)

AWSControl Tower prend en charge jusqu'à 1 000 comptes par unité d'organisation

30 août 2024

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl Tower a augmenté le nombre maximum de comptes autorisés par unité organisationnelle (UO) de 300 à 1 000. Vous pouvez désormais inscrire jusqu'à 1 000 Comptes AWS dans la gouvernance AWS de la Control Tower en une seule fois, sans modifier la structure de votre unité d'organisation. Les processus d'enregistrement et de réenregistrement des unités d'organisation sont également plus efficaces et nécessitent beaucoup moins de temps pour déployer les ressources de base de AWS Control Tower sur vos comptes.

Certaines limites du compte s'appliquent toujours en raison de la limitation du nombre de AWS CloudFormation ensembles de piles disponibles. Plus précisément, le nombre maximum de comptes que vous pouvez inscrire dans une unité d'organisation peut varier en fonction du nombre de régions que vous gérez. Pour en savoir plus, consultez [Limitations basées sur le sous-jacent AWS services décrits](#) dans le [guide de l'utilisateur de AWS Control Tower](#). Pour une liste complète des Régions AWS où AWS Control Tower est disponible, consultez le [Région AWS Tableau](#).

AWSControl Tower ajoute une sélection de versions pour les zones d'atterrissage

15 août 2024

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

Si vous utilisez la version 3.1 ou supérieure de AWS Control Tower landing zone, vous pouvez mettre à jour ou réparer votre zone d'atterrissage sur place dans la version actuelle, ou vous pouvez

passer à la version de votre choix. Auparavant, toute mise à jour ou réparation de zone d'atterrissage nécessitait une mise à niveau vers la dernière version de la zone d'atterrissage.

Grâce à la sélection des versions dans la zone de landing zone, vous disposez d'une plus grande flexibilité pour planifier les mises à niveau des versions tout en évaluant les modifications potentielles de votre environnement. Vous n'avez pas à choisir entre réparer la dérive pour rester en conformité, mettre à jour les configurations de votre zone d'atterrissage ou passer à la dernière version de la zone d'atterrissage. Si vous utilisez la version 3.1 ou supérieure de la zone d'atterrissage, vous pouvez choisir de conserver la version actuelle ou de passer à une version plus récente lorsque vous mettez à jour ou réinitialisez les configurations de votre zone d'atterrissage.

Contrôle descriptif API disponible, accès étendu aux régions et aux contrôles

6 août 2024

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl Tower a ajouté deux nouvelles API opérations qui vous aident à trouver plus d'informations sur les commandes disponibles, par programmation. Cette fonctionnalité facilite le déploiement des contrôles grâce à l'automatisation.

- [GetControl](#) API Renvoie des informations sur un contrôle activé, notamment l'identifiant de la cible, un résumé des informations de contrôle, une liste des régions cibles et l'état de dérive.
- [ListControls](#) API Renvoie une liste paginée de tous les contrôles disponibles dans la bibliothèque de contrôles AWS Control Tower.

Ils APIs sont accessibles par le biais du [AWS Espace de noms](#) Control Catalog. Le AWS Control Catalog fait partie de AWS Control Tower, qui inclut des commandes qui vous aident à gérer les autres AWS des services, pas seulement AWS Control Tower. Ce catalogue étendu consolide les contrôles de plusieurs AWS services, afin que vous puissiez voir AWS contrôles en fonction de certains cas d'utilisation courants, tels que : la sécurité, le coût, la durabilité et les opérations. Pour plus d'informations, consultez [la API référence du catalogue de contrôle](#).

Disponibilité régionale étendue

À partir de cette version, vous pouvez étendre la gouvernance AWS de la Control Tower à Régions AWS où certaines de vos commandes (déjà) activées ne sont pas disponibles. En outre, vous pouvez

désormais activer certains contrôles dans un plus grand nombre de régions, même si le contrôle n'est pas pris en charge dans toutes les régions que vous gérez.

Auparavant, AWS Control Tower vous empêchait d'étendre la gouvernance aux régions ou d'activer les contrôles, alors qu'elle n'assurait pas la cohérence entre tous vos contrôles activés et régions gouvernées. Avec cette version, vous disposez d'une plus grande flexibilité et d'une plus grande responsabilité pour vous assurer que votre configuration est correcte pour tous les contrôles activés et toutes les régions gouvernées. La [AWScommande Control Tower APIs](#) et le [catalogue de commandes APIs](#) peuvent vous aider à obtenir des informations sur AWS Les régions dans lesquelles vous êtes protégé par des contrôles activés et les régions dans lesquelles des contrôles supplémentaires peuvent être déployés. Les informations de région et de contrôle sont également disponibles dans la console AWS Control Tower.

AWSControl Tower soutient AFT et CfCT dans les régions optionnelles

18 juillet 2024

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

Aujourd'hui, les frameworks de personnalisation de AWS Control Tower Account Factory for Terraform (AFT) et Customizations for AWS Control Tower (CfCT) sont disponibles en cinq versions supplémentaires Régions AWS: Asie-Pacifique (Hyderabad, Jakarta et Osaka), Israël (Tel Aviv) et Moyen-Orient (UAE).

Account Factory for Terraform (AFT) met en place un pipeline Terraform pour vous aider à approvisionner et à personnaliser des comptes dans Control Tower. AWS Customizations for AWS Control Tower (CfCT) vous permet de personnaliser votre zone d'atterrissage et vos comptes AWS Control Tower avec AWS CloudFormation modèles et politiques de contrôle des services (SCPs).

Pour en savoir plus, consultez les pages Account Factory pour Terraform et Customizations for AWS Control Tower ; consultez le guide de l'utilisateur de AWS Control Tower. Vous pouvez également consulter les notes de publication sur les pages AFT Github et CfCT Github. AFTet CfCT sont pris en charge dans tous AWS Régions, à quelques exceptions près. Pour plus de détails, consultez [la section Limitations régionales](#).

AWSControl Tower ajoute le **ListLandingZoneOperations** API

26 juin 2024

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl Tower a ajouté un API qui vous permet de récupérer une liste des opérations récemment appliquées à votre zone d'atterrissage et des opérations en cours. Ils API peuvent afficher l'historique des opérations de la zone d'atterrissage et leurs identifiants pendant une période maximale de 90 jours. Pour des exemples d'utilisation, voir [Afficher le statut des opérations de votre zone d'atterrissage](#).

Pour plus d'informations à ce sujet `ListLandingZoneOperationsAPI`, consultez [ListLandingZoneOperations](#) le AWSControl Tower API Reference.

AWSControl Tower prend en charge jusqu'à 100 opérations de contrôle simultanées

20 mai 2024

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl Tower prend désormais en charge plusieurs opérations de contrôle avec une plus grande simultanéité. Vous pouvez soumettre jusqu'à 100 AWS opérations de contrôle de la Control Tower, dans plusieurs unités organisationnelles (OUs), en même temps, depuis la console ou avec APIs. 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 suivre l'état de vos opérations de contrôle en cours et en file d'attente, vous pouvez accéder à la nouvelle page des opérations récentes de la console AWS Control Tower, ou vous pouvez appeler la nouvelle. [ListControlOperationsAPI](#)

La bibliothèque AWS Control Tower contient plus de 500 contrôles, qui correspondent à différents objectifs, cadres 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.

AWSControl Tower disponible en AWS Canada Ouest (Calgary)

3 mai 2024

(Aucune mise à jour requise pour la zone d'atterrissage de 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 la [zone d'atterrissage](#) de AWS Control Tower APIs. Ou depuis la console, rendez-vous sur la page des 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 prend pas en charge AWS Service Catalog. C'est pourquoi certaines fonctionnalités de 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 de 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](#).

Le Service Catalog APIs n'est pas disponible dans la région du Canada Ouest (Calgary). L'exemple de script présenté dans [Automate Account Provisioning in AWS Control Tower by Service Catalog](#) n'APIest pas réalisable.

Account Factory Customizations (AFC), Account Factory for Terraform (AFT) et Customizations for AWS Control Tower (CfCT) ne sont pas disponibles dans le Canada-Ouest (Calgary) en raison de l'absence d'autres dépendances sous-jacentes pour Control Tower. AWS Si vous étendez la gouvernance à la région du Canada Ouest (Calgary), vous pouvez continuer à gérer les AFC plans dans toutes les régions prises en charge par AWS Control Tower, à condition que Service Catalog soit disponible dans votre région d'origine.

Contrôles

Contrôles proactifs et contrôles pour AWS Security Hub Service-Managed Standard : AWS Control Tower n'est pas disponible dans la région du Canada Ouest (Calgary). Le contrôle préventif n'CT.CLOUDFORMATION.PR.1est pas disponible dans le Canada-Ouest (Calgary) car il n'est nécessaire que pour activer les contrôles proactifs basés sur des crochets. Certains contrôles de détection basés sur AWS Config ne sont pas disponibles. Pour plus de détails, consultez [Limites de contrôle](#).

Fournisseur d'identité

IAM Identity Center n'est pas disponible dans le Canada-Ouest (Calgary). La meilleure pratique recommandée est de configurer votre zone de landing zone dans une région où IAM Identity Center 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 dans le 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 une liste complète des régions dans lesquelles AWS Control Tower est disponible, consultez le [AWS Tableau des régions](#).

AWSControl Tower prend en charge les ajustements de quotas en libre-service

25 avril 2024

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl Tower prend désormais en charge les ajustements de quotas en libre-service via la console Service Quotas. Pour de plus amples informations, veuillez consulter [Demander une augmentation de quota](#).

AWSControl Tower publie le guide de référence sur les contrôles

21 avril 2024

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl Tower a publié le Controls Reference Guide, un nouveau document dans lequel vous pouvez trouver des informations détaillées sur les commandes spécifiques à l'environnement de la AWS Control Tower. Ce matériel figurait auparavant dans le guide de l'utilisateur AWS de la 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 de AWS Control Tower Controls](#).

AWSControl Tower met à jour et renomme deux contrôles proactifs

26 mars 2024

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl 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 2. TLSv1](#)
- [\[CT.OPENSEARCH.PR.16 \] Nécessite 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 la version 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 TLS version 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 Support](#).

Les contrôles obsolètes ne sont plus disponibles

12 mars 2024

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl Tower a rendu certains contrôles obsolètes. 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

AWSControl Tower prend en charge le balisage des **EnabledControl** ressources dans AWS CloudFormation

22 février 2024

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

Cette version de AWS Control Tower met à jour le comportement de la `EnabledControl` ressource, afin de mieux l'aligner sur les commandes 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 tags APIs uniquement via la console AWS Control Tower.

La AWS Control Tower et `GetEnabledControl` `EnableControl` les `ListTagsForResource` API opérations sont mises à jour avec cette version, car elles reposent sur les fonctionnalités `EnabledControl` des ressources.

Pour plus d'informations, consultez la section [Marquage EnabledControl des ressources dans AWS Control Tower](#) et [EnabledControl](#) dans AWS CloudFormation Guide de l'utilisateur.

AWSControl Tower prend en charge APIs l'enregistrement et la configuration des unités d'organisation avec des lignes de base

14 février 2024

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

Ils APIs 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 AWS de 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 commandes facultatives ainsi que des commandes obligatoires. Lorsque vous appelez APIs, vous devrez peut-être effectuer une étape supplémentaire pour que les commandes facultatives soient activées.

Une base de référence AWS Control Tower intègre les meilleures pratiques en matière de gouvernance d'une unité d'organisation et des comptes des membres par la AWS Control Tower. 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, notamment AWS CloudTrail, AWS Config, IAM Identity Center, et obligatoire AWS IAM rôles.

Des lignes de base spécifiques sont compatibles avec des versions spécifiques AWS de la zone d'atterrissage de Control Tower. AWSControl Tower peut appliquer la dernière ligne de base compatible à votre zone d'atterrissage lorsque vous modifiez les paramètres de votre zone d'atterrissage. Pour de plus amples informations, veuillez consulter [Compatibilité des versions de base de l'OU et de la zone d'atterrissage](#).

Cette version inclut quatre éléments essentiels [Types de lignes de base](#)

- `AWSControlTowerBaseline`
- `AuditBaseline`
- `LogArchiveBaseline`
- `IdentityCenterBaseline`

Grâce aux nouvelles APIs lignes de base définies, vous pouvez enregistrer OUs et automatiser votre flux de travail de provisionnement des unités d'organisation. Ils peuvent APIs également gérer ceux OUs qui sont déjà sous la gouvernance de la AWS Control Tower, afin que vous puissiez vous réinscrire OUs après les mises à jour de la zone d'atterrissage. Ils APIs incluent le support d'un `AWS CloudFormation EnabledBaselineressource`, qui vous permet de gérer votre infrastructure sous forme OUs de code (IaC).

Base de référence APIs

- `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 la dérive de contrôle imbriquée OUs et obligatoire). Corrige également la dérive pour la landing-zone-level Région, refuse le contrôle
- `GetBaseline`, `ListBaselines`: Découvrez le contenu des lignes de base de AWS Control Tower.

Pour en savoir plus à ce sujet APIs, consultez les [lignes de base](#) du guide de l'utilisateur de la AWS Control Tower et le manuel de [API référence](#). Les nouveaux APIs sont disponibles en Régions AWS où AWS Control Tower est disponible, sauf dans les régions GovCloud (États-Unis). Pour une liste des Régions AWS où AWS Control Tower est disponible, consultez le [Région AWS Tableau](#).

janvier - décembre 2023

En 2023, AWS Control Tower a publié les mises à jour suivantes :

- [Transition vers le nouveau AWS Service Catalog Type de produit externe \(phase 3\)](#)
- [AWSZone d'atterrissage de la Control Tower, version 3.3](#)
- [Transition vers le nouveau AWS Service Catalog Type de produit externe \(phase 2\)](#)
- [AWSControl Tower annonce des contrôles pour favoriser la souveraineté numérique](#)
- [AWSControl Tower soutient la zone d'atterrissage APIs](#)
- [AWSControl Tower prend en charge le balisage pour les commandes activées](#)
- [AWSControl Tower disponible dans la région Asie-Pacifique \(Melbourne\)](#)
- [Transition vers le nouveau AWS Service Catalog Type de produit externe \(phase 1\)](#)
- [Nouveau contrôle API disponible](#)
- [AWSControl Tower ajoute des commandes supplémentaires](#)
- [Nouveau type de dérive signalé : accès sécurisé désactivé](#)
- [Quatre supplémentaires Régions AWS](#)
- [AWSControl Tower disponible dans la région de Tel Aviv](#)
- [AWSControl Tower lance 28 nouveaux contrôles proactifs](#)
- [AWSControl Tower déconseille deux commandes](#)
- [AWSZone d'atterrissage de la Control Tower, version 3.2](#)
- [AWSControl 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](#)
- [AWSControl Tower publie des tables de métadonnées de contrôle](#)
- [Support de Terraform pour la personnalisation d'Account Factory](#)
- [AWS IAML'autogestion du centre d'identité est disponible pour la zone de landing zone](#)

- [AWSControl Tower résout le problème de la gouvernance mixte pour OUs](#)
- [Contrôles proactifs supplémentaires disponibles](#)
- [Contrôles EC2 proactifs Amazon mis à jour](#)
- [Sept supplémentaires Régions AWS available](#)
- [Account Factory for Terraform \(AFT\) : suivi des demandes de personnalisation du compte](#)
- [AWSZone d'atterrissage de la Control Tower, version 3.1](#)
- [Contrôles proactifs généralement disponibles](#)

Transition vers le nouveau AWS Service Catalog Type de produit externe (phase 3)

14 décembre 2023

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl Tower ne prend plus en charge Terraform Open Source en tant que type de produit (plan) lors de la création de nouveaux 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 AWS Service Catalog Type de produit 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 de Terraform.

AWSZone d'atterrissage de la Control Tower, version 3.3

14 décembre 2023

(Mise à jour requise pour la zone d'atterrissage de AWS Control Tower vers la version 3.3. Pour plus d'informations, voir [Mettez à jour votre zone de landing zone](#)).

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 que 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, AWS les 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 comptes de votre organisation peuvent écrire des journaux dans votre compartiment S3 ; elle empêche les CloudTrail 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, voir [Politique relative au compartiment Amazon S3 dans le compte d'audit](#).

Pour plus d'informations sur la nouvelle clé de condition, consultez la IAM documentation et le billet de IAM blog intitulé « Utiliser des contrôles évolutifs pour AWS services accédant à vos ressources. »

Mises à jour de la politique figurant dans le AWS Config SNSsujet

Nous avons ajouté la nouvelle clé de `aws:SourceOrgID` condition à la politique pour AWS Config SNSSUJET. Pour consulter la politique mise à jour, consultez le [AWS Config SNSpolitique thématique](#).

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`.

Mis à jour AWS CloudFormation modèle

Nous avons mis à jour le AWS CloudFormation modèle pour la pile nommée de BASELINE-CLOUDTRAIL-MASTER telle sorte qu'elle ne montre pas de dérive lorsque AWS KMS le chiffrement n'est pas utilisé.

Transition vers le nouveau AWS Service Catalog Type de produit externe (phase 2)

7 décembre 2023

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

HashiCorp a mis à jour leur licence Terraform. En conséquence, 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 éviter de perturber les charges de travail existantes et AWS ressources de vos comptes, suivez les étapes de transition de AWS Control Tower dans [Transition vers le AWS Service Catalog Type de produit externe](#) d'ici le 14 décembre 2023.

AWSControl Tower annonce des contrôles pour favoriser la souveraineté numérique

27 novembre 2023

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl Tower annonce 65 nouveaux AWS-des contrôles gérés, pour vous aider à répondre à vos exigences 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 aident à appliquer vos stratégies de chiffrement et de résilience, telles que Exiger un AWS AppSync APIcache pour activer le chiffrement en transit ou exiger un AWS Network Firewall à déployer dans plusieurs zones de disponibilité. Vous pouvez également personnaliser le AWS contrôle des refus de la Control Tower Region 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 de 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 de la nouvelle amélioration du refus des régions, cette version inclut un nouveau `APIUpdateEnabledControl`, qui vous permet de rétablir les paramètres par défaut de vos commandes activées. Cela 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 version API, consultez [le AWS Control Tower API Reference](#)

Nouveaux contrôles proactifs

- CT.APIGATEWAY.PR.6: Exiger qu'un REST domaine Amazon API Gateway utilise une politique de sécurité qui spécifie une version de TLS protocole minimale de TLSv1.2.
- CT.APPSYNC.PR.2: Nécessite un AWS AppSync GraphQL API à configurer avec une visibilité privée
- CT.APPSYNC.PR.3: Exiger qu'un AWS AppSync GraphQL n'API est pas authentifié avec des clés API
- CT.APPSYNC.PR.4: Nécessite un AWS AppSync APICache GraphQL pour activer le chiffrement en transit.
- CT.APPSYNC.PR.5: Nécessite un AWS AppSync APICache GraphQL pour activer le chiffrement au repos.
- CT.AUTOSCALING.PR.9: Exiger un EBS volume Amazon 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 soit utilisé uniquement AWS Types d'instances Nitro lors du remplacement d'un modèle de lancement
- CT.AUTOSCALING.PR.11: Nécessite uniquement AWS Types d'instances Nitro qui prennent en charge le chiffrement du trafic réseau entre les instances à ajouter 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 Transport Layer Security () TLS
- CT.DMS.PR.2: Nécessite un AWS Database Migration Service (DMS) Endpoint pour chiffrer les connexions pour les points de terminaison source et cible
- CT.EC2.PR.15: Exiger qu'une EC2 instance Amazon utilise un AWS Type d'instance Nitro lors de la création à partir du type de AWS : : EC2 : : LaunchTemplate ressource
- CT.EC2.PR.16: Exiger qu'une EC2 instance Amazon utilise un AWS Type d'instance Nitro lorsqu'elle est créée à l'aide du type de AWS : : EC2 : : Instance ressource
- CT.EC2.PR.17: Exiger qu'un hôte EC2 dédié Amazon utilise un type d'instance AWS Nitro

- CT.EC2.PR.18: Exiger qu'une EC2 flotte Amazon remplace uniquement les modèles de lancement par AWS Types d'instances Nitro
- CT.EC2.PR.19: Exiger qu'une EC2 instance Amazon 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 AWS :: EC2 :: Instance type de ressource
- CT.EC2.PR.20: Exiger qu'une EC2 flotte Amazon remplace uniquement les modèles de lancement par AWS Types d'instances Nitro qui prennent en charge le chiffrement lors du transit entre les instances
- CT.ELASTICACHE.PR.8: Exiger l'activation de l'RBAC authentication auprès d'un groupe de ElastiCache réplication Amazon des versions ultérieures de Redis
- 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: Nécessite un AWS Le pare-feu Network Firewall sera déployé dans plusieurs zones de disponibilité
- CT.RDS.PR.26: nécessite un proxy Amazon RDS DB pour exiger des connexions Transport Layer Security (TLS)
- CT.RDS.PR.27: Exiger un groupe de paramètres de cluster Amazon RDS DB pour exiger des connexions Transport Layer Security (TLS) pour les types de moteurs pris en charge
- CT.RDS.PR.28: Exiger un groupe de paramètres Amazon RDS DB pour exiger des connexions Transport Layer Security (TLS) pour les types de moteurs pris en charge
- CT.RDS.PR.29: Exiger qu'un RDS cluster Amazon 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 RDS base de données Amazon soit configuré pour utiliser une KMS clé que vous spécifiez pour les types de moteurs pris en charge
- CT.S3.PR.12: Exiger qu'un point d'accès Amazon S3 ait une configuration Block Public Access (BPA) avec toutes les options définies sur true

Nouveaux contrôles préventifs

- CT.APPSYNC.PV.1 Exiger qu'un AWS AppSync GraphQL API est configuré avec une visibilité privée
- CT.EC2.PV.1 Exiger la création d'un EBS instantané Amazon à partir d'un EC2 volume chiffré
- CT.EC2.PV.2 Exiger qu'un EBS volume Amazon attaché soit configuré pour chiffrer les données au repos
- CT.EC2.PV.3 Exiger qu'un EBS instantané Amazon ne puisse pas être restauré publiquement
- CT.EC2.PV.4 Exiger qu'Amazon EBS Direct APIs ne soit pas appelé
- CT.EC2.PV.5 Interdire l'utilisation de l'importation et de l'exportation de EC2 machines virtuelles Amazon
- CT.EC2.PV.6 Interdire l'utilisation d'Amazon EC2 RequestSpotFleet et d'actions obsolètes RequestSpotInstances API
- CT.KMS.PV.1 Exiger un AWS KMS politique clé consistant à avoir une déclaration limitant la création de AWS KMS subventions à AWS services
- CT.KMS.PV.2 Exiger qu'un AWS KMS une clé asymétrique dont le matériau de RSA clé est utilisé pour le chiffrement n'a pas une longueur de clé de 2048 bits
- CT.KMS.PV.3 Exiger qu'un AWS KMS la clé est configurée avec le contrôle de sécurité du verrouillage de la politique de contournement activé
- CT.KMS.PV.4 Exiger qu'un AWS KMS la clé gérée par le client (CMK) est configurée avec du matériel clé provenant de AWS Nuage HSM
- CT.KMS.PV.5 Exiger qu'un AWS KMS la clé gérée par le client (CMK) est configurée avec du matériel clé importé
- CT.KMS.PV.6 Exiger qu'un AWS KMS la clé gérée par le client (CMK) est configurée avec du matériel clé provenant d'un magasin de clés externe () XKS
- CT.LAMBDA.PV.1 Exiger un AWS Lambda fonction URL à utiliser AWS IAMauthentification basée
- CT.LAMBDA.PV.2 Exiger un AWS Lambda fonction URL à configurer pour un accès réservé aux principaux au sein de votre Compte AWS
- CT. MULTISERVICE.PV.1 : Refuser l'accès à AWS sur la base de la demande Région AWS pour une unité organisationnelle

Les nouvelles commandes détectives qui améliorent votre posture de gouvernance en matière de souveraineté numérique font partie du AWS Security Hub AWSControl Tower standard avec gestion des services.

Nouvelles commandes de détection

- SH.ACM.2: RSA les certificats gérés par ACM doivent utiliser une longueur de clé d'au moins 2 048 bits
- SH.AppSync.5: AWS AppSync GraphQL ne APIs doit pas être authentifié avec des clés 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 DMS points de terminaison doivent utiliser 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 EC2 transit ne doivent pas accepter automatiquement les demandes de VPC pièces jointes
- SH.EKS.1: les points de terminaison du EKS cluster 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 doit être activé pour les groupes de ElastiCache réplication des versions antérieures de Redis AUTH
- 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: MSK les clusters doivent être chiffrés lors du transit entre les nœuds du broker

- SH.RDS.12: IAM l'authentification doit être configurée pour les RDS clusters
- SH.RDS.15: les RDS clusters de base de données doivent être configurés pour plusieurs zones de disponibilité
- SH.S3.17: Les compartiments S3 doivent être chiffrés au repos avec AWS KMS clés

Pour plus d'informations sur les commandes ajoutées au AWS Security Hub Service-Managed Standard AWS Control Tower, voir [Contrôles qui s'appliquent à Service-Managed Standard : Control Tower in the AWS](#) AWS Security Hub .

Pour une liste des Régions AWS qui ne prennent pas en charge certains contrôles faisant partie du AWS Security Hub Service-Managed Standard AWS Control Tower, voir 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, les IAM principes et les actions exemptés qui sont autorisés, au niveau de l'unité d'organisation, plutôt que pour l'ensemble de la zone d'AWSatterrissage de la 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](#).

Le `UpdateEnabledControl` API

Cette version AWS de Control Tower ajoute la prise en API charge suivante pour les commandes :

- La mise à jour `EnableControl` API permet de configurer des contrôles configurables.
- La mise à jour `GetEnabledControl` API affiche les paramètres configurés sur un contrôle activé.
- Le nouveau `UpdateEnabledControl` API peut modifier les paramètres d'un contrôle activé.

Pour plus d'informations, consultez le AWS Control Tower [APIReference](#).

AWSControl Tower soutient la zone d'atterrissage APIs

26 novembre 2023

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl Tower prend désormais en charge la configuration de la zone d'atterrissage et le lancement à l'aide de APIs. Vous pouvez créer, mettre à jour, obtenir, répertorier, réinitialiser et supprimer des zones d'atterrissage à l'aide de APIs.

Les instructions suivantes vous permettent de configurer et de gérer votre zone d'atterrissage par programme à l'aide de AWS CloudFormation ou le AWS CLI.

AWSControl Tower prend en charge les éléments suivants APIs pour les zones d'atterrissage :

- `CreateLandingZone`—Cet API appelle crée une zone d'atterrissage à l'aide d'une version de zone d'atterrissage et d'un fichier manifeste.
- `GetLandingZoneOperation`—Cet API appelle renvoie l'état d'une opération de zone d'atterrissage spécifiée.
- `GetLandingZone`—Cet API appelle renvoie des informations sur la zone d'atterrissage spécifiée, notamment la version, le fichier manifeste et le statut.
- `UpdateLandingZone`—Cet API appelle met à jour la version ou le fichier manifeste de la zone d'atterrissage.
- `ListLandingZone`—Cet API appelle renvoie un identifiant de zone d'atterrissage (ARN) pour une configuration de zone d'atterrissage dans le compte de gestion.
- `ResetLandingZone`—Cet API appelle rétablit 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 API appelle met hors service la zone d'atterrissage.

Pour commencer à utiliser la zone d'atterrissage APIs, consultez le [Commencez à utiliser AWS Control Tower en utilisant APIs](#).

AWSControl Tower prend en charge le balisage pour les commandes activées

10 novembre 2023

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl Tower prend désormais en charge le balisage des ressources pour les commandes activées, depuis la console AWS Control Tower ou au moyen de APIs. Vous pouvez ajouter, supprimer ou répertorier des balises pour les contrôles activés.

Avec la sortie de ce qui suit APIs, vous pouvez configurer des balises pour les commandes 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.

AWSControl Tower prend en charge les éléments suivants APIs pour le balisage des commandes :

- `TagResource`—Cet API appel ajoute des balises aux commandes activées dans AWS Control Tower.
- `UntagResource`—Cet API appel supprime les tags des commandes activées dans AWS Control Tower.
- `ListTagsForResource`—Cet API appel renvoie des balises pour les commandes activées dans AWS Control Tower.

AWS Les commandes Control Tower APIs sont disponibles en Régions AWS où AWS Control Tower est disponible. Pour une liste complète des Régions AWS dans lequel AWS Control Tower est disponible, consultez le [AWS Tableau des régions](#). Pour une liste complète des AWS Control Tower APIs, consultez la [API référence](#).

AWSControl Tower disponible dans la région Asie-Pacifique (Melbourne)

3 novembre 2023

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl 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 d'atterrissage, vous devez [mettre à jour tous les comptes régis par AWS Control Tower](#), afin de les OUs placer sous gouvernance dans la nouvelle région. Pour plus d'informations, voir [À propos des mises à jour](#).

Pour une liste complète des régions dans lesquelles AWS Control Tower est disponible, consultez le [Région AWS Tableau](#).

Transition vers le nouveau AWS Service Catalog Type de produit externe (phase 1)

31 octobre 2023

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

HashiCorp a mis à jour leur licence Terraform. En conséquence, AWS Service Catalog support mis à jour pour les produits Open Source Terraform et produits fournis à un nouveau type de produit, appelé External.

AWSControl Tower ne prend pas en charge les personnalisations d'Account Factory qui reposent sur AWS Service Catalog Type de produit externe. Pour éviter de perturber les charges de travail existantes et AWS ressources dans vos comptes, suivez les étapes de transition de AWS Control Tower dans cet ordre suggéré, d'ici le 14 décembre 2023 :

1. Mettez à niveau votre moteur de référence Terraform existant pour 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. Accéder à AWS Service Catalog et dupliquez tous les plans Open Source Terraform existants 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 Control TowerAWS.

Nouveau contrôle API disponible

14 octobre 2023

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl Tower prend désormais en charge un API module supplémentaire que vous pouvez utiliser pour déployer et gérer vos commandes AWS Control Tower, à grande échelle. Pour plus d'informations sur le AWS contrôle de la Control TowerAPIs, consultez la [APIréférence](#).

AWSControl Tower a ajouté un nouveau contrôleAPI.

- `GetEnabledControlAPI`—L'appel fournit des informations sur un contrôle activé.

Nous avons également mis à jour ceci API :

`ListEnabledControls`—Cet API appel 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.

Grâce à ceux-ci APIs, vous pouvez effectuer plusieurs opérations courantes par programmation. Par exemple :

- Consultez la liste de toutes les commandes que vous avez activées dans la bibliothèque de commandes de 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.

AWS Les commandes Control Tower APIs sont disponibles en Régions AWS où AWS Control Tower est disponible. Pour une liste complète des Régions AWS dans lequel AWS Control Tower est disponible, consultez le [AWS Tableau des régions](#). Pour une liste complète des AWS Control Tower APIs, consultez la [API référence](#).

AWS Control Tower ajoute des commandes supplémentaires

5 octobre 2023

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWS Control Tower annonce de nouvelles commandes proactives et détectives.

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 AWS CloudFormation les provisionne. Les contrôles proactifs complètent les capacités de contrôle préventif et de détection existantes de 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] Demander à un groupe de travail Amazon Athena de chiffrer les résultats des requêtes Athena au repos avec un AWS Key Management Service (KMS) clé
- [CT.CLOUDTRAIL.PR.4] Exiger un AWS CloudTrail Lake Event Data Store pour permettre le chiffrement au repos à l'aide d'un AWS KMS clé
- [CT.DAX.PR.2] Exiger qu'un DAX cluster Amazon déploie des nœuds dans au moins trois zones de disponibilité
- [CT.EC2.PR.14] Exiger un EBS volume Amazon configuré via un modèle de EC2 lancement Amazon pour chiffrer les données au repos
- [CT.EKS.PR.2] Exiger qu'un EKS cluster Amazon soit configuré avec un chiffrement secret à l'aide de 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 crypter les données au repos dans Amazon S3 avec un AWS KMS clé
- [CT.EMR.PR.3] Exiger qu'une configuration de sécurité Amazon EMR (EMR) soit configurée avec le chiffrement du disque local en EBS volume à l'aide d'un AWS KMS clé
- [CT.EMR.PR.4] Exiger qu'une configuration de sécurité Amazon EMR (EMR) soit configurée pour crypter les données en transit
- [CT.GLUE.PR.1] Exiger un AWS Job Glue pour avoir une configuration de sécurité associée
- [CT.GLUE.PR.2] Exiger un AWS Configuration de sécurité Glue pour chiffrer les données dans les cibles Amazon S3 à l'aide de AWS KMS clés
- [CT.KMS.PR.2] Exigez qu'un AWS KMS une clé asymétrique dont le matériau de RSA clé est utilisé pour le chiffrement a une longueur de clé supérieure à 2048 bits
- [CT.KMS.PR.3] Exiger un AWS KMS politique clé consistant à avoir une déclaration limitant la création de AWS KMS subventions à AWS services
- [CT.LAMBDA.PR.4] Exiger un AWS Lambda autorisation de couche pour accorder l'accès à un AWS organisation ou spécifique AWS compte
- [CT.LAMBDA.PR.5] Exiger un AWS Lambda fonction URL à utiliser AWS IAM authentication basée

- [CT.LAMBDA.PR.6] Exiger un AWS Lambda URLCORSpolitique fonctionnelle 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 d'audit par Amazon
- [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 Secure Sockets Layer (SSL) pour le chiffrement des données en transit

Ces nouveaux contrôles proactifs sont disponibles dans le commerce 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 des clusters Neptune doit être IAM activée

- [SH.Neptune.8] Les clusters de base de données Neptune doivent être configurés pour copier des balises dans des instantanés
- [SH.RDS.27] Les RDS clusters de base de données doivent être chiffrés au repos

Le nouveau AWS Security Hub les commandes de détection sont disponibles dans la plupart des Régions AWS où AWS Control Tower est disponible. Pour plus de détails sur ces contrôles, consultez [Contrôles applicables à Service-Managed Standard : AWS Control Tower](#). Pour plus de détails sur les endroits où les commandes sont disponibles, consultez [Limites de contrôle](#).

Nouveau type de dérive signalé : accès sécurisé désactivé

21 septembre 2023

(Aucune mise à jour requise pour la zone d'atterrissage de 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 AWS de votre 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 requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl Tower est désormais disponible en Asie-Pacifique (Hyderabad), en Europe (Espagne et Zurich) et au Moyen-Orient (UAE).

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 d'atterrissage, vous devez [mettre à jour tous les comptes régis par AWS Control Tower](#), afin de les OUs placer sous gouvernance dans la nouvelle région. Pour plus d'informations, voir [À propos des mises à jour](#).

Pour une liste complète des régions dans lesquelles AWS Control Tower est disponible, consultez le [Région AWS Tableau](#).

AWSControl Tower disponible dans la région de Tel Aviv

28 août 2023

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl 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 d'atterrissage, vous devez [mettre à jour tous les comptes régis par AWS Control Tower](#), afin de les OUs placer sous gouvernance dans la nouvelle région. Pour plus d'informations, voir [À propos des mises à jour](#).

Pour une liste complète des régions dans lesquelles AWS Control Tower est disponible, consultez le [Région AWS Tableau](#).

AWSControl Tower lance 28 nouveaux contrôles proactifs

24 juillet 2023

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl Tower ajoute 28 nouveaux contrôles proactifs pour vous aider à gérer votre AWS environnement.

Les contrôles proactifs améliorent les capacités de gouvernance de AWS Control Tower sur l'ensemble de vos comptes multiples AWS environnements, en bloquant les ressources non conformes avant qu'elles ne soient provisionnées. Ces contrôles aident à gérer AWS des services tels qu'Amazon CloudWatch, Amazon Neptune, Amazon, ElastiCache AWS Step Functions, et Amazon 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] Nécessite un AWS AppSync GraphQL va activer API la journalisation

- [CT. CLOUDWATCH.PR.1] Exiger qu'une action d'une CloudWatch alarme Amazon soit configurée pour l'état de l'alarme
- [CT. CLOUDWATCH.PR.2] Exiger qu'un groupe de CloudWatch journaux Amazon soit conservé pendant au moins un an
- [CT. CLOUDWATCH.PR.3] Exiger qu'un groupe de CloudWatch logs Amazon soit chiffré au repos avec un AWS KMS clé
- [CT. CLOUDWATCH.PR.4] Exiger l'activation d'une action CloudWatch d'alarme Amazon
- [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 AWS KMS clés
- [CT. EC2.PR.13] Exiger que la surveillance détaillée soit activée sur une EC2 instance Amazon
- [CT. EKS.PR.1] Exiger qu'un EKS cluster Amazon soit configuré avec l'accès public désactivé au point de terminaison du serveur API Kubernetes du cluster
- [CT. ELASTICACHE.PR.1] Exiger que les sauvegardes automatiques soient activées sur un cluster Amazon ElastiCache pour Redis
- [CT. ELASTICACHE.PR.2] Exiger que les mises à niveau automatiques ElastiCache des versions mineures soient activées sur un cluster Amazon pour Redis
- [CT. ELASTICACHE.PR.3] Exiger qu'un groupe de réplication Amazon ElastiCache pour Redis active le basculement automatique
- [CT. ELASTICACHE.PR.4] Exiger qu'un groupe de ElastiCache réplication Amazon active le chiffrement au repos
- [CT. ELASTICACHE.PR.5] Exiger qu'un groupe de réplication Amazon ElastiCache pour Redis active le chiffrement en transit
- [CT. ELASTICACHE.PR.6] Exiger qu'un cluster de ElastiCache cache Amazon utilise un groupe de sous-réseaux personnalisé
- [CT. ELASTICACHE.PR.7] Exiger qu'un groupe de ElastiCache réplication Amazon de versions antérieures de Redis dispose d'une authentification Redis AUTH
- [CT. ELASTICBEANSTALK[PR.3] Nécessite un AWS L'environnement Elastic Beanstalk doit disposer d'une configuration de journalisation
- [CT. LAMBDA[PR.3] Nécessite un AWS Lambda fonction à intégrer dans un Amazon Virtual Private Cloud () géré par le client VPC

- [CT. NEPTUNE.PR.1] Exiger qu'un cluster de base de données Amazon Neptune ait AWS Identity and Access Management (IAM) authentication de base de données
- [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 AWS KMS clés
- [CT.S3.PR.11] Exiger l'activation du versionnement d'un compartiment Amazon S3
- [CT. STEPFUNCTIONS.PR.1] Nécessite un AWS Step Functions machine à états pour activer la journalisation
- [CT. STEPFUNCTIONS.PR.2] Nécessite un AWS Step Functions machine à états à avoir AWS X-Ray traçage activé

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 AWS CloudFormation les approvisionne. Les contrôles proactifs complètent les capacités de contrôle préventif et de détection existantes de AWS Control Tower.

Ces nouveaux contrôles proactifs sont disponibles dans tous Régions AWS où AWS Control Tower est disponible. Pour plus de détails sur ces contrôles, voir [Contrôles proactifs](#).

AWSControl Tower déconseille deux commandes

18 juillet 2023

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl 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 déjà doté du chiffrement SSE -S3 ou côté serveur avec AWS Service de gestion des clés (AWS KMS) touches (SSE-KMS) configurées.

AWSZone d'atterrissage de la Control Tower, version 3.2

16 juin 2023

(Mise à jour requise pour la zone d'atterrissage de AWS Control Tower vers la version 3.2. Pour plus d'informations, voir [Mettez à jour votre zone de landing zone](#)).

AWS La version 3.2 de la zone d'atterrissage de Control Tower intègre les commandes qui font partie du AWS Security Hub Service-Managed Standard : AWS Control Tower jusqu'à la disponibilité générale. 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 « `AWSServiceRoleForAWSControlTowerManagedRule` dans chaque compte membre ». Cette règle gérée collecte AWS Security Hub La recherche d'événements à l'aide de AWS Control Tower 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 depuis le EventBridge APIs. Vous pouvez consulter la règle dans la EventBridge console ou à l'aide du EventBridge APIs. Si le `managed-by` champ est renseigné, il affichera le principal du service AWS Control Tower.

Auparavant, AWS Control Tower assumait le `AWSServiceRoleForAWSControlTowerExecution` rôle 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 compte multiple AWS environnement. 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 et de SNS vérifier la dérive. Pour de plus amples informations, veuillez consulter [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 zone d'atterrissage 3.2 et versions ultérieures), AWS Control Tower reçoit une mise à jour quotidienne du statut de Security Hub. Bien que les contrôles soient actifs dans chaque région gouvernée, AWS Control Tower envoie le AWS Security Hub Recherche des événements dans la région d'origine de la AWS Control Tower uniquement. 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.

Services globaux et APIs ajoutés

- 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 APIs 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.

AWSControl Tower gère les comptes en fonction de leur identifiant

14 juin 2023

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl Tower crée et gère désormais les comptes que vous créez dans Account Factory en suivant les AWS l'identifiant du compte, plutôt que l'adresse e-mail du compte.

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.

Contrôles de détection supplémentaires du Security Hub disponibles dans la bibliothèque de contrôles AWS Control Tower

12 juin 2023

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl Tower a ajouté dix nouveaux AWS Security Hub contrôles de détection vers la bibliothèque de commandes de 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, SageMaker Amazon et 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 de API passerelle 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 EC2 lancement ne doivent pas attribuer de public IPs aux interfaces réseau
- [SH. ELB.1] Application Load Balancer doit être configuré pour rediriger toutes les HTTP demandes 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 de manière personnalisée VPC
- [SH. SageMaker.3] Les utilisateurs ne doivent pas avoir d'accès root aux instances de SageMaker bloc-notes
- [SH. WAF.10] Un WAFV2 site Web ACL doit comporter au moins une règle ou un groupe de règles

Le nouveau AWS Security Hub les commandes de détection sont disponibles dans tous Régions AWS où AWS Control Tower est disponible. Pour plus de détails sur ces contrôles, consultez [Contrôles applicables à Service-Managed Standard : AWS Control Tower](#).

AWSControl Tower publie des tables de métadonnées de contrôle

7 juin 2023

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl Tower fournit désormais des tables complètes de métadonnées de contrôle dans le cadre de la documentation publiée. Lorsque vous travaillez avec le contrôle APIs, vous pouvez rechercher celui de chaque contrôle API `controlIdentifier`, qui est unique ARN associé à chaque 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 du [AWS Security Hub Norme de gestion des services : AWS Control Tower](#). Pour plus de détails, consultez la section [Tableaux des métadonnées de contrôle](#).

Pour une liste abrégée des identificateurs de contrôle et quelques exemples d'utilisation, voir [Identifiants de ressources pour les contrôles et les contrôles](#). APIs

Support de Terraform pour la personnalisation d'Account Factory

6 juin 2023

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl Tower offre 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 AFC compte, dans l'open source Terraform. Vous pouvez personnaliser votre nouveau et votre existant 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 de Control Tower.

Un plan de compte décrit les ressources et les configurations spécifiques requises lorsqu'un Compte AWS est provisionné. Vous pouvez utiliser le plan comme modèle pour 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 de AWS Control Tower Account Factory. Les clients qui préfèrent travailler avec Terraform peuvent utiliser la personnalisation des comptes AWS Control Tower à AFC grande échelle et accéder immédiatement à chaque compte une fois celui-ci approvisionné.

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 dans tous Régions AWS où AWS Control Tower est disponible.

AWS IAML'autogestion du centre d'identité est disponible pour la zone de landing zone

6 juin 2023

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl Tower propose désormais un choix optionnel de fournisseur d'identité pour une zone d'atterrissage AWS de Control Tower, que vous pouvez configurer lors de la configuration ou de la mise à jour. Par défaut, la zone d'atterrissage est activée pour utiliser AWS IAMIdentity Center, conformément aux directives relatives aux meilleures pratiques définies dans [Organizing Your AWS Environnement utilisant plusieurs comptes](#). Trois alternatives s'offrent à vous :

- Vous pouvez accepter la valeur par défaut et autoriser AWS Control Tower à configurer et à gérer AWS IAMIdentity Center pour vous.

- Vous pouvez choisir de vous gérer vous-même AWS IAMIdentity Center, pour répondre aux 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 Régions AWS où AWS IAMIdentity Center n'est pas disponible.

Pour de plus amples informations, veuillez consulter [IAMConseils relatifs au centre d'identité](#).

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. AWSL'option du fournisseur d'identité Control Tower est disponible dans tous Régions AWS où AWS Control Tower est disponible.

AWSControl Tower résout le problème de la gouvernance mixte pour OUs

1er juin 2023

(Aucune mise à jour requise pour la zone d'atterrissage de 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 que AWS Control Tower a étendu la gouvernance à une nouvelle Région AWS, ou supprime la gouvernance. Cette version vous aide à garantir la conformité uniforme des comptes des membres de cette unité d'organisation. Pour de plus amples informations, veuillez consulter [Évitez la gouvernance mixte lors de la configuration des régions](#).

Contrôles proactifs supplémentaires disponibles

19 mai 2023

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl 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 crochets qui vérifient vos ressources avant qu'elles

ne soient provisionnées. Les nouveaux contrôles peuvent aider à gouverner AWS des services tels qu'Amazon OpenSearch Service, Amazon EC2 Auto Scaling, Amazon SageMaker, Amazon API Gateway et Amazon Relational Database Service RDS ().

Les contrôles proactifs sont pris en charge dans toutes les entreprises Régions AWS où AWS Control Tower est disponible.

Amazon OpenSearch Service

- [ACTE. OPENSEARCH.PR.1] Exiger un domaine Elasticsearch pour chiffrer les données au repos
- [ACTE. OPENSEARCH.PR.2] Exiger la création d'un domaine Elasticsearch dans un Amazon spécifié par l'utilisateur VPC
- [ACTE. OPENSEARCH.PR.3] Exiger un domaine Elasticsearch pour chiffrer les données envoyées entre les nœuds
- [ACTE. OPENSEARCH.PR.4] Exiger un domaine Elasticsearch pour envoyer des journaux d'erreurs à Amazon Logs CloudWatch
- [ACTE. OPENSEARCH.PR.5] Exiger un domaine Elasticsearch pour envoyer des journaux d'audit à Amazon Logs CloudWatch
- [ACTE. OPENSEARCH.PR.6] Exiger qu'un domaine Elasticsearch dispose d'une reconnaissance de zone et d'au moins trois nœuds de données
- [ACTE. OPENSEARCH.PR.7] Exiger qu'un domaine Elasticsearch possède au moins trois nœuds maîtres dédiés
- [ACTE. OPENSEARCH.PR.8] Nécessite un domaine Elasticsearch Service pour utiliser .2 TLSv1
- [ACTE. OPENSEARCH.PR.9] Exiger un domaine Amazon OpenSearch Service pour chiffrer les données au repos
- [ACTE. OPENSEARCH.PR.10] Exiger la création d'un domaine Amazon OpenSearch Service dans un Amazon spécifié par l'utilisateur VPC
- [ACTE. OPENSEARCH.PR.11] Exiger un domaine Amazon OpenSearch Service pour chiffrer les données envoyées entre les nœuds
- [ACTE. OPENSEARCH.PR.12] Exiger un domaine Amazon OpenSearch Service pour envoyer des journaux d'erreurs à Amazon Logs CloudWatch
- [ACTE. OPENSEARCH.PR.13] Exiger un domaine Amazon OpenSearch Service pour envoyer des journaux d'audit à Amazon Logs CloudWatch
- [ACTE. OPENSEARCH.PR.14] Exiger qu'un domaine Amazon OpenSearch Service dispose d'une reconnaissance de zone et d'au moins trois nœuds de données

- [ACTE. OPENSEARCH.PR.15] Exiger qu'un domaine Amazon OpenSearch Service utilise un contrôle d'accès précis
- [ACTE. OPENSEARCH.PR.16] Nécessite un domaine Amazon OpenSearch Service pour utiliser .2 TLSv1

Amazon EC2 Auto Scaling

- [ACTE. AUTOSCALING.PR.1] Exiger qu'un groupe Amazon EC2 Auto Scaling possède plusieurs zones de disponibilité
- [ACTE. AUTOSCALING.PR.2] Exiger une configuration de lancement de groupe Amazon EC2 Auto Scaling pour configurer les instances Amazon EC2 pour IMDSv2
- [ACTE. AUTOSCALING.PR.3] Exiger une configuration de lancement d'Amazon EC2 Auto Scaling pour avoir une limite de réponse aux métadonnées à saut unique
- [ACTE. AUTOSCALING.PR.4] Exiger qu'un groupe Amazon EC2 Auto Scaling associé à un Amazon Elastic Load Balancing (ELB) fasse activer les bilans de ELB santé
- [ACTE. AUTOSCALING.PR.5] Exiger qu'une configuration de lancement de groupe Amazon EC2 Auto Scaling ne comporte pas d'EC2 instances Amazon avec des adresses IP publiques
- [ACTE. AUTOSCALING.PR.6] Exiger que tous les groupes Amazon EC2 Auto Scaling utilisent plusieurs types d'instances
- [ACTE. AUTOSCALING.PR.8] Exiger qu'un groupe Amazon EC2 Auto Scaling ait des modèles de lancement configurés EC2

Amazon SageMaker

- [ACTE. SAGEMAKER.PR.1] Exiger une instance de SageMaker bloc-notes Amazon pour empêcher l'accès direct à Internet
- [ACTE. SAGEMAKER.PR.2] Exiger que les instances de SageMaker blocs-notes Amazon soient déployées au sein d'un Amazon personnalisé VPC
- [ACTE. SAGEMAKER.PR.3] Exiger que l'accès root soit interdit aux instances d'Amazon SageMaker Notebook

API Passerelle Amazon

- [ACTE. APIGATEWAY.PR.5] Exiger qu'Amazon API Gateway V2 Websocket et HTTP routes spécifient un type d'autorisation

Amazon Relational Database Service RDS ()

- [ACTE. RDS.PR.25] Exiger que la journalisation soit configurée sur un cluster RDS de bases de données Amazon

Pour plus d'informations, voir [Contrôles proactifs](#).

Contrôles EC2 proactifs Amazon mis à jour

2 mai 2023

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl Tower a mis à jour deux contrôles proactifs : CT.EC2.PR.3 and CT.EC2.PR.4.

Pour la mise à jour CT.EC2.PR.3 contrôle, n'importe lequel AWS CloudFormation le déploiement qui fait référence à une liste de préfixes pour une ressource de groupe de sécurité est bloqué, sauf pour le port 80 ou 443.

Pour la mise à jour CT.EC2.PR.4 contrôle, n'importe lequel AWS CloudFormation un déploiement qui fait 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 supplémentaires Régions AWS available

19 avril 2023

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl Tower est désormais disponible en sept versions supplémentaires 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.

Certaines commandes de AWS Control Tower ne fonctionnent pas dans certaines de ces options 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). Disponibilité dans d'autres Régions AWS est inchangé.

Pour plus d'informations sur la façon dont AWS Control Tower gère les limites des régions et des contrôles, consultez [Considérations relatives à l'activation des AWS régions optionnelles](#).

Les VPCe points de terminaison requis par ne AFT sont pas disponibles dans la région Moyen-Orient (Bahreïn). Les clients déployant AFT dans cette région doivent effectuer le déploiement avec paramètre `aft_vpc_endpoints=false`. Pour plus d'informations, consultez le paramètre dans [le README fichier](#).

AWSControl Tower VPCs dispose 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 sur AmazonEC2. Dans l'ouest des États-Unis (Californie du Nord), six sous-réseaux sont répartis sur deux zones de disponibilité. Pour de plus amples informations, veuillez consulter [Présentation d'AWS Control Tower et des VPC](#).

AWSControl Tower a ajouté de nouvelles autorisations `AWSControlTowerServiceRolePolicy` qui permettent à AWS Control Tower de passer des appels au `EnableRegionListRegions`, et `GetRegionOptStatus` APIs mises en œuvre par AWS Service de gestion de compte, pour les rendre supplémentaires Régions AWS disponible pour vos comptes partagés dans la zone de landing zone (compte de gestion, compte d'archivage des journaux, compte d'audit) et pour vos comptes de membres de l'UO. Pour de plus amples informations, veuillez consulter [Politiques gérées pour AWS Control Tower](#).

Account Factory for Terraform (AFT) : suivi des demandes de personnalisation du compte

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, un jeton de suivi unique est AFT généré qui passe par une AFT personnalisation AWS Step Functions machine à états, 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 AFT flux de travail. Pour plus d'informations AFT, consultez la section [Présentation de 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 AWS Step Functions?](#) dans le AWS Step Functions Guide du développeur

AWSZone d'atterrissage de la Control Tower, version 3.1

9 février 2023

(Mise à jour requise pour la zone d'atterrissage de AWS Control Tower vers la version 3.1. Pour plus d'informations, voir [Mettez à jour votre zone de landing zone](#))

AWSLa version 3.1 de Control Tower landing zone inclut les mises à jour suivantes :

- Avec cette version, AWS Control Tower désactive la journalisation inutile des accès à 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, telles que AWS Support Plans et AWS Artifact.
- La désactivation de la journalisation des accès au serveur pour le bucket de journalisation des accès de AWS Control Tower oblige Security Hub à créer une recherche pour le bucket de journalisation des accès du compte Log Archive, en raison d'un AWS Security Hub règle, [\[S3.9\] La journalisation des accès au serveur de compartiment S3 doit être activée](#). 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 à ce sujetSCP, voir [Refuser l'accès à AWS sur la base de la demande Région AWS](#) et [des 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:*)
- IAMCentre d'identité (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 requise pour la zone d'atterrissage de 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 de plus amples informations, veuillez consulter [Des commandes complètes aident à AWS approvisionnement et gestion des 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 commandes complètes aident à AWS approvisionnement et gestion des ressources](#)
- [État de conformité consultable par tous AWS Config rules](#)
- [API pour les commandes et un nouveau AWS CloudFormation ressource](#)
- [CfCT prend en charge la suppression d'ensembles de piles](#)
- [Conservation personnalisée des journaux](#)
- [Réparation de la dérive des rôles disponible](#)
- [AWSZone d'atterrissage de la Control Tower, version 3.0](#)
- [La page Organisation combine les vues OUs et les 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](#)
- [AWSZone d'atterrissage de la Control Tower, version 2.9](#)
- [AWSZone d'atterrissage de la Control Tower, version 2.8](#)

Opérations de compte simultanées

16 décembre 2022

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl 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, pendant 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 requise pour la zone d'atterrissage de 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 donnent la flexibilité de définir des plans de compte, qui sont 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, créés et gérés par 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, pour inscrire d'autres AWS des comptes dans AWS Control Tower et pour 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 le AWS Bibliothèque de mise en route. Pour de plus amples informations, veuillez consulter [Personnalisez les comptes avec Account Factory Customization \(AFC\)](#).

Des commandes complètes aident à AWS approvisionnement et gestion des ressources

28 novembre 2022

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl Tower prend désormais en charge la gestion complète des contrôles, y compris de nouveaux contrôles proactifs optionnels, mis en œuvre via AWS CloudFormation crochets. 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 de AWS Control Tower, à répondre aux exigences des cadres de conformité aux normes du secteur et à régir les interactions de la AWS Control Tower dans plus de vingt autres AWS services.

La bibliothèque de contrôles AWS Control Tower classe ces contrôles en fonction des paramètres associés AWS services et ressources. Pour plus de détails, voir [Contrôles proactifs](#).

Dans cette version, AWS Control Tower est également intégré à AWS Security Hub, grâce à la nouvelle norme Security Hub Service-Managed Standard : AWS Control Tower, qui prend en charge le AWS Norme relative aux meilleures pratiques de sécurité fondamentales (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 par tous AWS Config rules

18 novembre 2022

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl Tower affiche désormais l'état de conformité de tous AWS Config règles déployées dans les unités organisationnelles enregistrées auprès AWS de Control Tower. Vous pouvez consulter l'état de conformité de tous 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.

Précédemment, AWS Config règles déployées par le biais du AWS Config le service n'était pas visible dans la console AWS Control Tower. Les clients devaient accéder au AWS Config service d'identification des non-conformes AWS Config règles. Vous pouvez désormais identifier tout non-

conforme AWS Config règle dans la console AWS Control Tower. Pour connaître l'état de conformité de toutes vos règles de 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 de configuration déployées en dehors de AWS Control Tower.

API pour les commandes et un nouveau AWS CloudFormation ressource

1er septembre 2022

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWS Control Tower prend désormais en charge la gestion programmatique des commandes, également appelées garde-corps, par le biais d'une série d'appels API. Un nouveau AWS CloudFormation La ressource prend en charge les API fonctionnalités des contrôles. Pour de plus amples informations, veuillez consulter [Automatisez les tâches dans AWS Control Tower](#) et [Créez AWS Control Tower des ressources avec AWS CloudFormation](#).

Ils vous APIs permettent d'activer, de désactiver et de consulter l'état de l'application des commandes de la bibliothèque AWS Control Tower. Ils APIs incluent le support pour AWS CloudFormation, afin que vous puissiez gérer AWS ressources en tant que infrastructure-as-code (iAc). AWS Control Tower propose des contrôles préventifs et de détection optionnels 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.

APIs inclus dans cette version

- **EnableControl**— Cet API appel active un contrôle. Il lance une opération asynchrone qui crée AWS les ressources de l'unité organisationnelle spécifiée et les comptes qu'elle contient.
- **DisableControl**— Cet API appel désactive une commande. Il lance une opération asynchrone qui supprime AWS les ressources de l'unité organisationnelle spécifiée et les comptes qu'elle contient.
- **GetControlOperation**— Renvoie le statut d'un particulier EnableControl ou d'une DisableControl opération.
- **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 des commandes facultatives, consultez la section [Identifiants de ressource APIs et commandes](#) dans le guide de l'utilisateur AWS de Control Tower.

CfCT prend en charge la suppression d'ensembles de piles

26 août 2022

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

Customizations for AWS Control Tower (CfCT) prend désormais en charge la suppression d'ensembles de piles, en définissant un paramètre dans le `manifest.yaml` fichier. Pour de plus amples informations, veuillez consulter [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, les ALLressources 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 d'atterrissage de la AWS Control Tower. Pour plus d'informations, voir [Mettez à jour votre zone de landing zone](#))

AWSControl Tower permet désormais de personnaliser la politique de conservation 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 de la AWS Control Tower.

Réparation de la dérive des rôles disponible

11 août 2022

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl 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 de landing zone soit à nouveau disponible.

AWSZone d'atterrissage de la Control Tower, version 3.0

29 juillet 2022

(Mise à jour requise pour la zone d'atterrissage de AWS Control Tower vers la version 3.0. Pour plus d'informations, voir [Mettez à jour votre zone de landing zone](#))

AWSLa version 3.0 de Control Tower landing zone inclut les mises à jour suivantes :

- La possibilité de choisir au niveau de l'organisation AWS CloudTrail ou pour choisir de ne pas suivre les CloudTrail sentiers gérés par AWS Control Tower.
- Deux nouvelles commandes de détection pour déterminer si AWS CloudTrail enregistre l'activité dans vos comptes.
- La possibilité d'agréger AWS Config 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 IAM rôle `aws-controltower-CloudWatchLogsRole` ni le groupe de CloudWatch log `aws-controltower/CloudTrailLogs` dans chaque compte inscrit. Auparavant, nous les avons 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 organisés au niveau de l'organisation dans Control Tower AWS

Avec la version 3.0 de landing zone, AWS Control Tower prend désormais en charge le niveau de l'organisation AWS CloudTrail sentiers.

Lorsque vous mettez à jour votre zone de landing zone de AWS Control Tower vers la version 3.0, vous avez la possibilité de sélectionner au niveau de l'organisation AWS CloudTrail sentiers selon vos préférences en matière d'exploitation forestière, ou pour 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. AWSControl 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 que 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 partir de la landing zone 3.0, AWS Control Tower ne propose plus de pistes au niveau du compte qui AWS gère. AWSControl 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 à suivre 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 sous la forme suivante : `/org id/AWSLogs/...`
- Les journaux de suivi de l'organisation sont stockés avec un chemin de la forme suivante : `/org id/AWSLogs/org id/...`

Le chemin créé par AWS Control Tower pour les journaux au niveau de votre organisation CloudTrail 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 parcours au niveau de votre compte, nous vous recommandons de créer les nouveaux sentiers avant de terminer la mise à jour de la version 3.0 de la zone d'atterrissage de 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 parcours gérés par AWS Control Tower au niveau de l'organisation est disponible lors de toute mise à jour de la zone d'atterrissage 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, au niveau du compte AWS CloudTrail les sentiers ne sont pas pris en charge par AWS Control Tower. Vous pouvez créer et gérer vos propres parcours au niveau de votre compte à tout moment, ou vous pouvez opter pour des parcours au niveau de l'organisation gérés par Control Tower. AWS

Enregistrer AWS Config ressources dans la région d'origine uniquement

Dans la version 3.0 de landing zone, AWS Control Tower a mis à jour la configuration de base pour AWS Config afin qu'il enregistre les ressources mondiales 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 and AWS Config, et elle 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 a été créé pour chaque élément dans chaque région gouvernée.

Deux nouvelles commandes de détection pour AWS CloudTrail journalisation

Dans le cadre du changement au niveau de l'organisation AWS CloudTrail Trails, 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 il est éventuellement appliqué à toute OUs autre option 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 ont AWS CloudTrail ou CloudTrail Lake activé](#)

Contrôle fortement recommandé : [détectez si un compte a AWS CloudTrail ou CloudTrail Lake activé](#)

Pour plus d'informations sur les nouvelles commandes, consultez [la bibliothèque de commandes The 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 existante d'une tour de AWS contrôle vers la zone d'atterrissage 3.](#)

La page Organisation combine les vues OUs et les comptes

18 juillet 2022

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower)

La nouvelle page Organisation de AWS Control Tower présente une vue hiérarchique de toutes les unités organisationnelles (OUs) et de tous les comptes. Il combine les informations des pages OUs et des comptes, qui existaient auparavant.

Sur la nouvelle page, vous pouvez voir les relations entre le parent OUs et ses comptes imbriqués OUs. Vous pouvez agir sur les regroupements de ressources. Vous pouvez configurer l'affichage des pages. Par exemple, vous pouvez développer ou réduire la vue hiérarchique, filtrer la vue pour afficher les comptes ou OUs uniquement, choisir de n'afficher que vos comptes inscrits et enregistrés OUs, 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 de AWS Control Tower)

AWS Control Tower vous offre désormais une fonctionnalité améliorée pour mettre à jour et inscrire les comptes des membres individuellement. Chaque compte indique la date à laquelle 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 enregistrer des comptes dans AWS Control Tower en OUs bénéficiant de 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. Vous pouvez ensuite 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 de 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 enregistrés. 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 `AWSAFTExecution` rôle existant déploie désormais les personnalisations dans tous les comptes. Vous pouvez configurer IAM des autorisations avec des limites qui limitent l'accès au `AWSAFTExecution` rôle 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 `AWSAFTService` rôle pour déployer les AFT ressources dans tous les comptes gérés, y compris les comptes partagés et le compte de gestion. Les ressources étaient auparavant déployées par le `AWSAFTExecution` rôle.

Les comptes partagés et de gestion de la AWS Control Tower ne sont pas approvisionnés via Account Factory, ils ne disposent donc pas de produits provisionnés correspondants dans 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 de AWS Control Tower)

AWSControl 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 d'atterrissage ou lorsqu'elle étend 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 différents OUs appareils.
- Appliquez et supprimez le même contrôle préventif sur plusieurs OUs appareils 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 de AWS Control Tower.

Lorsque vous appliquez des contrôles préventifs à NestedOUs, les contrôles préventifs affectent tous les comptes OUs imbriqués sous l'unité d'organisation cible, même si ces comptes ne OUs sont pas enregistrés auprès de AWS Control Tower. Les contrôles préventifs sont mis en œuvre à l'aide des politiques de contrôle des services (SCPs), qui font partie de 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 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 une liste complète des commandes disponibles, consultez [la bibliothèque de commandes The AWS Control Tower](#).

Comptes de sécurité et de journalisation existants

16 mai 2022

(Disponible lors de la configuration initiale.)

AWSControl Tower vous offre désormais la possibilité de spécifier un AWS compte en tant que compte de sécurité ou de connexion de AWS Control Tower, lors du processus initial de configuration de la zone d'atterrissage. Cette option évite à AWS Control Tower 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 API activités 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 de la AWS Control Tower à vos organisations existantes ou de passer d'une autre zone d'atterrissage à AWS Control Tower. 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. AWSControl 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.

Limite : si vous prévoyez d'apporter des objets existants AWS comptes enregistrés dans AWS Control Tower en tant que comptes d'audit et d'archivage des journaux, et si ces comptes existent AWS Config ressources, vous devez supprimer les ressources existantes AWS Config ressources avant de pouvoir enregistrer les comptes dans AWS Control Tower.

AWSZone d'atterrissage de la Control Tower, version 2.9

22 avril 2022

(Mise à jour requise pour la zone d'atterrissage de AWS Control Tower vers la version 2.9. Pour plus d'informations, voir [Mettez à jour votre zone de landing zone](#))

AWSLa version 2.9 de 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](#).

AWSZone d'atterrissage de la Control Tower, version 2.8

10 février 2022

(Mise à jour requise pour la zone d'atterrissage de AWS Control Tower vers la version 2.8. Pour plus d'informations, voir [Mettez à jour votre zone de landing zone](#))

AWSLa version 2.8 de Control Tower landing zone ajoute des fonctionnalités conformes aux récentes mises à jour du [AWS Bonnes pratiques](#) 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 AWS Rôle lié au service (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 en conséquence 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 KMS configuration AWS de la Control Tower pour le chiffrement. AWS Config , et cela améliore la messagerie d'état associée 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 dansus-west-2.
- Mise à jour : Le 15 février 2022, nous avons supprimé la file d'attente des lettres mortes pour AWS Fonctions Lambda.

Informations supplémentaires :

- Si vous désactivez votre zone d'atterrissage, AWS Control Tower ne supprime pas le AWS Config rôle lié au service.
- Si vous désapprovisionnez un compte Account Factory, AWS Control Tower ne supprime pas le AWS Config rôle lié au 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 d'atterrissage, vous devez mettre à jour tous les comptes régis par AWS Control Tower, comme indiqué dans [Gestion 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](#)
- [AWSControl Tower présente le provisionnement et la personnalisation des comptes Terraform](#)
- [Nouvel événement du cycle de vie disponible](#)
- [AWSControl Tower permet d'imbriquer OUs](#)
- [Detective Control Concurrence](#)
- [Deux nouvelles régions disponibles](#)
- [Désélection de la région](#)
- [AWSControl Tower fonctionne avec AWS Systèmes de gestion des clés](#)
- [Contrôles renommés, fonctionnalités inchangées](#)
- [AWSControl Tower scanne SCPs tous les jours pour détecter toute dérive](#)
- [Noms OUs et comptes personnalisés](#)
- [AWSZone d'atterrissage de la Control Tower, version 2.7](#)
- [Trois nouveaux AWS Régions disponibles](#)
- [Gouverner uniquement les régions sélectionnées](#)
- [AWSControl Tower étend désormais la gouvernance à l'existant OUs dans votre AWS organisations](#)
- [AWSControl Tower fournit des mises à jour groupées des comptes](#)

Fonctionnalités de refus régional

30 novembre 2021

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower.)

AWSControl Tower propose désormais des fonctionnalités de refus de région, qui vous aident à limiter l'accès à AWS services et opérations pour les comptes inscrits dans votre environnement AWS Control Tower. La fonction 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 à AWS services dans les régions situées en dehors de la région de Francfort. Vous pouvez sélectionner des régions restreintes pendant le processus de configuration de la AWS Control Tower ou sur la page des paramètres de la zone d'atterrissage. La fonction Region Deny est disponible lorsque vous mettez à jour votre version de la zone d'atterrissage de AWS Control Tower. Select AWS les services sont exemptés des fonctionnalités de refus régional. 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 de AWS Control Tower)

AWSControl Tower propose désormais des commandes spécialement conçues pour garantir que toutes les données clients que vous téléchargez sur AWS les services sont situés uniquement dans le AWS Régions que vous spécifiez. Vous pouvez sélectionner AWS Région ou régions dans lesquelles les données de vos clients sont stockées et traitées. Pour une liste complète des AWS Régions dans lesquelles AWS Control Tower est disponible, consultez le [AWS Tableau des 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 commandes dans la console AWS Control Tower. Pour une liste complète des commandes disponibles, consultez [la bibliothèque de commandes The AWS Control Tower](#).

AWSControl Tower présente le provisionnement et la personnalisation des comptes Terraform

29 novembre 2021

(Mise à jour facultative pour la zone d'atterrissage de la AWS Control Tower)

Vous pouvez désormais utiliser Terraform pour approvisionner et mettre à jour des comptes personnalisés via AWS Control Tower, avec AWSControl Tower Account Factory for Terraform (). AFT

AFTfournit un pipeline unique d'infrastructure en tant que code (IaC) Terraform, 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 AFT automatique de comptes 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'AFTune des options de fonctionnalité 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 de AWS Control Tower et en le téléchargeant AFT pour votre instance Terraform. [Déployez AWS Control Tower Account Factory pour Terraform \(\) AFT](#) AFTprend 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 de AWS Control Tower)

L'PrecheckOrganizationalUnitévénement enregistre si des ressources bloquent le succès de la tâche de gouvernance Extend, y compris les ressources imbriquées. OUs Pour de plus amples informations, veuillez consulter [PrecheckOrganizationalUnit](#).

AWSControl Tower permet d'imbriquer OUs

16 novembre 2021

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower)

AWSControl Tower vous permet désormais d'inclure Nested OUs dans votre zone de landing zone.

AWSControl Tower prend en charge les unités organisationnelles imbriquées (OUs), ce qui vous permet d'organiser les comptes en plusieurs niveaux hiérarchiques et d'appliquer des contrôles préventifs de manière hiérarchique. Vous pouvez enregistrer le OUs contenu imbriquéOUs, créer et enregistrer OUs sous parentOUs, et activer les contrôles sur n'importe quelle unité d'organisation enregistrée, quelle que soit sa profondeur. Pour prendre en charge cette fonctionnalité, la console indique le nombre de comptes gouvernés etOUs.

Avec nestedOUs, vous pouvez aligner votre AWS Control Tower OUs sur AWS stratégie multi-comptes, et vous pouvez réduire le temps nécessaire pour activer les contrôles sur plusieursOUs, en appliquant les contrôles au niveau de l'unité d'organisation parent.

Considérations clés

1. Vous pouvez enregistrer une unité d'organisation existante à plusieurs niveaux OUs auprès de AWS Control Tower, une unité d'organisation à la fois, en commençant par l'unité d'organisation supérieure, puis en descendant dans l'arborescence. Pour de plus amples informations, veuillez consulter [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 (SCPs) sont hérités automatiquement vers le bas de la hiérarchie ; SCPs ceux appliqués au parent sont hérités par tous les éléments imbriqués. OUs
4. Contrôles Detective (AWS Config (règles) sont NOT héritées automatiquement.
5. La conformité aux contrôles de détection est signalée par chaque unité d'organisation.
6. SCPLa dérive sur une UO affecte tous les comptes et ceux situés OUs en dessous de celle-ci.
7. Vous ne pouvez pas créer de nouvelles unités imbriquées OUs sous l'unité d'organisation de sécurité (unité d'organisation principale).

Detective Control Concurrence

5 novembre 2021

(Mise à jour facultative pour la zone d'atterrissage de la AWS Control Tower)

AWSLes commandes de détection de Control Tower prennent désormais en charge les opérations simultanées pour les commandes de détection, améliorant ainsi 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 l'accès en écriture publique aux compartiments Amazon S3 est activé MFA pour l'utilisateur root et détectez si l'accès public en écriture aux compartiments Amazon S3 est autorisé).
- Activez différents contrôles de détection simultanément sur différents OUs appareils.
- 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 sites OUs n'est pas prise en charge.
- La simultanéité des contrôles préventifs n'est pas prise en charge.

Découvrez les améliorations apportées par Detective Control à la concurrence dans toutes les versions de 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 d'atterrissage de la AWS Control Tower)

AWSControl Tower est désormais disponible en deux versions supplémentaires AWS Régions : Amérique du Sud (Sao Paulo) et Europe (Paris). Cette mise à jour étend la disponibilité de 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 que AWS Control Tower crée et gère votre environnement multi-comptes.

Si vous possédez déjà un environnement AWS Control Tower et que vous souhaitez étendre ou supprimer les fonctionnalités de gouvernance de 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 d'atterrissage, vous devez [mettre à jour tous les comptes régis par AWS Control Tower](#).

Désélection de la région

29 juillet 2021

(Mise à jour facultative pour la zone d'atterrissage de la AWS Control Tower)

AWS La désélection de la région Control Tower améliore votre capacité à gérer l'empreinte géographique des ressources de votre AWS Control Tower. Vous pouvez désélectionner les régions que vous ne souhaitez plus voir gouvernées par 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 votre version de la zone d'atterrissage de 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 une journalisation, une surveillance et des contrôles centralisés, dans les régions que vous avez choisies dans les comptes. Choisir de désélectionner une région et de supprimer la gouvernance de la AWS Control Tower de cette région supprime cette fonctionnalité de gouvernance, mais cela n'empêche pas la capacité de vos utilisateurs à déployer AWS ressources ou charges de travail dans ces régions.

AWSControl Tower fonctionne avec AWS Systèmes de gestion des clés

28 juillet 2021

(Mise à jour facultative pour la zone d'atterrissage de la AWS Control Tower)

AWSControl Tower vous offre la possibilité d'utiliser un AWS Service de gestion des clés (AWS KMS) clé. Une clé est fournie et gérée par vous, afin de sécuriser les services déployés par AWS Control Tower, notamment AWS CloudTrail, AWS Config, et les données Amazon S3 associées. AWS KMS

chiffrement est un niveau de cryptage amélioré par rapport au cryptage SSE -S3 que AWS Control Tower utilise par défaut.

L'intégration de AWS KMSLe soutien apporté à AWS Control Tower s'aligne sur AWS Bonnes pratiques de sécurité fondamentales, qui recommandent une couche de sécurité supplémentaire pour vos fichiers journaux sensibles. Vous devez utiliser AWS KMS—clés gérées (SSE-KMS) pour le chiffrement au repos. AWS KMSLe support de chiffrement 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 Configuration des KMStouches lors de la configuration initiale de votre zone d'atterrissage. Vous pouvez choisir une KMS clé existante ou sélectionner un bouton qui vous dirige vers le AWS KMSconsole pour en créer une nouvelle. Vous avez également la possibilité de passer du chiffrement par défaut à SSE une cléKMS, ou à une KMS clé différenteSSE.

Pour une zone d'atterrissage AWS de Control Tower existante, vous pouvez effectuer une mise à jour pour commencer à utiliser AWS KMSclés.

Contrôles renommés, fonctionnalités inchangées

26 juillet 2021

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower)

AWSControl Tower est en train de réviser les noms et descriptions de certains contrôles 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.

AWSControl Tower scanne SCPs tous les jours pour détecter toute dérive

11 mai 2021

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower)

AWSControl Tower effectue désormais des scans automatisés quotidiens de votre SCPs manette pour vérifier que les commandes correspondantes sont correctement appliquées et qu'elles n'ont pas dérivé. Si un scan détecte une dérive, vous recevrez une notification. AWSControl Tower n'envoie qu'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 objet de dérive ne soit trouvé.

Noms OUs et comptes personnalisés

16 avril 2021

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower)

AWSControl Tower vous permet désormais de personnaliser le nom de votre zone d'atterrissage. Vous pouvez conserver les noms recommandés par AWS Control Tower pour les unités organisationnelles (OUs) 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 comptes OUs et principaux correspondent aux AWS guide des meilleures pratiques multi-comptes. 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 pour améliorer notre alignement sur l'ensemble AWS guide des meilleures pratiques en matière de dénomination.

Les nouveaux clients verront ces nouveaux noms d'unités d'organisation. Les clients existants continueront de voir leurs noms d'origine OUs. 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 le AWS Console de gestion, accédez à la console AWS Control Tower, puis sélectionnez Set up landing zone en haut à droite. Pour plus

d'informations, vous pouvez lire comment planifier la zone d'atterrissage AWS de votre Control Tower.

AWS Zone d'atterrissage de la Control Tower, version 2.7

8 avril 2021

(Mise à jour requise pour la zone d'atterrissage de AWS Control Tower vers la version 2.7. Pour plus d'informations, voir [Mettez à jour votre zone de landing zone](#))

Avec la version 2.7 de 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 AWS de la Control Tower. Nous avons ajusté les directives relatives à quatre contrôles d'archivage des logs existants, passant de obligatoires à facultatifs, car ils définissent la politique pour les ressources extérieures à AWS Control Tower. Ce changement et cette extension du contrôle permettent de séparer la gouvernance des archives de logs pour les ressources au sein de 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 de AWS Archives du journal. Les environnements AWS Control Tower existants maintiendront ces quatre commandes modifiées activées automatiquement, pour garantir la cohérence de l'environnement ; toutefois, ces commandes électives peuvent désormais être désactivées. Les nouveaux environnements AWS de Control Tower doivent permettre toutes les commandes électives. 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 l'archive des journaux
- Interdire les modifications apportées à la configuration du cycle de vie pour les compartiments S3 créés par AWS Control Tower dans Log Archive

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]

AWS La version 2.7 de Control Tower inclut des modifications apportées au plan de la zone d'atterrissage de 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 de AWS Control Tower `BlockPublicAccess` s'active automatiquement sur les buckets 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](#).
- AWS La version 2.7 de Control Tower inclut une exigence pour HTTPS. Toutes les demandes envoyées aux buckets S3 déployés par AWS Control Tower doivent utiliser le protocole secure socket layer (SSL). Seules les HTTPS demandes sont autorisées à être transmises. Si vous utilisez HTTP (withoutSSL) comme point de terminaison pour envoyer les demandes, cette modification génère une erreur de refus d'accès, qui peut potentiellement 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 pour utiliser TLS au lieu de HTTP.

Trois nouveaux AWS Régions disponibles

8 avril 2021

(Mise à jour requise pour la zone d'atterrissage de la AWS Control Tower)

AWSControl Tower est disponible en trois versions supplémentaires AWS Régions : région Asie-Pacifique (Tokyo), région Asie-Pacifique (Séoul) et 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 de AWS Control Tower)

AWSLa sélection de la région Control Tower permet de mieux gérer l'empreinte géographique des ressources de votre AWS Control Tower. Pour augmenter le nombre de régions dans lesquelles vous hébergez AWS ressources ou 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 AWS de votre zone d'atterrissage de 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, consultez [Configurez les régions AWS de votre Control Tower](#).

AWSControl Tower étend désormais la gouvernance à l'existant OUs dans votre AWS organisations

28 janvier 2021

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower)

Étendez la gouvernance aux unités organisationnelles existantes (OUs) (celles qui ne font pas partie de AWS Control Tower) depuis la console AWS Control Tower. Grâce à cette fonctionnalité, vous

pouvez intégrer des comptes de haut niveau OUs et des comptes inclus sous la gouvernance AWS de Control Tower. Pour plus d'informations sur l'extension de la gouvernance à l'ensemble d'une unité d'organisation, consultez [Enregistrer une unité organisationnelle existante auprès AWS de 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, consultez [Causes 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](#).

AWSControl Tower fournit des mises à jour groupées des comptes

28 janvier 2021

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower)

Grâce à la fonctionnalité de mise à jour groupée, vous pouvez désormais mettre à jour tous les comptes d'un compte enregistré AWS Organizations unité organisationnelle (UO) contenant jusqu'à 300 comptes, en un seul clic, depuis le tableau de bord de AWS Control Tower. Cela est particulièrement utile lorsque vous mettez à jour votre zone d'atterrissage de AWS Control Tower et que vous devez également mettre à jour vos comptes enregistrés 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 la zone d'atterrissage de votre AWS Control Tower pour l'étendre à de nouvelles régions, ou lorsque vous souhaitez réenregistrer une unité organisationnelle 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, consultez [Mettez à jour votre zone de landing zone](#).

Pour plus d'informations sur l'enregistrement ou le réenregistrement d'une UO, consultez [Enregistrer une unité organisationnelle existante auprès AWS de Control Tower](#).

janvier - décembre 2020

En 2020, AWS Control Tower a publié les mises à jour suivantes :

- [AWS La console Control Tower est désormais reliée à une interface externe AWS Règles de configuration](#)
- [AWS Control Tower est désormais disponible dans d'autres régions](#)
- [Mise à jour du garde-corps](#)
- [AWS La console Control Tower affiche plus de détails sur OUs les comptes](#)
- [Utilisez AWS Control Tower pour configurer de nouveaux comptes multiples AWS environnements dans AWS Organizations](#)
- [Personnalisations de la AWS solution Control Tower](#)
- [Disponibilité générale de la version 2.3 de AWS Control Tower](#)
- [Provisionnement de compte en une seule étape dans Control Tower AWS](#)
- [AWS Outil de mise hors service de Control Tower](#)
- [AWS Notifications d'événements liés au cycle de vie de la Control Tower](#)

AWS La console Control Tower est désormais reliée à une interface externe AWS Règles de configuration

29 décembre 2020

(Mise à jour requise pour la zone d'atterrissage de AWS Control Tower vers la version 2.6. Pour plus d'informations, voir [Mettez à jour votre zone de landing zone](#))

AWS Control Tower inclut désormais un agrégateur au niveau de l'organisation, qui aide à détecter les données externes AWS Règles de configuration. Cela vous permet de voir dans la console AWS Control Tower l'existence de AWS Règles de configuration en plus de celles-ci AWS Règles de configuration créées par AWS Control Tower. L'agrégateur permet à AWS Control Tower de détecter les règles externes et de fournir un lien vers le AWS Config console sans que AWS Control Tower n'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 [How AWS Control Tower aggregates AWS Config règles dans les comptes](#) non gérés OUs et.

AWSControl Tower est désormais disponible dans d'autres régions

18 novembre 2020

(Mise à jour requise pour la zone d'atterrissage de AWS Control Tower vers la version 2.5. Pour plus d'informations, voir [Mettez à jour votre zone de landing zone](#))

AWSControl Tower est désormais disponible en 5 versions supplémentaires AWS Régions :

- Région Asie-Pacifique (Singapour)
- Région Europe (Francfort)
- Région Europe (Londres)
- Région Europe (Stockholm)
- Région Canada (Centre)

L'ajout de ces 5 AWS Les régions sont le seul changement introduit dans la version 2.5 de AWS Control Tower.

AWSControl 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 en version 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 d'atterrissage vers la version 2.5, vous devez mettre à jour manuellement tous les comptes inscrits pour que AWS Control Tower puisse gouverner dans les 10 comptes pris en charge AWS Régions. Pour plus d'informations, veuillez consulter [Configurez les régions AWS de votre Control Tower](#).

Mise à jour du garde-corps

8 octobre 2020

(Aucune mise à jour requise pour la zone d'atterrissage de 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 sur les comptes inscrits automatiquement dans AWS Control Tower. La version précédente du contrôle empêchait la création de ce rôle.

Pour plus d'informations, voir Interdire [les modifications apportées à AWS IAM Rôles définis par AWS Control Tower et AWS CloudFormation](#) dans le guide de référence de AWS Control Tower Controls.

AWS La console Control Tower affiche plus de détails sur OUs les comptes

22 juillet 2020

(Aucune mise à jour requise pour la zone d'atterrissage de 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 voir plus de détails sur votre AWS comptes et unités organisationnelles (OUs). La page Accounts 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 comptes multiples AWS environnements dans AWS Organizations

22 avril 2020

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower)

AWS Organizations les clients peuvent désormais utiliser AWS Control Tower pour gérer les unités organisationnelles (OUs) et les comptes nouvellement créés en tirant parti de ces nouvelles fonctionnalités :

- Existant AWS Organizations les clients peuvent désormais configurer une nouvelle zone de landing zone pour les nouvelles unités organisationnelles (OUs) dans leur compte de gestion existant. Vous pouvez créer de nouveaux comptes OUs dans AWS Control Tower et créer de nouveaux comptes dans ceux OUs dont la gouvernance est AWS assurée par Control Tower.
- AWS Organizations les clients peuvent inscrire des comptes existants à l'aide du processus d'inscription ou à l'aide de scripts.

AWSControl Tower fournit un service d'orchestration qui utilise d'autres AWS services. Il est conçu pour les organisations possédant plusieurs comptes et pour les équipes qui recherchent le moyen le plus simple de configurer leur compte multiple nouveau ou existant AWS environnement et gouvernance 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 fournir de nouveaux AWS comptes rapidement, sans se soucier indûment de la conformité.

Pour plus d'informations sur la configuration d'une zone d'atterrissage, consultez [Planifiez la zone d'atterrissage 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 en compte Enroll. Il permet désormais l'inscription des personnes existantes AWS ainsi que la création de nouveaux comptes. Pour de plus amples informations, veuillez consulter [Inscrire un compte existant](#).

Personnalisations de la AWS solution Control Tower

17 mars 2020

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower)

AWSControl Tower inclut désormais une nouvelle implémentation de référence qui vous permet d'appliquer facilement des modèles et des politiques personnalisés à votre zone d'atterrissage AWS Control Tower.

Grâce aux personnalisations de AWS Control Tower, vous pouvez utiliser 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 de service personnalisées (SCPs) à ces comptes en plus de celles SCPs déjà fournies par AWS Control Tower. Les personnalisations du pipeline AWS Control Tower s'intègrent aux événements et aux notifications du cycle de vie de 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 d'atterrissage.

La documentation de déploiement de cette architecture de solution AWS Control Tower est disponible via le [AWS Page Web sur les solutions](#).

Disponibilité générale de la version 2.3 de AWS Control Tower

5 mars 2020

(Mise à jour requise pour la zone d'atterrissage de la AWS Control Tower. Pour plus d'informations, voir [Mettez à jour votre zone de landing zone.](#))

AWSControl Tower est désormais disponible en Asie-Pacifique (Sydney) AWS Région, en plus des régions de l'est des États-Unis (Ohio), de l'est des États-Unis (Virginie du Nord), de l'ouest des États-Unis (Oregon) et de l'Europe (Irlande). L'ajout de la région Asie-Pacifique (Sydney) est le seul changement introduit pour la version 2.3 de AWS Control Tower.

Si vous n'avez jamais utilisé AWS Control Tower auparavant, vous pouvez le lancer dès aujourd'hui dans toutes les 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. Ensuite, 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 [Configure your AWS Control Tower Regions.](#)

Provisionnement de compte en une seule étape dans Control Tower AWS

2 mars 2020

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower)

AWSControl Tower prend désormais en charge le provisionnement de comptes en une seule étape via la console AWS Control Tower. Cette fonctionnalité vous permet de créer 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. AWSControl Tower attribue la même adresse e-mail au compte provisionné et à l'utilisateur d'authentification unique (IAMIdentity 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 la fabrique 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 de s'inscrire AWS comptes. Pour de plus amples informations, veuillez consulter [Inscrire un compte existant](#).

AWSOutil de mise hors service de Control Tower

28 février 2020

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower)

AWSControl 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 souhaitez 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](#)

AWSNotifications d'événements liés au cycle de vie de la Control Tower

22 janvier 2020

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower)

AWSControl 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 de AWS Control Tower susceptible de modifier l'état de ressources telles que les unités organisationnelles (OUs), les comptes et les contrôles créés et gérés par AWS Control Tower. Les événements du cycle de vie sont enregistrés sous la forme AWS CloudTrail événements et livrés à Amazon EventBridge sous forme d'événements.

AWSControl 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 unité organisationnelle ; activation ou désactivation d'un contrôle sur une unité d'organisation ; utilisation de Account Factory pour créer un nouveau compte ou pour déplacer un compte vers une autre unité d'organisation.

AWSControl Tower utilise plusieurs AWS services pour créer et gérer un multicompte basé sur les meilleures pratiques AWS environnement. L'exécution d'une action de la 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 de AWS Control Tower](#)
- [Nouvelles commandes électives dans AWS Control Tower](#)
- [Nouvelles commandes de détective dans AWS Control Tower](#)
- [AWSControl 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 de AWS Control Tower](#)

Disponibilité générale de la version 2.2 de AWS Control Tower

13 novembre 2019

(Mise à jour requise pour la zone d'atterrissage de la AWS Control Tower. Pour plus d'informations, voir [Mettez à jour votre zone de landing zone.](#))

AWSLa version 2.2 de Control Tower propose 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 de AWS Config Autorisations d'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 pour votre AWS environnement. Lorsque vous créez votre zone d'atterrissage AWS Control Tower, celle-ci ainsi que toutes les unités organisationnelles (OUs), comptes et 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 de plus amples informations, veuillez consulter [Déterminez et corrigez les dérives dans AWS Control Tower](#).

Nouvelles commandes électives dans AWS Control Tower

05 septembre 2019

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower)

AWSControl 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 pour votre AWS environnement. Les barrières de sécurité vous permettent d'exprimer vos intentions de stratégie. Pour plus d'informations, consultez [À propos des commandes dans AWS Control Tower](#).

Nouvelles commandes de détective dans AWS Control Tower

25 août 2019

(Aucune mise à jour requise pour la zone d'atterrissage de AWS Control Tower)

AWSControl Tower inclut désormais les huit nouvelles commandes de détection suivantes :

- [Détecter si la gestion des versions pour les compartiments Amazon S3 est activée](#)
- [Détectez si cette option MFA est activée pour IAM les utilisateurs du AWS Console](#)
- [Détecter si MFA c'est activé pour IAM les utilisateurs](#)
- [Détecter si Amazon EBS Optimization est activé pour les EC2 instances Amazon](#)
- [Détecter si EBS des volumes Amazon sont attachés à des EC2 instances Amazon](#)
- [Détecter si l'accès public aux instances RDS de base de données Amazon est activé](#)
- [Détecter si l'accès public aux instantanés RDS de base de données Amazon est activé](#)
- [Détecter si le chiffrement du stockage est activé pour les instances RDS de base de données Amazon](#)

Un contrôle est une règle de haut niveau qui fournit une gouvernance continue pour votre AWS environnement. 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 commandes dans AWS Control Tower](#).

AWSControl 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 de AWS Control Tower)

Dans AWS Control Tower, vous pouvez désormais soumettre des adresses e-mail pour des comptes partagés (archive des journaux et membre de l'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 de AWS Control Tower

24 juin 2019

(Mise à jour requise pour la zone d'atterrissage de la AWS Control Tower. Pour plus d'informations, voir [Mettre à jour votre zone d'atterrissage.](#))

AWSControl Tower est désormais généralement disponible et pris en charge pour une utilisation en production. AWSControl Tower est destiné aux organisations possédant plusieurs comptes et aux équipes qui recherchent le moyen le plus simple de configurer leur nouveau multicompte AWS environnement et gouvernance 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 fournir de nouvelles AWS comptes rapidement.

À l'aide AWS de Control Tower, vous pouvez [configurer une zone d'atterrissage](#) qui utilise les meilleures pratiques, telles que la configuration d'une [structure multi-comptes](#) à l'aide de AWS Organizations, en gérant les identités des utilisateurs et les accès fédérés avec AWS IAM Identity Center, en permettant le provisionnement des comptes via Service Catalog et en créant une archive de journaux centralisée à l'aide de AWS CloudTrail and 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 de AWS Control Tower fournit une visibilité centralisée sur AWS environnement, y compris 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. Il n'y a aucun frais supplémentaire ni engagement initial pour utiliser AWS Control Tower. Vous ne payez que pour ceux-ci AWS services que vous avez activés pour configurer une zone d'atterrissage et implémenter les contrôles sélectionnés.

Historique du document

- Dernière mise à jour de la documentation : 30 août 2024

Le tableau suivant décrit les modifications importantes apportées au guide de l'utilisateur AWS de la Control Tower. Pour recevoir des notifications concernant les mises à jour de la documentation, vous pouvez vous abonner au RSS flux.

Modification	Description	Date
AWSControl Tower prend en charge jusqu'à 1 000 comptes par unité d'organisation	Une augmentation de la limite de comptes par unité d'organisation.	30 août 2024
AWSControl Tower ajoute une sélection de versions pour les zones d'atterrissage	Mettez à jour ou réparez votre zone de landing zone sans passer à la dernière version, si vous utilisez la version 3.1 ou une version plus récente.	15 août 2024
GetControl et ListControls API opérations disponibles	Deux nouvelles opérations du catalogue de contrôles vous permettent de trouver plus d'informations sur les contrôles .	6 août 2024
AWSControl Tower soutient AFT et CfCT dans les régions optionnelles	AFTet CFCT sont disponibles en supplément Régions AWS.	18 juillet 2024
AWSControl Tower ajoute le ListLandingZoneOperations API	Une nouveauté API qui vous permet de récupérer les opérations récentes pour votre zone de landing zone.	26 juin 2024

AWSControl 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
AWSControl Tower disponible en AWS Région de Calgary Ouest (Canada)	AWSControl Tower est disponible dans la région du Canada Ouest (Calgary).	3 mai 2024
AWSControl Tower prend en charge les ajustements de quotas en libre-service	AWSControl Tower est intégré à AWS Service Quotas dans la console.	25 avril 2024
Documentation des commandes déplacée vers un nouveau guide	AWSControl Tower a publié le guide de référence sur les contrôles.	21 avril 2024
Marquage des EnabledControl ressources dans AWS CloudFormation	AWSControl Tower prend en charge l'ajout de balises aux EnabledControl ressources, au moyen de AWS CloudFormation modèles.	22 février 2024
Base de référence APIs disponible	AWSControl Tower a publié une nouvelle version APIs pour l'enregistrement OUs programmatique.	14 février 2024
AWSZone d'atterrissage de la Control Tower, version 3.3	AWSLa version 3.3 de la zone d'atterrissage de Control Tower est disponible.	14 décembre 2023
AWSControl Tower annonce des contrôles pour favoriser la souveraineté numérique	AWSControl Tower a publié un ensemble de contrôles pour aider les clients à répondre aux exigences de souveraineté numérique.	27 novembre 2023

AWSControl Tower soutient la zone d'atterrissage APIs	AWSControl Tower prend en charge la configuration et le lancement de zones d'atterrissage à l'aide de nouvelles APIs.	26 novembre 2023
AWSControl Tower prend en charge le balisage des commandes activées	AWSControl Tower prend en charge le balisage des commandes activées, dans la console et avec les nouvelles APIs.	10 novembre 2023
AWSControl Tower disponible en Asie-Pacifique (Melbourne) Région AWS	Disponible dans la région Asie-Pacifique (Melbourne).	3 novembre 2023
Nouveau contrôle API disponible	AWSControl Tower a publié un nouveau contrôleAPI.	14 octobre 2023
AWSControl Tower lance de nouvelles commandes	AWSControl Tower a publié de nouvelles commandes proactives et détectives.	5 octobre 2023
AWSControl Tower signale une dérive liée à la désactivation de l'accès sécurisé	AWSControl Tower avertit les clients en cas de dérive, si les clients désactivent l'accès sécurisé à AWS Control Tower dans AWS Organizations.	21 septembre 2023
AWSControl Tower disponible en quatre versions supplémentaires Régions AWS	Disponible en Asie-Pacifique (Hyderabad), en Europe (Espagne et Zurich) et au Moyen-Orient (UAE).	13 septembre 2023
AWSControl Tower disponible dans la région de Tel Aviv	AWSControl Tower est disponible dans la région de Tel Aviv, il-central-1.	28 août 2023

AWSControl Tower lance 28 nouveaux contrôles proactifs	AWSControl Tower a publié 28 nouveaux contrôles proactifs.	24 juillet 2023
AWSControl Tower déconseille 2 contrôles	AWSControl Tower supprimer a deux commandes de la bibliothèque de commandes à compter du 18 août 2023.	18 juillet 2023
AWSLa zone d'atterrissage 3.2 de la Control Tower est disponible	AWSLa version 3.2 de la zone d'atterrissage de Control Tower est disponible.	16 juin 2023
AWSControl Tower gère les comptes en fonction de leur identifiant	AWSControl Tower suit le AWS l'identifiant du compte, plutôt que l'adresse e-mail du compte.	14 juin 2023
Contrôles de détection supplémentaires du Security Hub disponibles	AWSControl Tower ajoute dix nouveaux contrôles à la bibliothèque de contrôles, pour le Security Hub Service-Managed Standard : AWS Control Tower.	12 juin 2023
AWSControl Tower publie des tables de métadonnées de contrôle	AWSControl 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 IAMautogestion disponible pour la zone d'atterrissage	AWSControl Tower aide désormais les clients à choisir leur fournisseur d'identité pour une zone d'atterrissage.	6 juin 2023

Nouveau rôle ajouté	AWSControl Tower a ajouté un nouveau rôle lié au service et AWSServiceRoleForAWSControlTowerla politique associée. AWSControlTowerAccountServiceRolePolicy	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 supplémentaires disponibles	Les nouveaux contrôles proactifs vous aident à gérer votre environnement multi-comptes et à atteindre des objectifs de contrôle spécifiques.	19 mai 2023
Sept régions supplémentaires disponibles	AWSControl Tower est désormais disponible en sept versions supplémentaires 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 les AWSControlTowerServiceRolePolicy afin que AWS Control Tower puisse appeler les EnableRegion ListRegions , GetRegionOptStatus APIs qui sont implémentés par le AWS Service de gestion de compte.	6 avril 2023
Suivi des demandes de personnalisation du compte généralement disponible	AWSControl 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
IAM mise à jour des meilleures pratiques	Guide mis à jour pour s'aligner sur les recommandations des IAM meilleures pratiques. Pour plus d'informations, consultez la section Bonnes pratiques en matière de sécurité dans IAM .	15 février 2023
AWS La zone d'atterrissage 3.1 de la Control Tower est disponible	AWS La zone d'atterrissage 3.1 de 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

<u>Opérations de compte simultanées</u>	AWSControl 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
<u>Les contrôles proactifs facilitent le provisionnement des ressources</u>	AWSControl Tower prend désormais en charge les contrôles proactifs, mis en œuvre via AWS CloudFormation crochets.	28 novembre 2022
<u>Personnalisation du compte en usine disponible</u>	AWSControl Tower prend désormais en charge le provisionnement des comptes grâce à des modèles de compte personnalisables, appelés blueprints, directement depuis la console AWS Control Tower.	28 novembre 2022
<u>État de conformité consultable par tous AWS Config règles</u>	AWSControl Tower affiche désormais l'état de conformité de tous AWS Config règles déployées dans les unités organisationnelles enregistrées auprès AWS de Control Tower.	18 novembre 2022

Passage à une politique gérée	Nous l'avons modifiée AWSControlTowerServiceRolePolicy afin que AWS Control Tower puisse assumer le AWSControlTowerBlueprintAccess rôle, ce qui est nécessaire pour les personnalisations d'Account Factory.	28 octobre 2022
API pour les commandes , AWS CloudFormation ressource	AWSControl Tower prend désormais en charge l'activation et la désactivation des commandes par le biais d'une série d'API appels, et d'un nouveau 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 CloudTrail 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](#)

AWSControl Tower prend en charge la réparation en cas de dérive des rôles, sans réparation complète de la zone d'atterrissage.

11 août 2022

[Version 3.0 disponible](#)

AWSLa version 3.0 de Control Tower landing zone passe d'une version basée sur un compte AWS CloudTrail des sentiers vers des sentiers basés sur l'organisation, et il met à jour la politique gérée pour activer les sentiers au niveau de l'organisation. Il vous permet d'agréger AWS Config informations dans votre région d'origine uniquement. 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 OUs et les comptes](#)

La nouvelle page Organisation de AWS Control Tower présente une vue hiérarchique de toutes les unités organisationnelles (OUs) et de tous les comptes.

18 juillet 2022

<u>Passage à une politique gérée</u>	Nous avons modifié le AWSControlTowerServiceRolePolicy afin que les clients puissent avoir un niveau organisationnel AWS CloudTrail pistes à agréger AWS CloudTrail journaux.	20 juin 2022
<u>Inscription et mise à jour simplifiées pour les comptes des membres</u>	AWSControl 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
<u>AFT prend en charge la personnalisation des comptes partagés</u>	AWSControl Tower Account Factory for Terraform prend désormais en charge la personnalisation du compte de gestion, AWS de l'archivage des journaux et des comptes d'audit de Control Tower.	27 mai 2022
<u>Opérations simultanées pour tous les contrôles optionnels</u>	AWSControl 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

<u>Comptes de sécurité et de journalisation existants</u>	AWSControl 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 d'atterrissage.	16 mai 2022
<u>Version 2.9 disponible</u>	AWSLa version 2.9 de 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
<u>Support mis à jour pour AWS meilleures pratiques, version 2.8 disponible</u>	AWSLa version 2.8 de Control Tower landing zone fournit une assistance supplémentaire pour garantir que vos charges de travail et AWS les comptes sont conformes à AWS meilleures pratiques.	10 février 2022
<u>Refuser le contrôle des régions</u>	AWSControl Tower inclut désormais une commande qui vous permet de restreindre l'accès à AWS Régions, pour répondre aux préoccupations en matière de conformité et de réglementation.	30 novembre 2021
<u>Contrôles de résidence des données</u>	AWSControl Tower prend désormais en charge des contrôles qui vous aident à gérer la résidence des données avec un contrôle granulaire.	30 novembre 2021

AWSControl Tower Account Factory pour Terraform	AWSControl 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 imbriquées. OUs	18 novembre 2021
Disponible imbriqué OUs	AWSControl Tower permet désormais à votre zone d'atterrissage de contenir des structures UO imbriquées.	16 novembre 2021
Detective contrôle la simultanéité	AWSLes commandes de détection de Control Tower prennent désormais en charge les opérations d'activation et de désactivation simultanées.	5 novembre 2021
Deux nouvelles régions disponibles	AWSControl Tower est désormais disponible en deux nouvelles versions AWS Régions, région Europe (Paris) et région Amérique du Sud (São Paulo).	29 juillet 2021
Désélection de région	Vous pouvez désélectionner AWS Régions que vous ne souhaitez plus gouverner par le biais AWS de Control Tower.	29 juillet 2021

KMSclés disponibles	Vous pouvez éventuellement créer ou choisir KMS des clés que vous gérez pour chiffrer vos données et vos ressources.	28 juillet 2021
Passage à une politique gérée	Nous avons modifié le AWSControlTowerServiceRolePolicy afin que les clients puissent utiliser leurs propres clés de KMS chiffrement pour 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 produits gérés SCPs	AWSControl Tower effectue des scans automatisés quotidiens du système géré SCPs pour détecter toute dérive.	11 mai 2021
Noms OUs et comptes personnalisés	AWSControl Tower vous permet de fournir des noms personnalisés pendant le processus de configuration de la zone d'atterrissage, pour les comptes essentiels OUs et pour les comptes, sans créer de dérive.	16 avril 2021

[La mise hors service d'une zone d'atterrissage est en libre-service](#)

AWSControl Tower vous permet désormais de mettre hors service une zone d'atterrissage sans contacter 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 de AWS Control Tower.

9 avril 2021

[Trois régions supplémentaires](#)

AWSControl Tower est désormais disponible en trois versions supplémentaires AWS Régions : région Asie-Pacifique (Tokyo), région Asie-Pacifique (Séoul) et région Asie-Pacifique (Mumbai).

08 avril 2021

[Nouvelles commandes Log Archive, version 2.7 de la zone d'atterrissage disponible](#)

Quatre nouveaux contrôles Log Archive fournissent une gouvernance des archives de log sur les ressources de la AWS Control Tower, indépendamment de la gouvernance des ressources 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 d'atterrissage de AWS Control Tower inclut une exigence HTTPS qui ne peut pas être annulée après la mise à jour.

08 avril 2021

[Sélection de la région](#)

AWS La sélection de la région Control Tower permet de mieux gérer l'empreinte géographique des ressources de votre AWS Control Tower. Pour augmenter le nombre de régions dans lesquelles vous hébergez AWS ressources ou 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 UO et gérez tous ses comptes avec AWS Control Tower en une seule fois](#)

AWSControl 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 de comptes multiples dans les comptes enregistrés OUs](#)

Vous pouvez désormais mettre à jour tous les comptes de tous les comptes enregistrés AWS Organizations unité organisationnelle (UO) contenant jusqu'à 300 comptes, en un seul clic, depuis le tableau de bord de 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 comptes non gérés OUs](#)

Un nouveau rôle aide à détecter les facteurs externes AWS Config règles, afin que AWS Control Tower n'ait pas besoin d'accéder à des comptes non gérés.

29 décembre 2020

[AWSControl Tower est disponible en plusieurs versions AWS Régions.](#)

AWSControl 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 en version 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 d'atterrissage vers la version 2.5, vous devez mettre à jour manuellement tous les comptes inscrits pour que AWS Control Tower puisse gouverner dans les 10 comptes pris en charge AWS Régions.

18 novembre 2020

[Mise à jour du contrôle](#)

Une version mise à jour a été publiée pour le contrôle obligatoireAWS-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 la zone d'atterrissage AWS de votre Control Tower.

18 septembre 2020

[AWS La console Control Tower affiche plus de détails sur les comptes OUs et les comptes.](#)

Dans la console AWS Control Tower, vous pouvez voir plus de détails sur votre AWS comptes et unités organisationnelles (OUs). La page « Comptes » répertorie désormais tous les comptes de votre organisation, quel que soit l'unité d'organisation ou le statut d'inscription à AWS Control Tower. Vous pouvez désormais rechercher, trier et filtrer dans toutes les tables.

22 juillet 2020

[AWS Control Tower permet aux organisations existantes de créer une zone d'atterrissage](#)

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 AWS de Control Tower a été renommée compte Enroll et permet désormais d'enregistrer des comptes existants AWS ainsi que la création de nouveaux comptes.

16 avril 2020

[AWSControl Tower est désormais disponible en Asie-Pacifique](#)

AWSControl Tower est désormais disponible pour être déployée en Asie-Pacifique (Sydney) AWS Région. 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 AWS de la 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 la 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 de AWS Control Tower permettent à votre organisation et à vos ressources de rester alignées sur votre environnement.

6 septembre 2019

[Des commandes de détection supplémentaires sont disponibles pour AWS Control Tower](#)

Les commandes Detective AWS de Control Tower fournissent des informations sur l'état de votre organisation et de ses ressources.

27 août 2019

[AWSControl Tower est désormais disponible pour tous](#)

AWSControl Tower est un service qui offre le moyen le plus simple de configurer et de gérer vos comptes multiples AWS environnement 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.