Guide de mise en œuvre

Réponse de sécurité automatisée sur AWS

Réponse de sécurité automatisée sur AWS: Guide de mise en œuvre

Table of Contents

Gérez automatiquement les menaces de sécurité grâce à des actions de réponse et de correction prédéfinies dans AWS Security Hub

Ce guide de mise en œuvre fournit une vue d'ensemble de la solution Automated Security Response on AWS, de son architecture de référence et de ses composants, des considérations relatives à la planification du déploiement, ainsi que des étapes de configuration pour le déploiement de la solution Automated Security Response on AWS sur le cloud Amazon Web Services (AWS).

Utilisez ce tableau de navigation pour trouver rapidement les réponses aux questions suivantes :

Si tu veux...	Lisez.
Connaître le coût de fonctionnement de cette solution	Coût
Comprendre les considérations de sécurité liées à cette solution	Sécurité
Savoir comment planifier les quotas pour cette solution	Quotas
Découvrez quelles régions AWS sont prises en charge pour cette solution	Régions AWS prises en charge
Consultez ou téléchargez le CloudFormation modèle AWS inclus dans cette solution pour déployer automatiquement les ressources d'infrastructure (la « pile ») de cette solution	CloudFormation Modèles AWS
Accédez au code source et utilisez éventuell ement l'AWS Cloud Development Kit (AWS CDK) pour déployer la solution.	GitHub référentiel

L'évolution continue de la sécurité nécessite des mesures proactives pour sécuriser les données, ce qui peut rendre la réaction des équipes de sécurité difficile, coûteuse et chronophage. La solution

Automated Security Response on AWS vous aide à réagir rapidement pour résoudre les problèmes de sécurité en fournissant des réponses prédéfinies et des actions correctives basées sur les normes de conformité du secteur et les meilleures pratiques.

Automated Security Response on AWS est une solution AWS qui fonctionne avec AWS Security Hub pour améliorer votre sécurité et vous aider à aligner vos charges de travail sur les meilleures pratiques du pilier de sécurité Well-Architected (0). SEC1 Cette solution permet aux clients d'AWS Security Hub de résoudre plus facilement les problèmes de sécurité courants et d'améliorer leur niveau de sécurité dans AWS.

Vous pouvez sélectionner des playbooks spécifiques à déployer sur votre compte principal Security Hub. Chaque playbook contient les actions personnalisées, les rôles Identity and Access Management (IAM), les EventBridge règles Amazon, les documents d'automatisation d'AWS Systems Manager, les fonctions AWS Lambda et les fonctions AWS Step Functions nécessaires pour démarrer un flux de travail de correction au sein d'un seul compte AWS ou sur plusieurs comptes. Les correctifs fonctionnent à partir du menu Actions d'AWS Security Hub et permettent aux utilisateurs autorisés de corriger une découverte concernant l'ensemble de leurs comptes gérés par AWS Security Hub en une seule action. Par exemple, vous pouvez appliquer les recommandations de l'AWS Foundations Benchmark du Center for Internet Security (CIS), une norme de conformité visant à sécuriser les ressources AWS, afin de garantir que les mots de passe expirent dans les 90 jours et d'appliquer le chiffrement des journaux d'événements stockés dans AWS.

> **Note**
>
> Les mesures correctives sont destinées aux situations d'urgence qui nécessitent une action immédiate. Cette solution apporte des modifications pour corriger les résultats uniquement lorsque vous l'avez initiée via la console de gestion AWS Security Hub, ou lorsque la correction automatique a été activée à l'aide de la table DynamoDB de configuration de correction. Pour annuler ces modifications, vous devez remettre manuellement les ressources dans leur état d'origine.
>
> Lorsque vous corrigez des ressources AWS déployées dans le cadre de la CloudFormation pile, sachez que cela peut provoquer une dérive. Dans la mesure du possible, corrigez les ressources de la pile en modifiant le code qui définit les ressources de la pile et en mettant à jour la pile. Pour plus d'informations, reportez-vous à Qu'est-ce que la dérive ? dans le guide de CloudFormation l'utilisateur AWS.

Automated Security Response on AWS inclut les correctifs relatifs aux normes de sécurité définies dans le cadre des directives suivantes :

- Centre pour la sécurité Internet (CIS) AWS Foundations Benchmark v1.2.0
- Test de référence CIS AWS Foundations v1.4.0
- Test de référence CIS AWS Foundations v3.0.0
- Bonnes pratiques de sécurité de base d'AWS (FSBP) v.1.0.0
- Norme de sécurité des données du secteur des cartes de paiement (PCI-DSS) v3.2.1
- Institut national des normes et de la technologie (NIST) SP 800-53 Rev. 5

La solution inclut également un manuel de contrôle de sécurité (SC) pour la fonctionnalité de consolidation des résultats de contrôle d'AWS Security Hub. Pour plus d'informations, reportez-vous à Playbooks. Nous vous recommandons d'utiliser le playbook SC ainsi que les résultats de contrôle consolidés dans Security Hub.

Ce guide de mise en œuvre aborde les considérations architecturales et les étapes de configuration pour le déploiement de la solution Automated Security Response on AWS dans le cloud AWS. Il inclut des liens vers des CloudFormation modèles AWS qui lancent, configurent et exécutent les services de calcul, de réseau, de stockage et autres services AWS nécessaires au déploiement de cette solution sur AWS, en utilisant les meilleures pratiques d'AWS en matière de sécurité et de disponibilité.

Le guide est destiné aux architectes d'infrastructure informatique, aux administrateurs et aux DevOps professionnels ayant une expérience pratique de l'architecture dans le cloud AWS.

Fonctionnalités et avantages

La réponse de sécurité automatisée sur AWS fournit les fonctionnalités suivantes :

Corriger automatiquement les résultats pour des contrôles spécifiques

Configurez la solution pour corriger automatiquement les résultats relatifs à des contrôles spécifiques en modifiant la table DynamoDB de configuration de correction déployée sur le compte administrateur.

Gérez les mesures correctives sur plusieurs comptes et régions à partir d'un seul emplacement

À partir d'un compte administrateur AWS Security Hub configuré comme destination d'agrégation pour les comptes et les régions de votre organisation, lancez une correction en cas de découverte dans tous les comptes et régions dans lesquels la solution est déployée.

Soyez informé des mesures correctives et des résultats

Abonnez-vous à la rubrique Amazon SNS déployée par la solution pour être averti lorsque des mesures correctives sont initiées et si elles ont réussi ou non.

Utiliser l'interface utilisateur Web pour démarrer, afficher et gérer les mesures correctives

Vous aurez la possibilité d'activer l'interface utilisateur Web de la solution lors du déploiement de la pile d'administration, qui fournira une vue complète et conviviale pour exécuter les corrections et visualiser toutes les corrections effectuées par la solution par le passé.

Intégrez des systèmes de tickets tels que Jira ou ServiceNow

Pour aider votre organisation à réagir aux mesures correctives (par exemple, en mettant à jour le code de votre infrastructure), cette solution peut envoyer des tickets vers votre système de billetterie externe.

Utiliser AWSConfig les mesures correctives dans les partitions GovCloud et Chine

Certaines des corrections incluses dans la solution sont des repackages de documents de AWSConfig correction appartenant à AWS qui sont disponibles sur la partition commerciale, mais pas en Chine ou en Chine. GovCloud Déployez cette solution pour utiliser ces documents dans ces partitions.

Étendez la solution grâce à des correctifs personnalisés et à des implémentations de Playbook

La solution est conçue pour être extensible et personnalisable. Pour spécifier une implémentation alternative de correction, déployez des documents d'automatisation AWS Systems Manager personnalisés et des rôles AWS IAM. Pour prendre en charge un tout nouvel ensemble de contrôles qui n'est pas implémenté par la solution, déployez un Playbook personnalisé.

Cas d’utilisation

Appliquez la conformité à une norme dans tous les comptes et régions de votre organisation

Déployez le Playbook pour une norme (par exemple, les meilleures pratiques de sécurité de base d'AWS) afin de pouvoir utiliser les correctifs fournis. Lancez automatiquement ou manuellement des

mesures correctives pour les ressources de tous les comptes et régions dans lesquels la solution est déployée afin de corriger les ressources non conformes.

Déployez des correctifs personnalisés ou des Playbooks pour répondre aux besoins de conformité de votre entreprise

Utilisez les composants d'Orchestrator fournis comme framework. Créez des solutions personnalisées pour gérer les out-of-compliance ressources en fonction des besoins spécifiques de votre organisation.

Concepts et définitions

Cette section décrit les concepts clés et définit la terminologie spécifique à cette solution :

remédiation, manuel de remédiation

Implémentation d'un ensemble d'étapes permettant de résoudre une constatation. Par exemple, une correction pour le contrôle Security Control (SC) Lambda.1 « Les politiques relatives aux fonctions Lambda doivent interdire l'accès public » modifierait la politique de la fonction AWS Lambda correspondante afin de supprimer les instructions autorisant l'accès public.

runbook de contrôle

L'un des documents d'automatisation d'AWS Systems Manager (SSM) que l'orchestrateur utilise pour acheminer une correction initiée pour un contrôle spécifique vers le manuel de correction approprié. Par exemple, les correctifs pour SC Lambda.1 et AWS Foundational Security Best Practices (FSBP) Lambda.1 sont mis en œuvre avec le même manuel de correction. L'orchestrateur appelle le runbook de contrôle pour chaque contrôle, nommés respectivement ASR-AFSBP_Lambda.1 et ASR-SC_2.0.0_Lambda.1. Chaque runbook de contrôle invoque le même runbook de correction, qui dans ce cas serait ASR-. RemoveLambdaPublicAccess

orchestrateur

Les Step Functions déployées par la solution qui prend en entrée un objet de recherche provenant d'AWS Security Hub et invoque le manuel de contrôle approprié dans le compte et la région cibles. L'orchestrateur informe également la rubrique SNS de la solution lorsque la correction est lancée et lorsque la correction réussit ou échoue.

norme

Groupe de contrôles défini par une organisation dans le cadre d'un cadre de conformité. Par exemple, l'une des normes prises en charge par AWS Security Hub et cette solution est AWS FSBP.

contrôle

Description des propriétés qu'une ressource doit ou ne doit pas posséder pour être conforme. Par exemple, le contrôle AWS FSBP Lambda.1 indique qu'AWS Lambda Functions doit interdire l'accès public. Une fonction autorisant l'accès public échouerait à ce contrôle.

résultats de contrôle consolidés, contrôle de sécurité, vue des contrôles de sécurité

Fonctionnalité d'AWS Security Hub qui, lorsqu'elle est activée, affiche les résultats avec leur contrôle consolidé IDs plutôt IDs que ceux correspondant à une norme particulière. Par exemple, les contrôles AWS FSBP S3.2, CIS v1.2.0 2.3, CIS v1.4.0 2.1.5.2 et PCI-DSS v3.2.1 S3.1 correspondent tous au contrôle consolidé (SC) S3.2 « Les compartiments S3 devraient interdire l'accès public en lecture ». Lorsque cette fonctionnalité est activée, les runbooks SC sont utilisés.

[Solution Web UI] administrateur délégué

Dans le contexte de l'interface utilisateur Web de la solution, un administrateur délégué est un utilisateur qui a été invité par l'administrateur et qui dispose d'un accès complet pour exécuter les corrections et consulter l'historique des corrections. Cet utilisateur peut également consulter et gérer les autres utilisateurs de l'opérateur de compte.

Opérateur de compte [Solution Web UI]

Dans le contexte de l'interface utilisateur Web de la solution, un opérateur de compte est un utilisateur invité par un administrateur ou un administrateur délégué à accéder à l'interface utilisateur Web de la solution. Cet utilisateur est associé à une liste d'identifiants de compte AWS fournis dans son invitation ; il peut uniquement exécuter des corrections et consulter l'historique des corrections en ce qui concerne les ressources de ces comptes.

Pour une référence générale des termes AWS, reportez-vous au glossaire AWS.

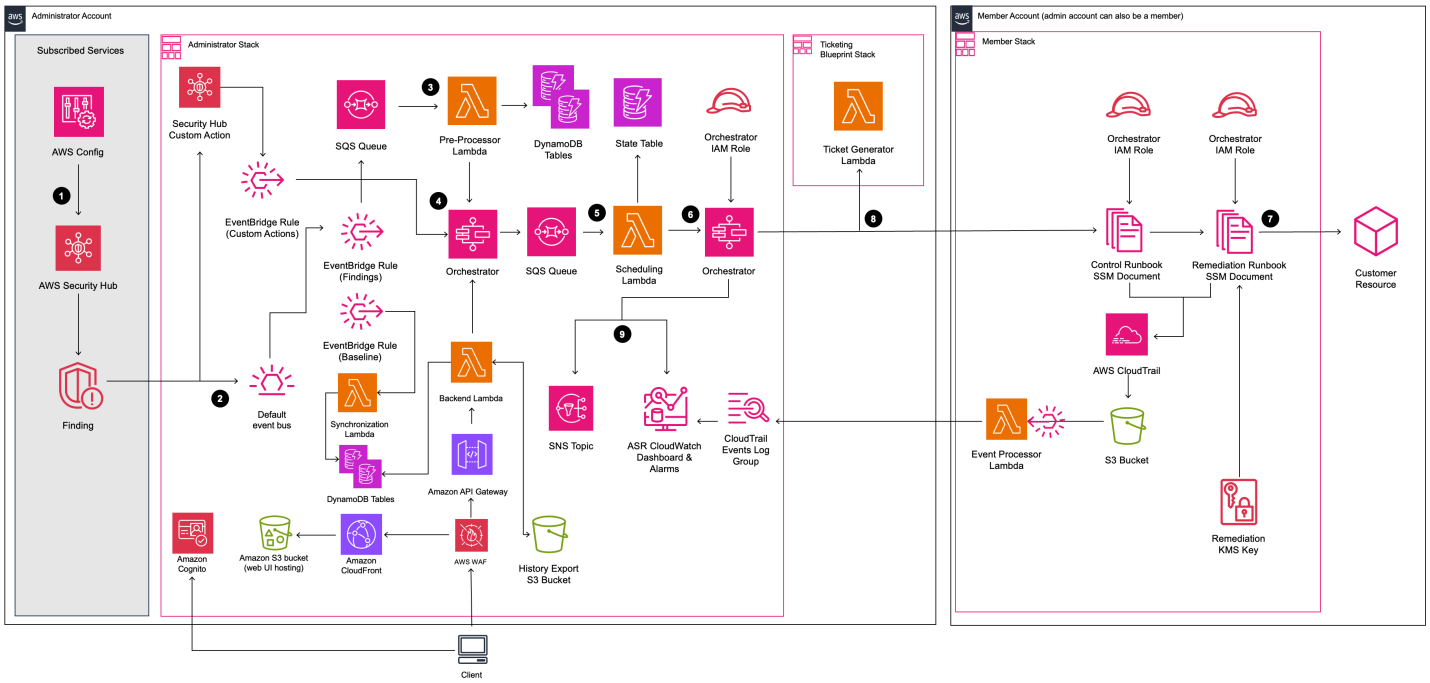
Présentation de l’architecture

Cette section fournit un schéma d'architecture d'implémentation de référence pour les composants déployés avec cette solution.

Diagramme d’architecture

Le déploiement de cette solution avec les paramètres par défaut crée l'environnement suivant dans le cloud AWS.

Réponse de sécurité automatisée sur l'architecture AWS



> **Note**
>
> Les CloudFormation ressources AWS sont créées à partir des constructions du kit AWS Cloud Development Kit (AWS CDK).

Le flux de haut niveau pour les composants de solution déployés avec le CloudFormation modèle AWS est le suivant :

1. Détecter : AWS Security Hub fournit aux clients une vue complète de leur état de sécurité AWS. Cela les aide à mesurer leur environnement par rapport aux normes et aux meilleures pratiques du secteur de la sécurité. Il fonctionne en collectant des événements et des données provenant d'autres services AWS, tels qu'AWS Config, Amazon Guard Duty et AWS Firewall Manager. Ces événements et données sont analysés par rapport aux normes de sécurité, telles que le CIS AWS Foundations Benchmark. Les exceptions sont invoquées sous forme de conclusions dans la console AWS Security Hub. Les nouvelles découvertes sont envoyées sous forme d' EventBridgeévénements Amazon.
2. Écoutez : EventBridge des événements sont émis par AWS Security Hub pour chaque découverte créée ou modifiée par le service. Automated Security Response on AWS (ASR) déploie deux EventBridge règles qui écoutent les événements générés par AWS Security Hub :
   - EventBridge Règle d'action personnalisée : écoute les événements d'actions personnalisées émis par AWS Security Hub CSPM lorsque l'action personnalisée « Corriger avec ASR » est déclenchée par un utilisateur. L'événement est transmis à l'orchestrateur pour y remédier.
   - EventBridge Règle des résultats : écoute tous les événements de création ou de mise à jour de recherche émis par AWS Security Hub et AWS Security Hub CSPM. Ces événements sont transmis à la file d'attente SQS du préprocesseur pour un traitement ultérieur.
3. Lancer : vous pouvez lancer les corrections manuellement ou les configurer pour qu'elles s'exécutent automatiquement. Pour exécuter une correction manuellement, vous pouvez utiliser l'interface utilisateur Web déployée par la solution ou la fonctionnalité d'actions personnalisées d'AWS Security Hub CSPM. Après des tests approfondis dans un environnement hors production, vous pouvez également activer les corrections automatisées. Vous pouvez activer les automatisations pour des corrections individuelles. Il n'est pas nécessaire d'activer les initiations automatiques pour toutes les corrections. Pour configurer les corrections afin qu'elles s'exécutent automatiquement, consultez la page Activer les corrections entièrement automatisées.
4. Pré-correction : dans le compte administrateur, AWS Step Functions traite l'événement de correction et le prépare à être planifié.
5. Planification : la solution invoque la fonction de planification AWS Lambda pour placer l'événement de correction dans la table d'état d'Amazon DynamoDB.
6. Orchestrate : dans le compte administrateur, Step Functions utilise des rôles AWS Identity and Access Management (IAM) multicomptes. Step Functions invoque la correction dans le compte membre contenant la ressource à l'origine de la constatation de sécurité.
7. Corriger : un document AWS Systems Manager Automation contenu dans le compte membre exécute l'action requise pour corriger le résultat sur la ressource cible, par exemple en désactivant l'accès public à Lambda.

Vous pouvez éventuellement activer la fonctionnalité Action Log dans les piles de membres à l'aide du paramètre EnableCloudTrailForASRActionLog. Cette fonctionnalité capture les actions entreprises par la solution dans vos comptes de membres et les affiche dans le tableau de CloudWatch bord Amazon de la solution.

8. (Facultatif) Créez un ticket : si vous utilisez le TicketGenFunctionNameparamètre pour activer la billetterie dans la pile d'administration, la solution invoque la fonction Lambda du générateur de tickets fournie. Cette fonction Lambda crée un ticket dans votre service de billetterie une fois que la correction a été exécutée avec succès dans le compte du membre. Nous fournissons des piles pour l'intégration avec Jira et. ServiceNow
9. Notifier et consigner : le playbook enregistre les résultats dans un CloudWatch groupe de journaux, envoie une notification à une rubrique Amazon Simple Notification Service (Amazon SNS) et met à jour les résultats du Security Hub. La solution conserve une piste d'audit des actions figurant dans les notes de constatation.

Considérations relatives à la conception d'AWS Well-Architected

Cette solution a été conçue selon les meilleures pratiques de l'AWS Well-Architected Framework, qui aide les clients à concevoir et à exploiter des charges de travail fiables, sécurisées, efficaces et rentables dans le cloud. Cette section décrit comment les principes de conception et les meilleures pratiques du Well-Architected Framework ont été appliqués lors de la création de cette solution.

Excellence opérationnelle

Cette section décrit comment nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du pilier de l'excellence opérationnelle.

- Ressources définies comme utilisant IaC CloudFormation.
- Mesures correctives mises en œuvre avec les caractéristiques suivantes, dans la mesure du possible :
  - Idempotence
  - Gestion des erreurs et signalement
  - Logging
  - Restaurer les ressources à un état connu en cas de défaillance

Sécurité

Cette section décrit comment nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du pilier de sécurité.

- IAM utilisé pour l'authentification et l'autorisation.
- Les autorisations de rôle ont été définies de manière à être aussi limitées que possible, bien que dans de nombreux cas, cette solution nécessite des autorisations génériques pour pouvoir agir sur toutes les ressources.
- Pour des raisons de sécurité,

Fiabilité

Cette section décrit comment nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du pilier de fiabilité.

- Security Hub continue de créer des résultats si la cause sous-jacente du résultat n'est pas résolue par la correction.
- Les services sans serveur permettent à la solution d'évoluer selon les besoins.

Efficacité des performances

Cette section décrit comment nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du pilier de l'efficacité des performances.

- Cette solution a été conçue pour être une plate-forme que vous pouvez étendre sans avoir à implémenter vous-même l'orchestration et les autorisations.

Optimisation des coûts

Cette section décrit comment nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du pilier d'optimisation des coûts.

- Les services sans serveur vous permettent de payer uniquement pour ce que vous utilisez.
- Utilisez le niveau gratuit pour l'automatisation du SSM dans chaque compte

Durabilité

Cette section décrit comment nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du pilier du développement durable.

- Les services sans serveur vous permettent d'augmenter ou de diminuer selon vos besoins.

Détails de l'architecture

Cette section décrit les composants et les services AWS qui constituent cette solution ainsi que les détails de l'architecture sur la manière dont ces composants fonctionnent ensemble.

Intégration à AWS Security Hub

Le déploiement de la `automated-security-response-admin` pile crée une intégration avec la fonctionnalité d'action personnalisée d'AWS Security Hub CSPM. Lorsque les utilisateurs de la console AWS Security Hub CSPM cliquent sur Actions > Corriger avec ASR, les résultats sélectionnés sont envoyés au flux de travail de correction EventBridge et déclenchent celui-ci.

Les autorisations entre comptes et les runbooks AWS Systems Manager doivent être déployés sur tous les comptes AWS Security Hub (administrateur et membre) à l'aide des modèles `automated-security-response-member.template` et `automated-security-response-member-roles.template` CloudFormation . Pour plus d'informations, reportez-vous à Playbooks. Ce modèle permet une correction automatique dans le compte cible.

Les utilisateurs peuvent configurer des corrections entièrement automatisées pour chaque contrôle à l'aide d'Amazon DynamoDB. Cette option active la correction entièrement automatique des résultats dès qu'ils sont signalés à AWS Security Hub. Par défaut, les initiations automatiques sont désactivées. Cette option peut être modifiée à tout moment après l'installation en modifiant la table DynamoDB de configuration de correction.

Assainissement entre comptes

La réponse de sécurité automatisée sur AWS utilise des rôles entre comptes pour fonctionner entre les comptes principaux et secondaires à l'aide de rôles entre comptes. Ces rôles sont déployés sur les comptes des membres lors de l'installation de la solution. Un rôle individuel est attribué à chaque correction. Le processus de correction dans le compte principal est autorisé à assumer le rôle de correction dans le compte qui nécessite une correction. La correction est effectuée par les runbooks AWS Systems Manager exécutés dans le compte qui nécessite une correction.

Playbooks

Un ensemble de mesures correctives est regroupé dans un package appelé playbook. Les playbooks sont installés, mis à jour et supprimés à l'aide des modèles de cette solution. Pour plus d'informations

sur les corrections prises en charge dans chaque playbook, reportez-vous au Guide du développeur → Playbooks. Cette solution prend actuellement en charge les playbooks suivants :

- Security Control, un manuel aligné sur la fonctionnalité Consolidated Control findings d'AWS Security Hub, publié le 23 février 2023.

> **Important**
>
> Lorsque les résultats de contrôle consolidés sont activés dans Security Hub, il s'agit du seul playbook qui doit être activé dans la solution.

- Benchmarks du Center for Internet Security (CIS) Amazon Web Services Foundations, version 1.2.0, publiés le 18 mai 2018.
- Benchmarks Amazon Web Services Foundations du Center for Internet Security (CIS), version 1.4.0, publiés le 9 novembre 2022.
- Benchmarks du Center for Internet Security (CIS) Amazon Web Services Foundations, version 3.0.0, publiés le 13 mai 2024.
- Meilleures pratiques de sécurité fondamentales (FSBP) d'AWS, version 1.0.0, publiée en mars 2021.
- Normes de sécurité des données de l'industrie des cartes de paiement (PCI-DSS) version 3.2.1, publiées en mai 2018.
- Version 5.0.0 du National Institute of Standards and Technology (NIST), publiée en novembre 2023.

Une fois les CloudFormation piles de la solution déployées, les playbooks sont immédiatement prêts à être utilisés. Aucune configuration supplémentaire n'est requise pour permettre de corriger les problèmes liés aux normes de sécurité répertoriées ci-dessus.

Journalisation centralisée

La réponse de sécurité automatisée sur AWS se connecte à un seul groupe de CloudWatch journaux, SO0111-ASR. Ces journaux contiennent une journalisation détaillée de la solution pour le dépannage et la gestion de la solution.

Notifications

Cette solution utilise une rubrique Amazon Simple Notification Service (Amazon SNS) pour publier les résultats des mesures correctives. Vous pouvez utiliser les abonnements à cette rubrique pour étendre les fonctionnalités de la solution. Par exemple, vous pouvez envoyer des notifications par e-mail et mettre à jour les tickets d'incident.

- SO0111-ASR_Topic — Utilisé pour envoyer des informations générales et des messages d'erreur relatifs aux corrections exécutées.
- SO0111-ASR_Alarm_Topic — Utilisé pour avertir lorsque l'une des alarmes de la solution est déclenchée, indiquant que la solution ne fonctionne pas comme prévu.

Services AWS inclus dans cette solution

La solution utilise les services suivants. Les services de base sont nécessaires pour utiliser la solution, et les services de support connectent les services principaux.

Service AWS	Description
Amazon EventBridge	Noyau. EventBridge les règles sont utilisées pour écouter et déclencher les événements émis par AWS Security Hub et AWS Security Hub CSPM.
AWS IAM	Noyau. Déploie de nombreux rôles pour permettre des corrections sur différentes ressources.
AWS Lambda	Noyau. Déploie plusieurs fonctions lambda qui seront utilisées par l'orchestrateur de fonctions par étapes pour résoudre les problèmes. Sert de backend à l'interface utilisateur Web de la solution intégrée à API Gateway.
AWS Security Hub	Noyau. Fournit aux clients une vue complète de leur état de sécurité AWS.

Service AWS	Description
AWS Step Functions	Noyau. Déploie un orchestrateur qui invoquera les documents de correction à l'aide des appels d'API AWS Systems Manager.
AWS Systems Manager	Noyau. Déploie les documents d'automatisation de System Manager qui contiennent la logique de correction à exécuter par la solution. Utilise le magasin de paramètres pour gérer les métadonnées et les paramètres de configura tion de la solution.
AWS DynamoDB	Noyau. Stocke la dernière correction exécutée dans chaque compte et région afin d'optimiser la planification des corrections. Stocke les résultats générés par AWS Security Hub et AWS Security Hub CSPM. Stocke les métadonnées de correction et de configuration de la solution. Stocke les données destinées aux utilisate urs accédant à l'interface utilisateur Web de la solution.
AWS CloudTrail	Soutenir. Enregistre les modifications apportées par la solution à vos ressources AWS et les affiche sur un CloudWatch tableau de bord.
Amazon CloudWatch	Soutenir. Déploie des groupes de journaux que les différents playbooks utiliseront pour enregistrer les résultats. Collecte des métriques à afficher sur un tableau de bord personnalisé avec des alarmes.

Service AWS	Description
Amazon Simple Notification Service	Soutenir. Déploie les rubriques SNS qui reçoivent une notification une fois la correction terminée.
AWS SQS	Soutenir. Aide à planifier les mesures correctives afin que la solution puisse les exécuter en parallèle. Met en mémoire tampon les exécutions Lambda à l'aide de mappages EventSource Lambda.
AWS Key Management Service	Soutenir. Utilisé pour chiffrer les données à des fins de correction.
AWS Config	Soutenir. Enregistre toutes les ressources destinées à être utilisées avec AWS Security Hub.
Amazon S3	Soutenir. Stocke l'historique des mesures correctives exportés et les données du journal. Héberge l'interface utilisateur Web de la solution sous la forme d'une application monopage (SPA).
Amazon CloudFront	Soutenir. Fournit l'interface utilisateur Web de la solution
Amazon API Gateway	Soutenir. Crée l'API REST de la solution pour prendre en charge l'interface utilisateur.
AWS WAF	Soutenir. Protège l'interface utilisateur Web de la solution.

Service AWS	Description
Amazon Cognito	Soutenir. Utilisé pour authentifier et autoriser l'accès à l'interface utilisateur Web de la solution.

Planifiez votre déploiement

Cette section décrit le coût, la sécurité du réseau, les régions AWS prises en charge, les quotas et d'autres considérations avant le déploiement de la solution.

Cost

Vous êtes responsable du coût des services AWS utilisés pour exécuter cette solution.

À compter de cette révision, les coûts mensuels estimés sont les suivants :

- Petit déploiement (10 comptes, 1 région) - États-Unis East/N. Virginia): Approximately $14.70 for 300 remediations/month
- Déploiement moyen (100 comptes, 1 région - États-Unis) East/N. Virginia): Approximately $106.40 for 3,000 remediations/month
- Déploiement à grande échelle (1 000 comptes, 10 régions) : environ 7 360$ pour 30 000 remédiations/mois

> **Important**
>
> Les prix sont susceptibles d’être modifiés. Pour plus de détails, consultez la page de tarification de chaque service AWS utilisé dans cette solution.

> **Note**
>
> De nombreux services AWS incluent un niveau gratuit, c'est-à-dire une quantité de base du service que les clients peuvent utiliser gratuitement. Les coûts réels peuvent être supérieurs ou inférieurs aux exemples de prix fournis.

Nous vous recommandons de créer un budget via AWS Cost Explorer pour vous aider à gérer les coûts. Les prix sont susceptibles d’être modifiés. Pour plus de détails, consultez la page Web de tarification de chaque service AWS utilisé dans cette solution.

Exemple de tableau des coûts

Le coût total d'exécution de cette solution dépend des facteurs suivants :

- Le nombre de comptes membres d'AWS Security Hub
- Le nombre de mesures correctives actives invoquées automatiquement
- La fréquence des mesures correctives

Cette solution utilise les composants AWS suivants, dont le coût dépend de votre configuration. Des exemples de tarification sont fournis pour les petites, moyennes et grandes entreprises.

Service	Offre gratuite	Tarification [USD]
AWS Systems Manager Automation : nombre d'étapes	Pas de niveau gratuit	Chaque étape de base est facturée à 0,002$ par étape. Pour les automatisations multi-comptes, toutes les étapes, y compris celles exécutées sur les comptes enfants, sont comptabilisées uniquement dans le compte d'origine.
AWS Systems Manager Automation : durée de l'étape	Pas de niveau gratuit	Chaque étape `aws:executeScript` d'action est facturée à 0,00003$ pour chaque seconde.
AWS Systems Manager Automation - Stockage	Pas de niveau gratuit	0,046$ par Go par mois
AWS Systems Manager Automation - Transfert de données	Pas de niveau gratuit	0,900$ par Go transféré (pour plusieurs comptes ou) out-of-Region
AWS Security Hub CSPM - Contrôles de sécurité	Pas de niveau gratuit	checks/account/Region/month Les 100 000 premiers coûtent 0,0010$ par chèque

Service	Offre gratuite	Tarification [USD]
		Les 400 000 dollars suivants checks/account/Region/month coûtent 0,0008$ par chèque Plus de 500 000 dollars checks/account/Region/month coûtent 0,0005$ par chèque
AWS Security Hub CSPM - Recherche d'événements d'ingestion	Les 10 000 premiers events/account/Region/month sont gratuits. Recherche d'événements d'ingestion associés aux contrôles de sécurité de Security Hub.	Plus de 10 000 dollars events/account/Region/month coûtent 0,00003$ par événement
Amazon CloudWatch - Métriques	Mesures de surveillance de base (à une fréquence de 5 minutes) 10 Mesures de surveillance détaillées (à une fréquence d'une minute) 1 1 million de demandes d'API (non applicable à GetMetric Data, GetInsightRuleReport et GetMetricWidgetImage)	Les 10 000 premiers indicateurs coûtent 0,30$ par mois Les 240 000 mesures suivantes coûtent 0,10$ par mois Les 750 000 métriques suivantes coûtent 0,05$ par mois Plus de 1 000 000 métriques coûtent 0,02$ par mois Les appels d'API coûtent 0,01$ pour 1 000 demandes
Amazon CloudWatch - Tableau de bord	3 tableaux de bord pour un maximum de 50 indicateurs par mois	3,00$ par tableau de bord par mois

Service	Offre gratuite	Tarification [USD]
Amazon CloudWatch - Alarmes	10 mesures d'alarme (ne s'applique pas aux alarmes haute résolution)	La résolution standard (60 secondes) coûte 0,10$ par alarme-métrique La haute résolution (10 secondes) coûte 0,30$ par métrique d'alarme La détection des anomalies à résolution standard coûte 0,30$ par alarme La détection des anomalies à haute résolution coûte 0,90$ par alarme Le composite coûte 0,50$ par alarme
Amazon CloudWatch - Collecte de journaux	5 Go de données (ingestion, stockage d'archives et données numérisées par les requêtes Logs Insights)	0,50$ par Go
Amazon CloudWatch - Stockage des journaux	5 Go de données (ingestion, stockage d'archives et données numérisées par les requêtes Logs Insights)	0,005$ par Go de données numérisées
AWS Lambda - Demandes	1 million de demandes gratuites par mois	0,20$ par million de demandes

Service	Offre gratuite	Tarification [USD]
AWS Lambda - Durée	400 000 Go de temps de calcul par mois	0,0000166667$ pour chaque Go par seconde. Le prix de Duration dépend de la quantité de mémoire que vous allouez à votre fonction. Vous pouvez allouer à votre fonction n'importe quelle quantité de mémoire comprise entre 128 Mo et 10 240 Mo, par incréments de 1 Mo.
AWS Step Functions - Transitions d'état	4 000 transitions d'État gratuites par mois	0,025$ par 1 000 transitions entre États par la suite
Amazon EventBridge	Tous les événements de changement d'état publiés par les services AWS sont gratuits	Les événements personnal isés coûtent 1,00 $/million d'événements personnalisés publiés Les événements tiers (SaaS) coûtent 1,00 $/million d'événements publiés Les événements multicomp tes coûtent 1,00 $/million de dollars. Les événements multicomptes envoyés
Amazon SNS	Les 1 premiers millions de demandes Amazon SNS par mois sont gratuites	0,50$ par million de demandes par la suite
Amazon SQS	Les 1 premiers millions de requêtes Amazon SQS par mois sont gratuites	0,40$ par tranche de 1 million à 100 milliards de demandes par la suite

Service	Offre gratuite	Tarification [USD]
Amazon DynamoDB	Les premiers 25 Go de stockage sont gratuits	2,00$ par million de lectures et d'écritures cohérentes par la suite
AWS Key Management Service	20 000 demandes/mois	1,00$ par clé KMS. 0,03$ par 10 000 demandes d'API. Pour les clés KMS que vous faites pivoter automatiquement ou à la demande, la première et la deuxième rotation de la clé ajoutent 1 dollar par mois (au prorata de l'heure) au coût. Remarque : Cette solution inclut des optimisations de la mise en cache KMS (clés de compartiment S3, réutilisation des clés de données SQS pendant 60 minutes, mise en cache de 5 minutes de Secrets Manager) qui réduisent les appels d'API KMS d'environ 70 %.
Amazon Cognito	Dans le niveau Essentials, les 10 000 premiers utilisateurs actifs par mois sont gratuits. Remarque : ce niveau gratuit est de 50 utilisateurs actifs par mois lorsque les utilisateurs s'authentifient via un IdP externe (SAML/OIDC).	0,015$ par utilisateur actif mensuel supérieur à 10 000 utilisateurs.

Service	Offre gratuite	Tarification [USD]
Amazon CloudFront	Le niveau gratuit inclut 1 To de transfert de données sortantes et 10 000 000 de requêtes HTTP ou HTTPS par mois.	(US/Canada/Mexico) Les 9 premiers To coûtent 0,085$ par mois. Les 40 To suivants coûtent 0,080$ par mois. 0,0075$ par requête HTTP. 0,0100$ par requête HTTPS.
Amazon S3	Pas de niveau gratuit	Les 50 premiers To coûtent 0,023$ par Go et par mois. 0,005$ par 1 000 requêtes PUT, COPY, POST, LIST. 0,0004$ par 1 000 requêtes GET, SELECT et toutes les autres requêtes.
Amazon API Gateway	1 million d'appels d'API REST au cours des 12 premiers mois d'utilisation.	3,50 dollars par million pour les 333 premiers millions d'appels d'API.

Optimisation des coûts KMS

Depuis la version 3.1.0, cette solution inclut des optimisations de mise en cache KMS qui réduisent les coûts des opérations cryptographiques d'environ 70 %

- Clés de compartiment S3 : réduit les GenerateDataKey appels KMS pour les opérations de chiffrement S3
- Réutilisation des clés de données SQS : période de cache de 60 minutes pour le chiffrement des messages
- Mise en cache de Secrets Manager : durée TTL de 5 minutes dans les fonctions Lambda

Impact sur les performances : ces optimisations améliorent la latence de 10 à 15 ms pour les opérations S3 et les flux de travail complets, tout en réduisant les coûts, sans dégradation du débit.

Exemples de prix (mensuels)

Exemple 1 : 300 mesures correctives par mois

- 10 comptes, 1 région
- 30 mesures correctives par account/Region/month
- 500 conclusions du Security Hub traitées par account/Region/month
- Interface utilisateur Web désactivée
- Journal des actions désactivé
- Coût total 14,70$ par mois

Service	Hypothèses	Charges mensuelles [USD]
AWS Systems Manager Automation	Étapes : ~4 étapes* 300 remédiations* 0,002$ = 2,40$ Durée : 10 s * 300 mesures correctives * 0,00003$ = 0,09$	2,49$
AWS Security Hub	Aucun service facturable utilisé	$0
Amazon CloudWatch Logs	0,50$ par Go	< 0,01$
AWS Lambda - Demandes	300 remédiations* 7 demandes = 2 100 demandes 5 000 trouvailles * 1 demande = 5 000 demandes 0,20 $/1 000 000 demandes = 0,0000002$ par demande	0,00142$
AWS Lambda - Durée	(512 Mo de mémoire) 4 000 ms * 300 mesures correctives * 0,0000000083$ = 0,00996$	0,029$

Service	Hypothèses	Charges mensuelles [USD]
	49 ms * 5 000 résultats * 0,0000000083$ = 0,0186$	
AWS Step Functions	19 transitions d'état* 300 mesures correctives = 5 700 0,025 $* (5 700/1 000) transitions d'état = 0,14$	0,14$
EventBridge Règles d'Amazon	Aucun frais pour les règles	$0
AWS Key Management Service	1 clé * 10 comptes * 1 région * 1$ = 10$ (Chiffrer/déchiffrer les demandes d'API) (300 remédiations* 2 demandes) + (5 000 constatations* 4 demandes) = 20 600 demandes Avec mise en cache KMS : 20 600 x 0,30 = 6 180 requêtes 0,03$ par 10 000 demandes ⇒ 0,03$ * (6 180/ 10 000) = 0,02$	10,02$

Service	Hypothèses	Charges mensuelles [USD]
Amazon DynamoDB	2,00 $* 1 000 000 livres lus et écrits = 2,00$ (Tableau des résultats) 15 Mo * 10 comptes * 1 région = 150 Mo (Tableau historique) 10 Mo * 10 comptes * 1 région = 100 Mo 0,25$ par Go par mois * 0,25 Go = 0,0625$	2,0625$
Amazon SQS	0,40$ * 1 000 000 demandes = 0,40$	0,40$
Amazon SNS	0,50 $* (600/1 000 000 notifications) = 0,0003$	0,0003$
Amazon CloudWatch - Métriques	(Métriques améliorées désactivées) 0,30$ * 7 mesures personnalisées = 2,10$ 0,01 $* (300 appels d'API de métriques de vente pour 1 000) = 0,003$	2,10$
Amazon CloudWatch - Tableaux de bord	3,00 $* 1 tableau de bord = 3,00$	3,00$
Amazon CloudWatch - Alarmes	(Métriques améliorées désactivées) 0,10$ * 4 alarmes = 0,40$	0,40$

Service	Hypothèses	Charges mensuelles [USD]
Amazon CloudWatch - X-Ray Traces	300 corrections * 7 requêtes = 2 100 appels Lambda 5 000 trouvailles * 1 demande = 5 000 appels Lambda 0,000005$ par trace * 7 100 traces = 0,0355$	0,0355$
Total		14,70$

Exemple 2 : 300 corrections par mois (interface utilisateur Web activée)

- 10 comptes, 1 région
- 30 mesures correctives par account/Region/month
- 5 000 conclusions du Security Hub traitées par account/Region/month
- Interface utilisateur Web activée
- Journal des actions désactivé
- Coût total 36,35$ par mois

Service	Hypothèses	Charges mensuelles [USD]
AWS Systems Manager Automation	Étapes : ~4 étapes* 300 remédiations* 0,002$ = 2,40$ Durée : 10 s * 300 mesures correctives * 0,00003$ = 0,09$	2,49$
AWS Security Hub	Aucun service facturable utilisé	$0
Amazon CloudWatch Logs	0,50$ par Go	< 0,01$

Service	Hypothèses	Charges mensuelles [USD]
AWS Lambda - Demandes	300 remédiations* 7 demandes = 2 100 demandes 5 000 trouvailles * 1 demande = 5 000 demandes 0,20 $/1 000 000 demandes = 0,0000002$ par demande	0,00142$
AWS Lambda - Durée	(512 Mo de mémoire) 4 000 ms * 300 mesures correctives * 0,0000000083$ = 0,00996$ 49 ms * 5 000 résultats * 0,0000000083$ = 0,0186$	0,029$
AWS Step Functions	19 transitions d'état* 300 mesures correctives = 5 700 0,025 $* (5 700/1 000) transitions d'état = 0,14$	0,14$
EventBridge Règles d'Amazon	Aucun frais pour les règles	$0

Service	Hypothèses	Charges mensuelles [USD]
AWS Key Management Service	1 clé * 10 comptes * 1 région * 1$ = 10$ (Chiffrer/déchiffrer les demandes d'API) (300 remédiations* 2 demandes) + (5 000 constatations* 4 demandes) = 20 600 demandes 0,03$ par 10 000 demandes ⇒ 0,03$ * (20 600/10 000) = 0,06$	10,06$
Amazon DynamoDB	2,00 $* 1 000 000 livres lus et écrits = 2,00$ (Tableau des résultats) 15 Mo * 10 comptes * 1 région = 150 Mo (Tableau historique) 10 Mo * 10 comptes * 1 région = 100 Mo 0,25$ par Go par mois * 0,25 Go = 0,0625$	2,0625$
Amazon SQS	0,40$ * 1 000 000 demandes = 0,40$	0,40$
Amazon SNS	0,50 $* (600/1 000 000 notifications) = 0,0003$	0,0003$

Service	Hypothèses	Charges mensuelles [USD]
Amazon CloudWatch - Métriques	(Métriques améliorées désactivées) 0,30$ * 7 mesures personnalisées = 2,10$ 0,01 $* (300 appels d'API de métriques de vente pour 1 000) = 0,003$	2,10$
Amazon CloudWatch - Tableaux de bord	3,00 $* 1 tableau de bord = 3,00$	3,00$
Amazon CloudWatch - Alarmes	(Métriques améliorées désactivées) 0,10$ * 4 alarmes = 0,40$	0,40$
Amazon CloudWatch - X-Ray Traces	300 corrections * 7 requêtes = 2 100 appels Lambda 5 000 trouvailles * 1 demande = 5 000 appels Lambda 0,000005$ par trace * 7 100 traces = 0,0355$	0,0355$
Amazon Cognito	(niveau Essentials) 500 utilisateurs actifs par mois	$0

Service	Hypothèses	Charges mensuelles [USD]
Amazon CloudFront	Transfert de données régional vers l'origine (par Go) = 0,020$ Transfert régional de données sortantes vers Internet (par Go) = 0,085$ Prix des demandes pour toutes les méthodes HTTP (par 10 000) = 0,0075$	0,1125$
Amazon S3	(Hébergement d'interface utilisateur) 0,023$ par Go * 0,002 Go = 0,000046$ (Exportation de l'historique) 0,023$ par Go * 0,50 Go = 0,0125$ 0,0004$ pour 1 000 requêtes GET	0,0125 USD
AWS WAF	1 ACL Web = 5,00$ par mois 7 règles * 1,00$ par règle = 7,00$	12$
Amazon API Gateway	3,50 dollars par million d'appels d'API REST	3,50$
Total		36,35$

Exemple 3 : 3 000 mesures correctives par mois

- 100 comptes, 1 région
- 30 mesures correctives par account/Region/month
- 500 conclusions du Security Hub traitées par account/Region/month
- Interface utilisateur Web désactivée
- Journal des actions désactivé
- Coût total 106,40$ par mois

Service	Hypothèses	Charges mensuelles [USD]
AWS Systems Manager Automation	Étapes : ~4 étapes* 3 000 assainissements* 0,002$ = 24,00$ Durée : 10 s * 3 000 mesures correctives * 0,00003$ = 0,90$	24,90$
AWS Security Hub	Aucun service facturable utilisé	$0
Amazon CloudWatch Logs	0,50$ par Go	< 0,01$
AWS Lambda - Demandes	3 000 mesures correctrices* 7 demandes = 2 100 demandes 50 000 trouvailles * 1 demande = 50 000 demandes 0,20 $/1 000 000 demandes = 0,0000002$ par demande	0,01$
AWS Lambda - Durée	(512 Mo de mémoire) 4 000 ms * 3 000 mesures correctives * 0,0000000083$ = 0,0996$	0,29$

Service	Hypothèses	Charges mensuelles [USD]
	449 ms * 50 000 résultats * 0,0000000083$ = 0,186$	
AWS Step Functions	19 transitions d'état* 3 000 mesures correctives = 57 000 0,025 $* (57 000/1 000) transitions d'état = 1,425$	1,425$
EventBridge Règles d'Amazon	Aucun frais pour les règles	$0
AWS Key Management Service	1 clé * 100 comptes * 1 région * 1$ = 100$ (Chiffrer/déchiffrer les demandes d'API) (3 000 mesures correctrices* 2 demandes) + (50 000 résultats * 4 demandes) = 206 000 demandes Avec mise en cache KMS : 206 000* 0,30 = 61 800 demandes 0,03$ par 10 000 demandes ⇒ 0,03$ * (61 800/10 000) = 0,185$	100,185$

Service	Hypothèses	Charges mensuelles [USD]
Amazon DynamoDB	2,00 $* 1 000 000 livres lus et écrits = 2,00$ (Tableau des résultats) 15 Mo * 100 comptes * 1 région = 1 500 Mo (Tableau historique) 10 Mo * 100 comptes * 1 région = 1 000 Mo 0,25$ par Go par mois * 2,5 Go = 0,625$	2,625$
Amazon SQS	0,40$ * 1 000 000 demandes = 0,40$	0,40$
Amazon SNS	0,50$ * 1 000 000 de notifications = 0,50$	0,50$
Amazon CloudWatch - Métriques	(Métriques améliorées désactivées) 0,30$ * 7 mesures personnalisées = 2,10$ 0,01 $* (3 000/1 000) appels d'API de métriques de vente = 0,03$	2,13$
Amazon CloudWatch - Tableaux de bord	3,00 $* 1 tableau de bord = 3,00$	3,00$
Amazon CloudWatch - Alarmes	0,10$ * 4 alarmes = 0,40$	0,40$

Service	Hypothèses	Charges mensuelles [USD]
Amazon CloudWatch - X-Ray Traces	3 000 corrections * 7 demandes = 2 100 appels Lambda 50 000 trouvailles * 1 demande = 50 000 appels Lambda 0,000005$ par trace * 52 100 traces = 0,2605$	0,2605$
Total		106,40$

Exemple 4 : 30 000 mesures correctives par mois

- 1 000 comptes, 10 régions
- 30 mesures correctives par account/Region/month
- 500 conclusions du Security Hub traitées par account/Region/month
- Interface utilisateur Web désactivée
- Journal des actions désactivé
- Coût total 7 360,00$ par mois

Service	Hypothèses	Charges mensuelles [USD]
AWS Systems Manager Automation	Étapes : ~4 étapes* 30 000 assainissements* 0,002$ = 240,00$ Durée : 10 s * 30 000 assainissements* 0,00003$ = 9,00$	249,00$
AWS Security Hub	Aucun service facturable utilisé	$0

Service	Hypothèses	Charges mensuelles [USD]
Amazon CloudWatch Logs	0,50$ par Go	< 0,01$
AWS Lambda - Demandes	30 000 mesures correctri ces* 7 demandes = 210 000 demandes 5 000 000 de trouvailles * 1 demande = 5 000 000 de demandes 0,20 $/1 000 000 demandes = 0,0000002$ par demande	1,042$
AWS Lambda - Durée	(512 Mo de mémoire) 4 000 ms * 30 000 mesures correctives * 0,0000000083$ = 0,996$ 449 ms * 5 000 000 de résultats * 0,0000000083$ = 18,63$	19,63$
AWS Step Functions	19 transitions entre états * 30 000 mesures correctives = 570 000 0,025 $* (570 000/1 000) transitions d'état = 14,25$	14,25$
EventBridge Règles d'Amazon	Aucun frais pour les règles	$0

Service	Hypothèses	Charges mensuelles [USD]
AWS Key Management Service	(1 clé) 1$ * 1 000 comptes * 10 régions = 10 000$ (Chiffrer/déchiffrer les demandes d'API) (30 000 remédiations* 2 demandes) + (5 000 000 de trouvailles * 4 demandes) = 20 060 000 demandes Avec la mise en cache KMS : 20 060 000* 0,30 = 6 018 000 requêtes 0,03$ par 10 000 demandes ⇒ 0,03$ * (6 018 000/ 10 000) = 18,05$	10 018,05$
Amazon DynamoDB	2,00 $* (10 000 000 lectures et écritures/1 000 000) = 20,00$ (Tableau des résultats) 15 Mo* 1 000 comptes * 10 régions = 150 Go (Tableau d'historique) 10 Mo* 1000 comptes* 10 régions = 100 Go 0,25$ par Go par mois * 250 Go = 62,50$	82,50$
Amazon SQS	0,40 $* (5 060 000 demandes/ 1 000 000) = 2,024$	2,024$

Service	Hypothèses	Charges mensuelles [USD]
Amazon SNS	0,000005$ * 1 000 000 de notifications = 0,50$	0,50$
Amazon CloudWatch - Métriques	(Métriques améliorées désactivées) 0,30$ * 7 mesures personnal isées = 2,10$ 0,01 $* (30 000/1 000) appels d'API de métriques de vente = 0,30$	2,40$
Amazon CloudWatch - Tableaux de bord	3,00 $* 1 tableau de bord = 3,00$	3,00$
Amazon CloudWatch - Alarmes	(Métriques améliorées désactivées) 0,10$ * 4 alarmes = 0,40$	0,40$
Amazon CloudWatch - X-Ray Traces	30 000 corrections * 7 demandes = 210 000 appels Lambda 5 000 000 de trouvailles * 1 demande = 5 000 000 d'invocations Lambda 0,000005$ par trace * 5 210 000 traces = 26,05$	26,05$
Total		7 360,00$

Exemple 5 : 30 000 corrections par mois (interface utilisateur Web activée)

- 1 000 comptes, 10 régions

- 30 mesures correctives par account/Region/month
- 500 conclusions du Security Hub traitées par account/Region/month
- Interface utilisateur Web activée
- Journal des actions désactivé
- Coût total 7 380,10$ par mois

Service	Hypothèses	Charges mensuelles [USD]
AWS Systems Manager Automation	Étapes : ~4 étapes* 30 000 assainissements* 0,002$ = 240,00$ Durée : 10 s * 30 000 assainissements* 0,00003$ = 9,00$	249,00$
AWS Security Hub	Aucun service facturable utilisé	$0
Amazon CloudWatch Logs	0,50$ par Go	< 0,01$
AWS Lambda - Demandes	30 000 mesures correctri ces* 7 demandes = 210 000 demandes 5 000 000 de trouvailles * 1 demande = 5 000 000 de demandes 0,20 $/1 000 000 demandes = 0,0000002$ par demande	1,042$
AWS Lambda - Durée	(512 Mo de mémoire) 4 000 ms * 30 000 mesures correctives * 0,0000000083$ = 0,996$	19,63$

Service	Hypothèses	Charges mensuelles [USD]
	449 ms * 5 000 000 de résultats * 0,0000000083$ = 18,63$	
AWS Step Functions	19 transitions entre états * 30 000 mesures correctives = 570 000 0,025 $* (570 000/1 000) transitions d'état = 14,25$	14,25$
EventBridge Règles d'Amazon	Aucun frais pour les règles	$0
AWS Key Management Service	(1 clé) 1$ * 1 000 comptes * 10 régions = 10 000$ (Chiffrer/déchiffrer les demandes d'API) (30 000 remédiations* 2 demandes) + (5 000 000 de trouvailles * 4 demandes) = 20 060 000 demandes Avec la mise en cache KMS : 20 060 000* 0,30 = 6 018 000 requêtes 0,03$ par 10 000 demandes ⇒ 0,03$ * (6 018 000/ 10 000) = 18,05$	10 018,05$

Service	Hypothèses	Charges mensuelles [USD]
Amazon DynamoDB	2,00 $* (10 000 000 lectures et écritures/1 000 000) = 20,00$ (Tableau des résultats) 15 Mo* 1 000 comptes * 10 régions = 150 Go (Tableau d'historique) 10 Mo* 1000 comptes* 10 régions = 100 Go 0,25$ par Go par mois * 250 Go = 62,50$	82,50$
Amazon SQS	0,40 $* (5 060 000 demandes/ 1 000 000) = 2,024$	2,024$
Amazon SNS	0,000005$ * 1 000 000 de notifications = 0,50$	0,50$
Amazon CloudWatch - Métriques	(Métriques améliorées désactivées) 0,30$ * 7 mesures personnal isées = 2,10$ 0,01 $* (30 000/1 000) appels d'API de métriques de vente = 0,30$	2,40$
Amazon CloudWatch - Tableaux de bord	3,00 $* 1 tableau de bord = 3,00$	3,00$
Amazon CloudWatch - Alarmes	(Métriques améliorées désactivées) 0,10$ * 4 alarmes = 0,40$	0,40$

Service	Hypothèses	Charges mensuelles [USD]
Amazon CloudWatch - X-Ray Traces	30 000 corrections * 7 demandes = 210 000 appels Lambda 5 000 000 de trouvailles * 1 demande = 5 000 000 d'invocations Lambda 0,000005$ par trace * 5 210 000 traces = 26,05$	26,05$
Amazon Cognito	(niveau Essentials) 5 000 utilisateurs actifs par mois	$0
Amazon CloudFront	Transfert de données régional vers l'origine (par Go) = 0,020$ Transfert régional de données sortantes vers Internet (par Go) = 0,085$ Prix des demandes pour toutes les méthodes HTTP (par 10 000) = 0,0075$	0,1125$

Service	Hypothèses	Charges mensuelles [USD]
Amazon S3	(Hébergement d'interface utilisateur) 0,023$ par Go * 0,002 Go = 0,000046$ (Exportation de l'historique) 0,023$ par Go * 100 Go = 2,30$ 0,0004$ pour 1 000 requêtes GET * 5 000 demandes = 2,00$	4,30$
AWS WAF	1 ACL Web = 5,00$ par mois 7 règles * 1,00$ par règle = 7,00$	12$
Amazon API Gateway	3,50 dollars par million d'appels d'API REST	3,50$
Total		7 380,10$

Important

Coûts de rotation des clés KMS AWS Key Management Service (KMS) effectue automatiquement une rotation des clés gérées par le client une fois par an lorsque la rotation est activée. Chaque rotation entraîne un coût de 1,00$ par clé et par an. Par exemple, avec 1 000 comptes dans une seule région, cela se traduit par 1 000 dollars supplémentaires par an (1 rotation × 1 000 clés × 1,00 dollar).

Coût supplémentaire pour les fonctionnalités optionnelles

Cette section identifie les coûts supplémentaires associés aux fonctionnalités optionnelles de cette solution.

CloudWatch Métriques améliorées

Si vous sélectionnez `yes` le EnableEnhancedCloudWatchMetricsparamètre lors du déploiement de la pile d'administration, la solution crée deux métriques personnalisées et une alarme pour chaque ID de contrôle. Le coût dépend du nombre de contrôles IDs que vous corrigez. Dans le tableau suivant, nous supposons que vous corrigez les 96 contrôles différents IDs par mois, afin de déterminer la limite supérieure des coûts.

Service	Hypothèses 96 % de contrôle IDs * 2 = 192 mesures personnalisées	Charges mensuelles [USD]
Amazon CloudWatch - Métriques	0,30$ * 192 mesures personnalisées = 57,60$	57,60$
Amazon CloudWatch - Alarmes	0,10$ * 96 alarmes = 9,60$	9,60$
Total		67,20$

CloudTrail Journal des actions

Dans chaque compte membre pour lequel vous activez la fonctionnalité Action Log, les solutions créent une CloudTrail trace pour consigner tous les événements de gestion des écritures. Une fonction Lambda filtre les événements non liés à la solution. Cela signifie que le coût est lié au nombre total d'événements de gestion de votre compte, car les événements non liés à la solution sont toujours capturés par le journal et traités par la fonction Lambda.

Pour le tableau suivant, nous supposons 150 000 événements de gestion par mois sur le compte. Le coût réel dépend de l'activité réelle des événements de gestion sur votre compte.

Service	Hypothèses	Charges mensuelles [USD]
AWS CloudTrail	150 000 * 2,00 $/100 000$ = 3,00$	3,00$
Lambda	150 000* 0,2 * 0,125 = 3 750 Go de secondes 3 750$ * 0,0000166667$ = coût du temps de calcul de 0,0625$ 0,15* 0,20$ = 0,03$ de coût de demande 0,0625$ + 0,03$ = coût Lambda total de 0,0952$	0,0925$
Total		3,09$ par compte membre

Sécurité

Lorsque vous créez des systèmes sur l'infrastructure AWS, les responsabilités en matière de sécurité sont partagées entre vous et AWS. Ce modèle partagé réduit votre charge opérationnelle car AWS exploite, gère et contrôle les composants, notamment le système d'exploitation hôte, la couche de virtualisation et la sécurité physique des installations dans lesquelles les services fonctionnent. Pour plus d'informations sur la sécurité AWS, consultez le site AWS Cloud Security.

Politique de sécurité d'API Gateway

Si vous choisissez d'activer l'interface utilisateur Web de la solution, une API REST API Gateway est déployée à côté de la CloudFormation pile d'administration qui sert de backend pour toutes les opérations de l'interface utilisateur Web. L'API REST déployée par la solution utilise la politique de sécurité TLS par défaut pour API Gateway, qui est `TLS-1-0` destinée aux régions APIs.

Cependant, après avoir déployé la CloudFormation pile d'administrateurs, vous pouvez choisir de personnaliser l'API REST de la solution en ajoutant une politique de sécurité TLS plus restrictive. Par exemple, vous pouvez choisir de `TLS_1_2 security policy` restreindre le trafic en utilisant

TLSv1 .2 ou TLSv1 .3. Vous trouverez l'API REST de la solution dans la console API Gateway sous le nom AutomatedSecurityResponseApi.

Afin de choisir une politique de sécurité pour l'API REST de la solution, vous devez d'abord configurer un nom de domaine personnalisé. Pour plus d'informations, consultez la section Nom de domaine personnalisé pour le REST public APIs dans API Gateway.

Pour plus d'informations sur l'ajout d'une politique de sécurité à votre API REST, voir Choisir une politique de sécurité pour le domaine personnalisé de votre API REST dans API Gateway dans le guide API Gateway.

Rôles IAM

Les rôles AWS Identity and Access Management (IAM) permettent aux clients d'attribuer des politiques d'accès et des autorisations détaillées aux services et aux utilisateurs du cloud AWS. Cette solution crée des rôles IAM qui accordent aux fonctions automatisées de la solution l'accès pour effectuer des actions de correction dans le cadre d'un ensemble restreint d'autorisations spécifiques à chaque correction.

La fonction Step du compte administrateur est attribuée au rôle SO0111-ASR-Orchestrator-Admin . Seul ce rôle est autorisé à assumer le rôle de membre SO0111-Orchestrator-Member dans chaque compte membre. Le rôle de membre est autorisé par chaque rôle de correction à le transmettre au service AWS Systems Manager pour exécuter des runbooks de correction spécifiques. Les noms des rôles de correction commencent par SO0111, suivi d'une description correspondant au nom du runbook de correction. Par exemple, SO0111-Remove VPCDefault SecurityGroupRules est le rôle du runbook de correction ASR-Remove. VPCDefault SecurityGroupRules

Régions AWS prises en charge

Important

L'activation de fonctionnalités facultatives dans la solution peut réduire la liste des régions prises en charge pour le déploiement. En d'autres termes, la liste ci-dessous ne s'applique qu'aux principaux composants de la solution. Par exemple, si vous choisissez d'activer l'interface utilisateur Web, vous ne pourrez pas déployer la solution dans les GovCloud régions car elle n'CloudFront est pas prise en GovCloud charge aux États-Unis à partir de novembre 2025.

Nom de la région	Code région
USA Est (Ohio)	us-east-2
USA Est (Virginie du Nord)	us-east-1
USA Ouest (Californie du Nord)	us-west-1
US West (Oregon)	us-west-2
Afrique (Le Cap)	af-south-1
Asie-Pacifique (Hong Kong)	ap-east-1
Asie-Pacifique (Hyderabad)	ap-south-2
Asie-Pacifique (Jakarta)	ap-southeast-3
Asie-Pacifique (Melbourne)	ap-southeast-4
Asie-Pacifique (Mumbai)	ap-south-1
Asie-Pacifique (Osaka)	ap-northeast-3
Asie-Pacifique (Séoul)	ap-northeast-2
Asie-Pacifique (Singapour)	ap-southeast-1
Asie-Pacifique (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1
Canada (Central)	ca-central-1
Europe (Francfort)	eu-central-1
Europe (Irlande)	eu-west-1
Europe (Londres)	eu-west-2
Europe (Milan)	eu-south-1

Nom de la région	Code région
Europe (Paris)	eu-west-3
Europe (Espagne)	eu-south-2
Europe (Stockholm)	eu-north-1
Europe (Zurich)	eu-central-2
Moyen-Orient (Bahreïn)	me-south-1
Moyen-Orient (EAU)	me-central-1
Amérique du Sud (Sao Paulo)	sa-east-1
AWS GovCloud (USA Est)	us-gov-east-1
AWS GovCloud (ouest des États-Unis)	us-gov-west-1
Chine (Beijing)	cn-north-1
China (Ningxia)	cn-northwest-1
Israël (Tel Aviv)	il-central-1
Canada-Ouest (Calgary)	ca-west-1
Mexique (Mexico)	mx-central-1
Asie-Pacifique (Thaïlande)	ap-southeast-7
Asie-Pacifique (Malaisie)	ap-southeast-5

Note

Toute nouvelle région AWS non répertoriée peut être prise en charge par le biais d'un déploiement local, mais pas par un déploiement en un clic.

Quotas

Les quotas de service, également appelés limites, représentent le nombre maximal de ressources ou d'opérations de service pour votre compte AWS.

Quotas pour les services AWS dans cette solution

Assurez-vous de disposer d'un quota suffisant pour chacun des services mis en œuvre dans cette solution. Pour plus d'informations, consultez la section Quotas de service AWS.

Utilisez les liens suivants pour accéder à la page de ce service. Pour consulter les quotas de service pour tous les services AWS dans la documentation sans changer de page, consultez plutôt les informations figurant sur la page Points de terminaison et quotas du service dans le PDF.

CloudFormation Quotas AWS

Votre compte AWS comporte CloudFormation des quotas AWS dont vous devez tenir compte lorsque vous lancez la pile dans cette solution. En comprenant ces quotas, vous pouvez éviter les erreurs de limitation qui vous empêcheraient de déployer correctement cette solution. Pour plus d'informations, consultez les CloudFormation quotas AWS dans le guide de CloudFormation l'utilisateur AWS.

CloudWatch Quotas AWS

Les CloudWatch quotas AWS de votre compte AWS sont liés à CloudWatch des politiques de ressources, qui autorisent uniquement 10 politiques de ressources par région et par compte. Cela ne peut pas être demandé pour une augmentation de quota. Consultez les quotas AWS CloudWatch Logs dans le guide de CloudWatch l'utilisateur AWS. Avant votre déploiement, veuillez vérifier votre utilisation actuelle pour vous assurer de ne pas dépasser ce seuil lors du déploiement de la solution.

AWS Organizations

Les fonctions Lambda de la solution appellent l'API AWS Organizations afin de récupérer l'alias du compte courant à inclure dans les messages publiés sur la rubrique SNS de la solution. Cela permet aux noms de compte lisibles par l'homme d'être visibles dans les notifications de la solution à des fins de débogage et de suivi.

AWS Organizations impose des limites quant à la fréquence à laquelle les clients peuvent invoquer leurs points de terminaison d'API. Si vous constatez que la solution dépasse les limites définies pour votre compte, vous pouvez désactiver la fonctionnalité qui récupère et affiche l'alias du compte.

Pour ce faire, accédez à la fonction Lambda nommée `SO0111-ASR-sendNotifications` située dans la région et le compte où vous avez déployé la pile d'administrateurs. Recherchez ensuite la variable d'environnement nommée `DISABLE_ACCOUNT_ALIAS_LOOKUP` et remplacez la valeur de « False » par « True ». Le champ d'alias du compte dans les notifications de la solution sera désormais « Inconnu », mais cela n'aura aucun impact sur les fonctionnalités de la solution.

Déploiement d'AWS Security Hub

Le déploiement et la configuration d'AWS Security Hub sont une condition préalable à cette solution. Pour plus d'informations sur la configuration d'AWS Security Hub CSPM, consultez la section Configuration d'AWS Security Hub CSPM dans le guide de l'utilisateur d'AWS Security Hub. Cette solution prend également en charge AWS Security Hub (version non CSPM). Pour plus d'informations sur la configuration d'AWS Security Hub, consultez la section Enabling Security Hub.

Au minimum, un Security Hub fonctionnel doit être configuré sur votre compte principal. Vous pouvez déployer cette solution sur le même compte (et dans la même région AWS) que le compte principal du Security Hub. Dans chaque compte principal et secondaire Security Hub, vous devez également déployer le modèle de membre qui autorise les AssumeRole autorisations d'accès aux AWS Step Functions de la solution pour exécuter des runbooks de correction dans le compte.

Stack ou StackSets déploiement

Un ensemble de piles vous permet de créer des piles dans les comptes AWS des régions AWS à l'aide d'un seul CloudFormation modèle AWS. À partir de la version 1.4, cette solution prend en charge le déploiement d'ensembles de piles en répartissant les ressources en fonction de l'endroit et de la manière dont elles sont déployées. Les clients disposant de plusieurs comptes, en particulier ceux qui utilisent AWS Organizations, peuvent tirer parti de l'utilisation d'ensembles de piles pour le déploiement sur de nombreux comptes. Cela réduit les efforts nécessaires à l'installation et à la maintenance de la solution. Pour plus d'informations StackSets, reportez-vous à la section Utilisation d'AWS CloudFormation StackSets.

Déploiement de la solution

> **Important**
>
> Si la fonctionnalité de consolidation des résultats de contrôle est activée dans Security Hub, activez uniquement le playbook Security Control (SC) lors du déploiement de cette solution. Si la fonctionnalité n'est pas activée, activez uniquement les playbooks conformément aux normes de sécurité activées dans Security Hub. Les résultats de contrôle consolidés sont activés par défaut si vous activez Security Hub CSPM le 23 février 2023 ou après cette date.

Cette solution utilise des CloudFormation modèles et des piles AWS pour automatiser son déploiement. Les CloudFormation modèles spécifient les ressources AWS incluses dans cette solution et leurs propriétés. La CloudFormation pile fournit les ressources décrites dans les modèles.

Pour que la solution fonctionne, trois modèles doivent être déployés. Décidez d'abord où déployer les modèles, puis comment les déployer.

Cette présentation décrit les modèles et explique comment décider où et comment les déployer. Les sections suivantes contiendront des instructions plus détaillées pour déployer chaque pile en tant que Stack ou StackSet.

Décider où déployer chaque stack

Les trois modèles seront désignés par les noms suivants et contiendront les ressources suivantes :

- Stack d'administration : fonction d'étape de l'orchestrateur, règles relatives aux événements et action personnalisée du Security Hub.
- Pile de membres : documents de correction SSM Automation.
- Les rôles des membres se cumulent : rôles IAM pour les mesures correctives.

La pile d'administrateurs doit être déployée une seule fois, dans un seul compte et dans une seule région. Il doit être déployé dans le compte et dans la région que vous avez configurés comme destination d'agrégation pour les résultats du Security Hub relatifs à votre organisation. Si vous souhaitez utiliser la fonctionnalité Action Log pour surveiller les événements de gestion, vous devez déployer la pile Admin dans le compte de gestion de votre organisation ou dans un compte d'administrateur délégué.

La solution fonctionne sur la base des résultats du Security Hub. Elle ne sera donc pas en mesure de fonctionner sur les résultats d'un compte ou d'une région en particulier si ce compte ou cette région n'a pas été configuré pour agréger les résultats dans le compte administrateur du Security Hub et dans la région.

> **Important**
>
> Si vous utilisez AWS Security Hub (non-CSPM), il vous incombe de vous assurer que vos comptes membres intégrés avec AWS Security Hub CSPM sont également intégrés avec AWS Security Hub (non-CSPM). Les régions agrégées dans AWS Security Hub CSPM doivent également correspondre aux régions agrégées dans AWS Security Hub (non CSPM).

Par exemple, une organisation possède des comptes opérant dans des régions `us-east-1` et dont `us-west-2` le compte est `111111111111` celui d'administrateur délégué du Security Hub dans la région`us-east-1`. Les comptes `222222222222` et les comptes `333333333333` doivent être des comptes membres du Security Hub pour le compte d'administrateur délégué`111111111111`. Les trois comptes doivent être configurés pour agréger les résultats de `us-west-2` à`us-east-1`. La pile d'administrateurs doit être déployée pour être prise `111111111111` en compte`us-east-1`.

Pour plus de détails sur la recherche de l'agrégation, consultez la documentation relative aux comptes d'administrateur délégué de Security Hub et à l'agrégation entre régions.

La pile d'administrateurs doit d'abord terminer le déploiement avant de déployer les piles de membres afin qu'une relation de confiance puisse être créée entre les comptes des membres et le compte du hub.

La pile de membres doit être déployée dans chaque compte et région dans lesquels vous souhaitez corriger les résultats. Cela peut inclure le compte d'administrateur délégué Security Hub sur lequel vous avez précédemment déployé la pile d'administrateurs ASR. Les documents d'automatisation doivent être exécutés dans les comptes des membres afin d'utiliser le niveau gratuit de SSM Automation.

Dans l'exemple précédent, si vous souhaitez corriger les résultats de tous les comptes et régions, la pile de membres doit être déployée sur les trois comptes (`111111111111222222222222`, et`333333333333`) et sur les deux régions (`us-east-1`et`us-west-2`).

La pile de rôles des membres doit être déployée sur chaque compte, mais elle contient des ressources globales (rôles IAM) qui ne peuvent être déployées qu'une seule fois par compte. Peu

importe la région dans laquelle vous déployez la pile de rôles des membres, par souci de simplicité, nous vous suggérons de déployer le déploiement dans la même région que celle dans laquelle la pile d'administrateurs est déployée.

À l'aide de l'exemple précédent, nous vous suggérons de déployer la pile de rôles des membres sur les trois comptes (`111111111111222222222222`,, et`333333333333`) de`us-east-1`.

Décider de la manière de déployer chaque stack

Les options de déploiement d'une pile sont les suivantes :

- CloudFormation StackSet (autorisations autogérées)
- CloudFormation StackSet (autorisations gérées par le service)
- CloudFormation Empilez

StackSets avec des autorisations gérées par les services sont les plus pratiques car elles ne nécessitent pas le déploiement de vos propres rôles et peuvent être automatiquement déployées sur de nouveaux comptes au sein de l'organisation. Malheureusement, cette méthode ne prend pas en charge les piles imbriquées, que nous utilisons à la fois dans la pile d'administration et dans la pile de membres. La seule pile qui peut être déployée de cette façon est la pile des rôles des membres.

Sachez que lors du déploiement dans l'ensemble de l'organisation, le compte de gestion de l'organisation n'est pas inclus. Par conséquent, si vous souhaitez corriger les résultats du compte de gestion de l'organisation, vous devez effectuer le déploiement sur ce compte séparément.

La pile de membres doit être déployée sur tous les comptes et régions, mais elle ne peut pas être déployée StackSets avec des autorisations gérées par le service car elle contient des piles imbriquées. Nous vous suggérons donc de déployer cette pile StackSets avec des autorisations autogérées.

La pile d'administration n'est déployée qu'une seule fois, elle peut donc être déployée en tant que CloudFormation pile simple ou en tant que pile StackSet avec des autorisations autogérées dans un seul compte et une seule région.

Conclusions de contrôle consolidées

Les comptes de votre organisation peuvent être configurés en activant ou en désactivant la fonction de consolidation des résultats de contrôle de Security Hub. Consultez les résultats des contrôles consolidés dans le guide de l'utilisateur d'AWS Security Hub.

> **Important**
>
> Lorsque cette fonctionnalité est activée, vous devez utiliser la version 2.0.0 ou ultérieure de la solution et activer le playbook « SC » (Security Control) à la fois dans les piles Admin et Member. Ces piles déploient les documents d'automatisation nécessaires pour fonctionner avec un contrôle IDs consolidé. Il n'est pas nécessaire de déployer des piles pour des normes individuelles (telles que AWS FSBP) lorsque vous utilisez des résultats de contrôle consolidés.

Déploiement en Chine

La solution prend en charge le déploiement dans les régions chinoises, mais vous devez utiliser les boutons de lancement suivants pour un déploiement en un clic dans les régions chinoises, plutôt que les boutons de lancement fournis dans d'autres sections de ce guide. L'utilisation des boutons « Lancer la solution » fournis dans les sections à venir de ce guide ne fonctionnera pas si vous effectuez un déploiement dans des régions de Chine. Vous pouvez toujours télécharger les modèles depuis n'importe quel lien vers un compartiment S3 et déployer les piles en chargeant le fichier modèle.

- automated-security-response-admin.modèle :

- automated-security-response-member-roles.template :

- automated-security-response-member.modèle :

GovCloud Déploiement (États-Unis)

La solution prend en charge le déploiement dans les régions GovCloud (États-Unis), mais vous devez utiliser les boutons de lancement suivants pour un déploiement en un clic dans les régions GovCloud (États-Unis), plutôt que les boutons de lancement fournis dans d'autres sections de ce guide. L'utilisation des boutons « Lancer la solution » fournis dans les sections à venir de ce guide ne fonctionnera pas si vous effectuez un déploiement dans des régions GovCloud (États-Unis). Vous pouvez toujours télécharger les modèles depuis n'importe quel lien vers un compartiment S3 et déployer les piles en chargeant le fichier modèle.

- automated-security-response-admin.modèle :

- automated-security-response-member-roles.template :

- automated-security-response-member.modèle :

CloudFormation Modèles AWS

automa

security-response-admin.template - Utilisez ce modèle pour lancer la solution Automated Security Response on AWS. Le modèle installe les composants principaux de la solution, une pile imbriquée pour les journaux AWS Step Functions et une pile imbriquée pour chaque norme de sécurité que vous choisissez d'activer.

Les services utilisés incluent Amazon Simple Notification Service, AWS Key Management Service, AWS Identity and Access Management, AWS Lambda, AWS Step Functions, Amazon CloudWatch Logs, Amazon S3 et AWS Systems Manager.

Support pour les comptes d'administrateur

Les modèles suivants sont installés dans le compte administrateur AWS Security Hub pour activer les normes de sécurité que vous souhaitez prendre en charge. Vous pouvez choisir le modèle à installer parmi les modèles suivants lors de l'installation du`automated-security-response-admin.template`.

automated-security-response-orchestrator-log.template - Crée un groupe de CloudWatch journaux pour la fonction Orchestrator Step.

automated-security-response-webui-nested-stack.template - Crée les ressources nécessaires à la prise en charge de l'interface utilisateur Web de la solution.

AFSBPStack.template - Règles relatives aux meilleures pratiques de sécurité de base d'AWS v1.0.0.

CIS120Stack.template - Benchmarks de la CIS Amazon Web Services Foundations, règles de la version v1.2.0.

CIS140Stack.template - Benchmarks de la CIS Amazon Web Services Foundations, règles de la version v1.4.0.

CIS300Stack.template - Benchmarks de la CIS Amazon Web Services Foundations, règles v3.0.0.

PCI321Stack.template - Règles PCI-DSS v3.2.1.

NISTStack.template - Institut national des normes et de la technologie (NIST), règles de la version 5.0.0.

SCStack.template - Règles de Security Controls v2.0.0.

Rôles des membres

View template

automa

security-response-member-roles.template - Définit les rôles de correction nécessaires dans chaque compte membre d'AWS Security Hub.

Comptes membres

View template

automa

security-response-member.template - Utilisez ce modèle après avoir configuré la solution principale pour installer les runbooks d'automatisation et les autorisations d'AWS Systems Manager sur chacun de vos comptes membres d'AWS Security Hub (y compris le compte administrateur). Ce modèle vous permet de choisir les playbooks standard de sécurité à installer.

`automated-security-response-member.template`Installe les modèles suivants en fonction de vos sélections :

automated-security-response-remediation-runbooks.template - Code de correction courant utilisé par une ou plusieurs normes de sécurité.

AFSBPMemberStack.template - Les meilleures pratiques de sécurité de base d'AWS v1.0.0, les paramètres, les autorisations et les manuels de correction.

CIS120MemberStack.template - Benchmarks CIS Amazon Web Services Foundations, paramètres de la version 1.2.0, autorisations et manuels de correction.

CIS140MemberStack.template - Benchmarks CIS Amazon Web Services Foundations, paramètres de la version 1.4.0, autorisations et manuels de correction.

CIS300MemberStack.template - Benchmarks CIS Amazon Web Services Foundations, paramètres de la version 3.0.0, autorisations et manuels de correction.

PCI321MemberStack.template - Paramètres, autorisations et manuels de correction de la norme PCI-DSS v3.2.1.

NISTMemberStack.template - National Institute of Standards and Technology (NIST), paramètres, autorisations et manuels de correction de la version 5.0.0.

SCMemberStack.template - Paramètres de contrôle de sécurité, autorisations et runbooks de correction.

automated-security-response-member-cloudtrail.template - Utilisé dans la fonctionnalité Action Log pour suivre et auditer l'activité des services.

Intégration du système de billetterie

Utilisez l'un des modèles suivants pour l'intégrer à votre système de billetterie.

View template

JiraBlu

- Déployez si vous utilisez Jira comme système de billetterie.

View template

Service

- Déployez si vous l'utilisez ServiceNow comme système de billetterie.

Si vous souhaitez intégrer un autre système de billetterie externe, vous pouvez utiliser l'une de ces piles comme modèle pour comprendre comment implémenter votre propre intégration personnalisée.

Déploiement automatisé - StackSets

> **Note**
>
> Nous vous recommandons de déployer avec StackSets. Toutefois, pour les déploiements à compte unique ou à des fins de test ou d'évaluation, envisagez l'option de déploiement stacks.

Avant de lancer la solution, passez en revue l'architecture, les composants de la solution, la sécurité et les considérations de conception abordées dans ce guide. Suivez les step-by-step instructions de cette section pour configurer et déployer la solution dans vos organisations AWS.

Temps de déploiement : environ 30 minutes par compte, selon StackSet les paramètres.

Conditions préalables

AWS Organizations vous aide à gérer et à gouverner de manière centralisée votre environnement et vos ressources AWS multi-comptes. StackSets fonctionnent de manière optimale avec AWS Organizations.

Si vous avez déjà déployé la version v1.3.x ou une version antérieure de cette solution, vous devez désinstaller la solution existante. Pour plus d'informations, reportez-vous à la section Mettre à jour la solution.

Avant de déployer cette solution, passez en revue votre déploiement d'AWS Security Hub :

- Il doit y avoir un compte administrateur Security Hub délégué dans votre organisation AWS.
- Security Hub doit être configuré pour agréger les résultats entre les régions. Pour plus d'informations, reportez-vous à la section Agrégation des résultats entre les régions dans le guide de l'utilisateur d'AWS Security Hub.
- Vous devez activer Security Hub pour votre organisation dans chaque région où vous utilisez AWS.

Cette procédure suppose que vous disposez de plusieurs comptes utilisant AWS Organizations et que vous avez délégué un compte administrateur AWS Organizations et un compte administrateur AWS Security Hub.

Notez que cette solution fonctionne à la fois avec AWS Security Hub et AWS Security Hub CSPM.

Vue d'ensemble du déploiement

> **Note**
>
> StackSets le déploiement de cette solution utilise une combinaison de gestion des services et d'autogestion. StackSets L'autogéré StackSets doit être utilisé actuellement, car ils utilisent le mode imbriqué StackSets, qui n'est pas encore pris en charge par le service géré. StackSets

StackSets Déployez-le à partir d'un compte d'administrateur délégué dans vos organisations AWS.

Planification

Utilisez le formulaire suivant pour faciliter le StackSets déploiement. Préparez vos données, puis copiez-collez les valeurs pendant le déploiement.

```
AWS Organizations admin account ID: _________________
Security Hub admin account ID: _________________
CloudTrail Logs Group: ____________________________
Member account IDs (comma-separated list):
____________________,
____________________,
____________________,
____________________,
____________________
AWS Organizations OUs (comma-separated list):
____________________,
```

```
_____',
_____',
_____',
_____
```

(Facultatif) Étape 0 : Déployer la pile d'intégration des tickets

- Si vous avez l'intention d'utiliser la fonctionnalité de billetterie, déployez d'abord la pile d'intégration de billetterie dans votre compte administrateur Security Hub.
- Copiez le nom de la fonction Lambda depuis cette pile et fournissez-le comme entrée à la pile d'administration (voir Étape 1).

Étape 1 : Lancez la pile d'administration dans le compte administrateur délégué du Security Hub

- À l'aide d'un outil autogéré StackSet, lancez le CloudFormation modèle `automated-security-response-admin.template` AWS sur votre compte d'administrateur AWS Security Hub dans la même région que votre administrateur Security Hub. Ce modèle utilise des piles imbriquées.
- Choisissez les normes de sécurité à installer. Par défaut, seul SC est sélectionné (recommandé).
- Choisissez un groupe de journaux Orchestrator existant à utiliser. Sélectionnez `Yes` s'il existe `SO0111-ASR- Orchestrator` déjà depuis une installation précédente.
- Choisissez d'activer ou non l'interface utilisateur Web de la solution. Si vous choisissez d'activer cette fonctionnalité, vous devez également saisir une adresse e-mail pour qu'un rôle d'administrateur soit attribué.
- Sélectionnez vos préférences en matière de collecte de CloudWatch statistiques relatives à l'état de fonctionnement de la solution.

Pour plus d'informations sur l'autogestion StackSets, reportez-vous à la section Accorder des autorisations autogérées dans le guide de CloudFormation l'utilisateur AWS.

Étape 2 : installer les rôles de correction dans chaque compte membre d'AWS Security Hub

Attendez que l'étape 1 soit terminée, car le modèle de l'étape 2 fait référence aux rôles IAM créés par l'étape 1.

- À l'aide d'un service géré StackSet, lancez le CloudFormation modèle `automated-security-response-member-roles.template` AWS dans une seule région dans chaque compte de vos organisations AWS.

- Choisissez d'installer ce modèle automatiquement lorsqu'un nouveau compte rejoint l'organisation.
- Entrez l'ID de compte de votre compte d'administrateur AWS Security Hub.
- Entrez une valeur pour le `namespace` qui sera utilisé pour éviter les conflits de noms de ressources avec un déploiement précédent ou simultané dans le même compte. Entrez une chaîne de 9 caractères alphanumériques minuscules maximum.

Étape 3 : Lancez la pile de membres dans chaque compte membre et région d'AWS Security Hub

- À l'aide de l'autogestion StackSets, lancez le CloudFormation modèle `automated-security-response-member.template` AWS dans toutes les régions où vous disposez de ressources AWS dans chaque compte de votre organisation AWS géré par le même administrateur du Security Hub.

> **Note**
>
> Jusqu'à ce que le StackSets support géré par les services soit intégré, vous devez effectuer cette étape pour tous les nouveaux comptes qui rejoignent l'organisation.

- Choisissez les playbooks Security Standard à installer.
- Indiquez le nom d'un groupe de CloudTrail journaux (utilisé par certaines corrections).
- Entrez l'ID de compte de votre compte d'administrateur AWS Security Hub.
- Entrez une valeur pour le `namespace` qui sera utilisé pour éviter les conflits de noms de ressources avec un déploiement précédent ou simultané dans le même compte. Entrez une chaîne de 9 caractères alphanumériques minuscules maximum. Cela doit correspondre à la `namespace` valeur que vous avez sélectionnée pour la pile des rôles des membres. De plus, la valeur de l'espace de noms n'a pas besoin d'être unique par compte membre.

(Facultatif) Étape 0 : Lancer une pile d'intégration d'un système de tickets

1. Si vous avez l'intention d'utiliser la fonctionnalité de billetterie, lancez d'abord la pile d'intégration correspondante.
2. Choisissez les piles d'intégration fournies pour Jira ou ServiceNow utilisez-les comme modèle pour implémenter votre propre intégration personnalisée.

   Pour déployer la pile Jira, procédez comme suit :

a. Entrez un nom pour votre pile.

b. Fournissez l'URI de votre instance Jira.

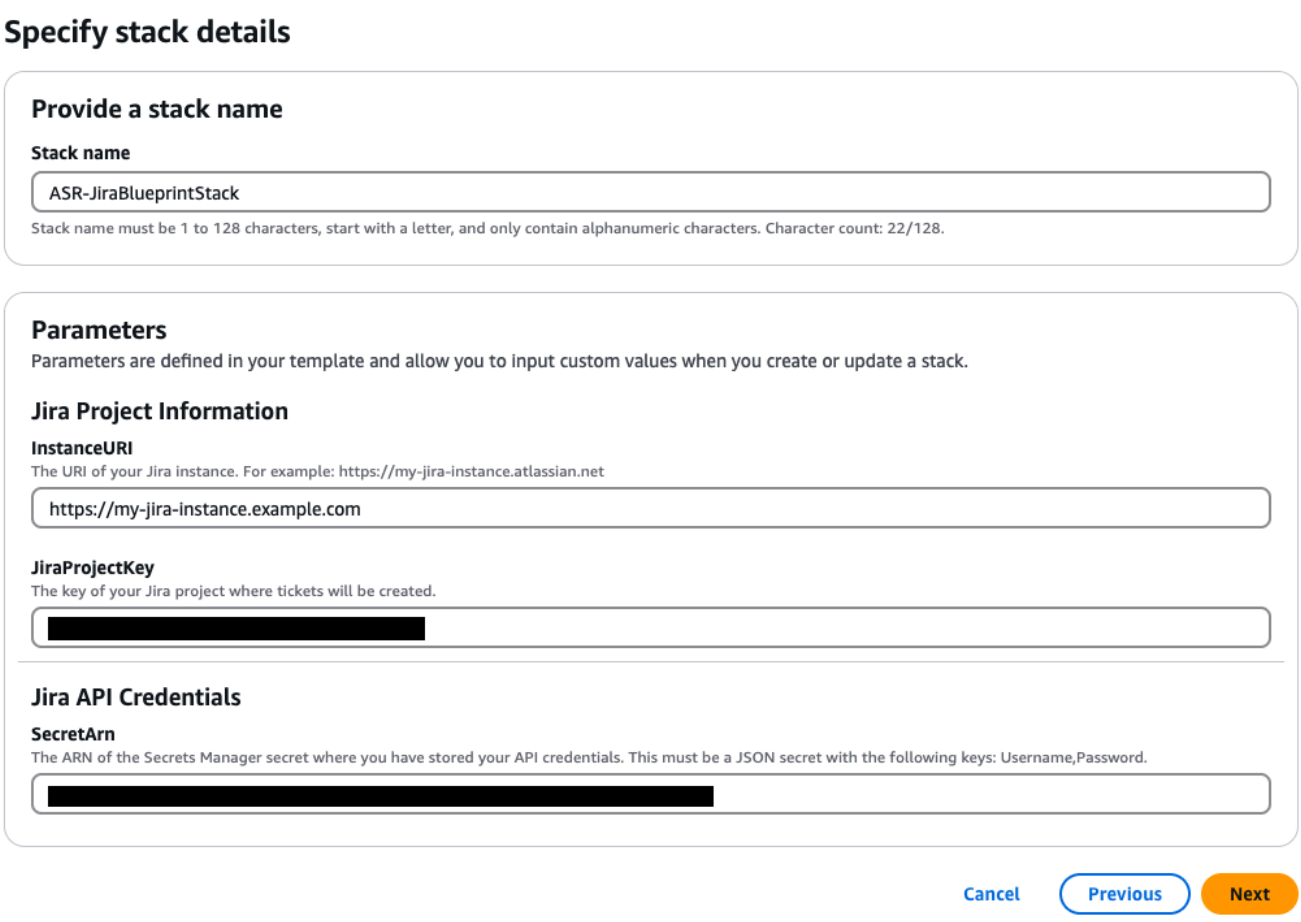
c. Fournissez la clé de projet pour le projet Jira auquel vous souhaitez envoyer des tickets.

d. Créez un nouveau secret clé-valeur dans Secrets Manager qui contient votre `Username` Jira et. `Password`

> **Note**
>
> Vous pouvez choisir d'utiliser une clé d'API Jira à la place de votre mot de passe en fournissant votre nom d'utilisateur `Username` et votre clé API en tant que. `Password`

e. Ajoutez l'ARN de ce secret comme entrée à la pile.

Fournissez un nom de pile, des informations sur le projet Jira et des informations d'identification de l'API Jira.



Configuration du champ Jira :

Après avoir déployé la pile Jira, vous pouvez personnaliser les champs des tickets Jira en définissant la variable d'`JIRA_FIELDS_MAPPING`environnement sur la fonction Lambda. Cette chaîne JSON remplace les champs de ticket Jira par défaut et doit suivre la structure des champs de l'API Jira.

Valeurs par défaut lorsqu'il `JIRA_FIELDS_MAPPING` est vide ou que les champs ne sont pas spécifiés :

- priorité : `{"id": "3"}` (Priorité moyenne)
- type de problème : **`{"id": "10006"}`** (Tâche)
- AccountID : Récupéré automatiquement à l'aide du point de terminaison de l'API `GET /rest/api/2/myself`

  Exemple de configuration avec des champs personnalisés :

```
{
  "reporter": {"accountId": "123456:494dcbff-1b80-482c-a89d-56ae81c145a4"},
  "priority": {"id": "1"},
  "issuetype": {"id": "10006"},
  "assignee": {"accountId": "123456:another-user-id"},
  "customfield_10001": "custom value"
}
```

  Champ IDs Jira commun :

- Priorité IDs : 1 (la plus élevée), 2 (haute), 3 (moyenne), 4 (faible), 5 (la plus faible)
- ID du type de problème : varie en fonction du projet Jira (par exemple, 10006 pour Task)
- Identifiant du compte : Format `123456:494dcbff-1b80-482c-a89d-56ae81c145a4`

  Vous pouvez trouver votre champ IDs et votre compte Jira à IDs l'aide de l'API REST de Jira :

- `GET /rest/api/2/myself`pour l'identifiant du compte
- `GET /rest/api/2/priority`pour la priorité IDs
- `GET /rest/api/2/project/{projectKey}`pour le type de problème IDs

  Pour plus d'informations, reportez-vous au format POST Issue POST de l'API Jira REST v2.

  Pour déployer la ServiceNow pile :

f. Entrez un nom pour votre pile.

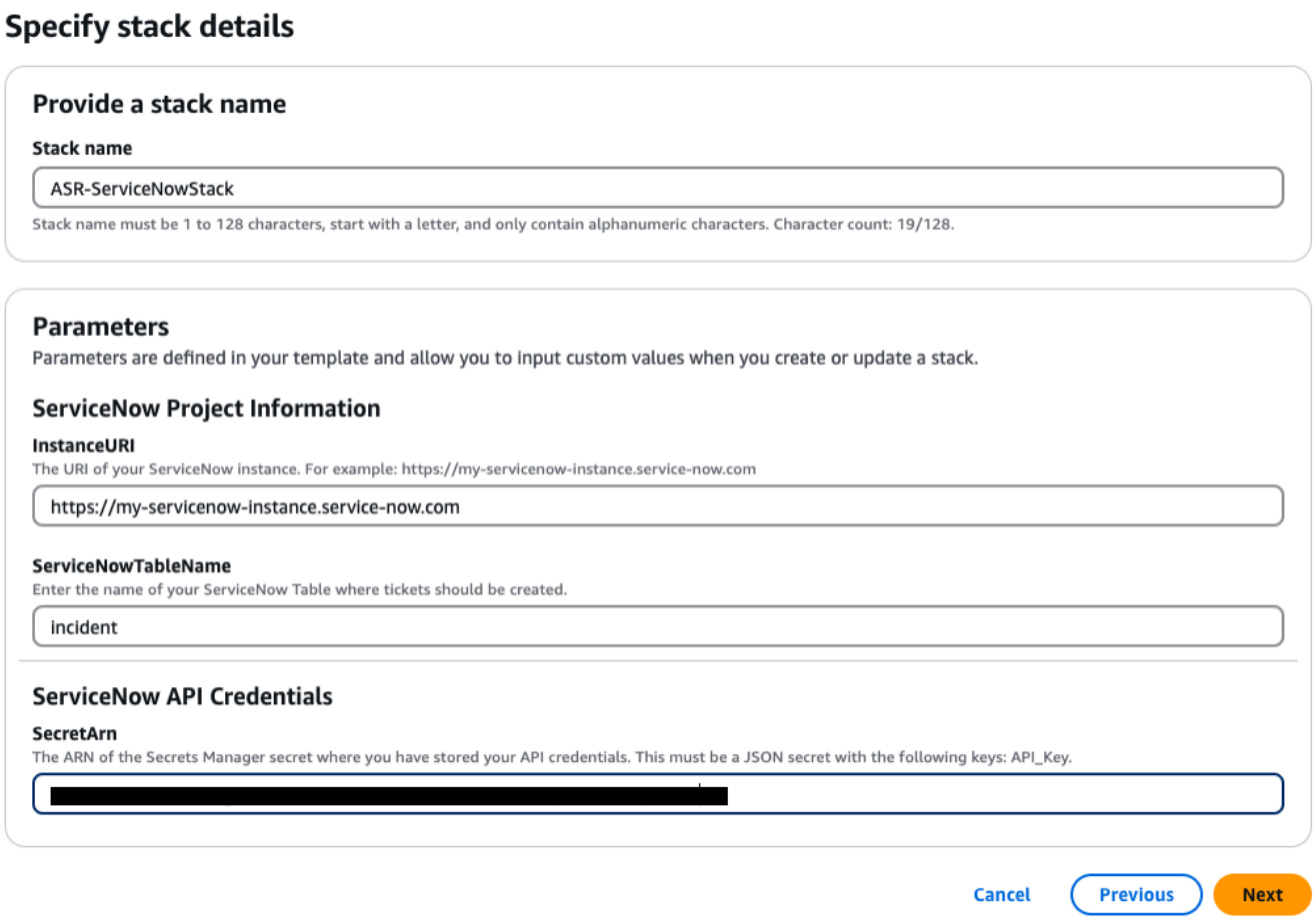
g. Indiquez l'URI de votre ServiceNow instance.

h. Entrez le nom ServiceNow de votre table.

i. Créez une clé d'API ServiceNow avec l'autorisation de modifier la table dans laquelle vous souhaitez écrire.

j. Créez un secret dans Secrets Manager avec la clé `API_Key` et fournissez l'ARN secret en entrée de la pile.

Fournissez un nom de pile, des informations sur le ServiceNow projet et des informations d'identification de ServiceNow l'API.



Pour créer une pile d'intégration personnalisée : incluez une fonction Lambda que l'orchestrateur de solutions Step Functions peut appeler pour chaque correction. La fonction Lambda doit prendre les données fournies par Step Functions, construire une charge utile conformément aux exigences de votre système de billetterie et demander à votre système de créer le ticket.

Étape 1 : Lancez la pile d'administration dans le compte administrateur délégué du Security Hub

1. Lancez la pile d'`automated-security-response-admin.template`administration avec votre compte d'administrateur Security Hub. Généralement, un par organisation dans une seule région. Comme cette pile utilise des piles imbriquées, vous devez déployer ce modèle en tant que modèle autogéré. StackSet

Parameters

Paramètre	Par défaut	Description
Charger SC Admin Stack	`yes`	Spécifiez s'il faut installer les composants d'administration pour la correction automatique des contrôles SC.
Charger la pile d'adminis tration AFSBP	no	Spécifiez s'il faut installer les composants d'administration pour la correction automatique des contrôles FSBP.
Charger CIS120 Admin Stack	no	Spécifiez s'il faut installer les composants d'administration pour la correction automatique des CIS120 contrôles.
Charger CIS140 Admin Stack	no	Spécifiez s'il faut installer les composants d'administration pour la correction automatique des CIS140 contrôles.
Charger CIS300 Admin Stack	no	Spécifiez s'il faut installer les composants d'administration pour la correction automatique des CIS300 contrôles.

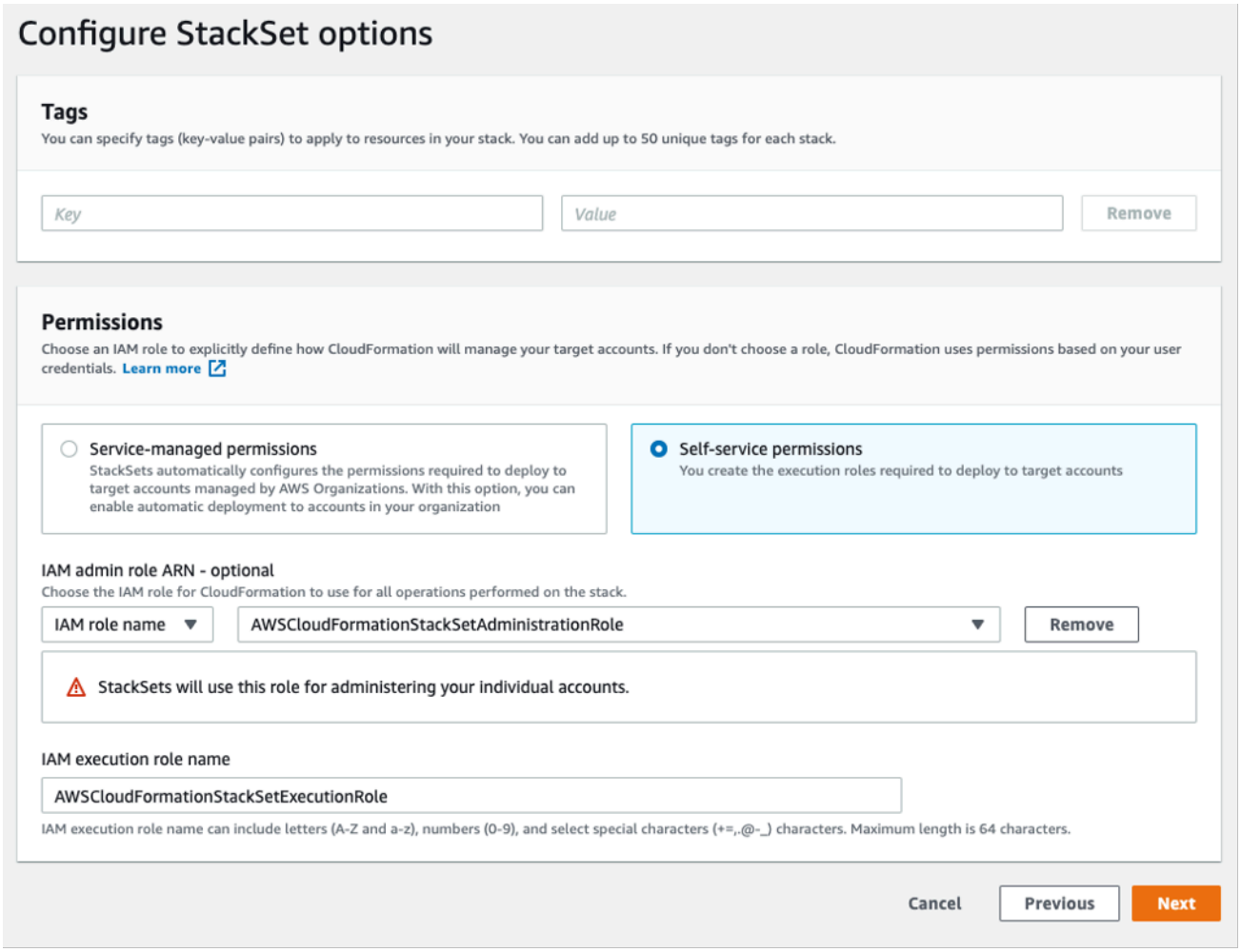
Paramètre	Par défaut	Description
Charger PC1321 Admin Stack	no	Spécifiez s'il faut installer les composants d'administration pour la correction automatique des PC1321 contrôles.
Charger le NIST Admin Stack	no	Spécifiez s'il faut installer les composants d'administration pour la correction automatique des contrôles NIST.
Réutiliser le groupe de journaux Orchestrator	no	Choisissez de réutiliser ou non un groupe de `SO0111-ASR-Orchestrator` CloudWatch journaux existant. Cela simplifie la réinstallation et les mises à niveau sans perdre les données du journal d'une version précédente. Réutilisez l'existant, `Orchestrator Log Group` choisissez `yes` s'il existe `Orchestrator Log Group` toujours depuis un déploiement antérieur dans ce compte, sinonno. Si vous effectuez une mise à jour de la pile à partir d'une version antérieure à la version 2.3.0, choisissez no

Paramètre	Par défaut	Description
ShouldDeployWebUI	`yes`	Déployez les composants de l'interface utilisateur Web, notamment API Gateway, les fonctions Lambda et CloudFront la distribution. Sélectionnez « Oui » pour activer l'interface utilisateur Web permettant de visualise r les résultats et l'état des mesures correctives. Si vous choisissez de désactiver cette fonctionnalité, vous pouvez toujours configurer des corrections automatisées et exécuter des corrections à la demande à l'aide de l'action personnalisée Security Hub CSPM.
AdminUserEmail	(Entrée facultative)	Adresse e-mail de l'utilisa teur administrateur initial. Cet utilisateur aura un accès administratif complet à l'interfa ce utilisateur Web d'ASR. Obligatoire uniquement lorsque l'interface utilisateur Web est activée.
Utiliser CloudWatch les métriques	`yes`	Spécifiez si vous souhaitez activer CloudWatch les métriques pour surveiller la solution. Cela créera un CloudWatch tableau de bord pour consulter les statistiques.

Paramètre	Par défaut	Description
Utiliser les alarmes CloudWatch métriques	`yes`	Spécifiez si vous souhaitez activer CloudWatch les alarmes métriques pour la solution. Cela créera des alarmes pour certaines métriques collectées par la solution.
RemediationFailureAlarmThreshold	5	Spécifiez le seuil pour le pourcentage d'échecs de correction par ID de contrôle. Par exemple, si vous entrez5, vous recevez une alarme si un ID de contrôle échoue dans plus de 5 % des cas de correction au cours d'une journée donnée. Ce paramètre ne fonctionne que si des alarmes sont créées (voir le paramètre Utiliser CloudWatch les alarmes métriques).

Paramètre	Par défaut	Description
EnableEnhancedCloudWatchMetrics	no	Si`yes`, crée des CloudWatch métriques supplémentaires pour suivre tous les contrôles IDs individuellement sur le CloudWatch tableau de bord et sous forme d' CloudWatch alarmes. Consultez la section Coût pour comprendre les coûts supplémentaires que cela entraîne.
TicketGenFunctionName	(Entrée facultative)	Facultatif. Laissez ce champ vide si vous ne souhaitez pas intégrer de système de billetterie. Sinon, fournissez le nom de la fonction Lambda à partir de la sortie de la pile de l'étape 0, par exemple :. `SO0111-ASR-ServiceNow-TicketGenerator`

StackSet Options de configuration



1. Pour le paramètre Account numbers, entrez l'ID de compte du compte administrateur AWS Security Hub.
2. Pour le paramètre Specify regions, sélectionnez uniquement la région dans laquelle l'administrateur Security Hub est activé. Attendez que cette étape soit terminée avant de passer à l'étape 2.

Étape 2 : installer les rôles de correction dans chaque compte membre d'AWS Security Hub

Utilisez un service géré StackSets pour déployer le modèle de rôles des membres,. `automated-security-response-member-roles.template` Cela StackSet doit être déployé dans une région par compte membre. Il définit les rôles globaux qui autorisent les appels d'API entre comptes à partir de la fonction d'étape ASR Orchestrator.

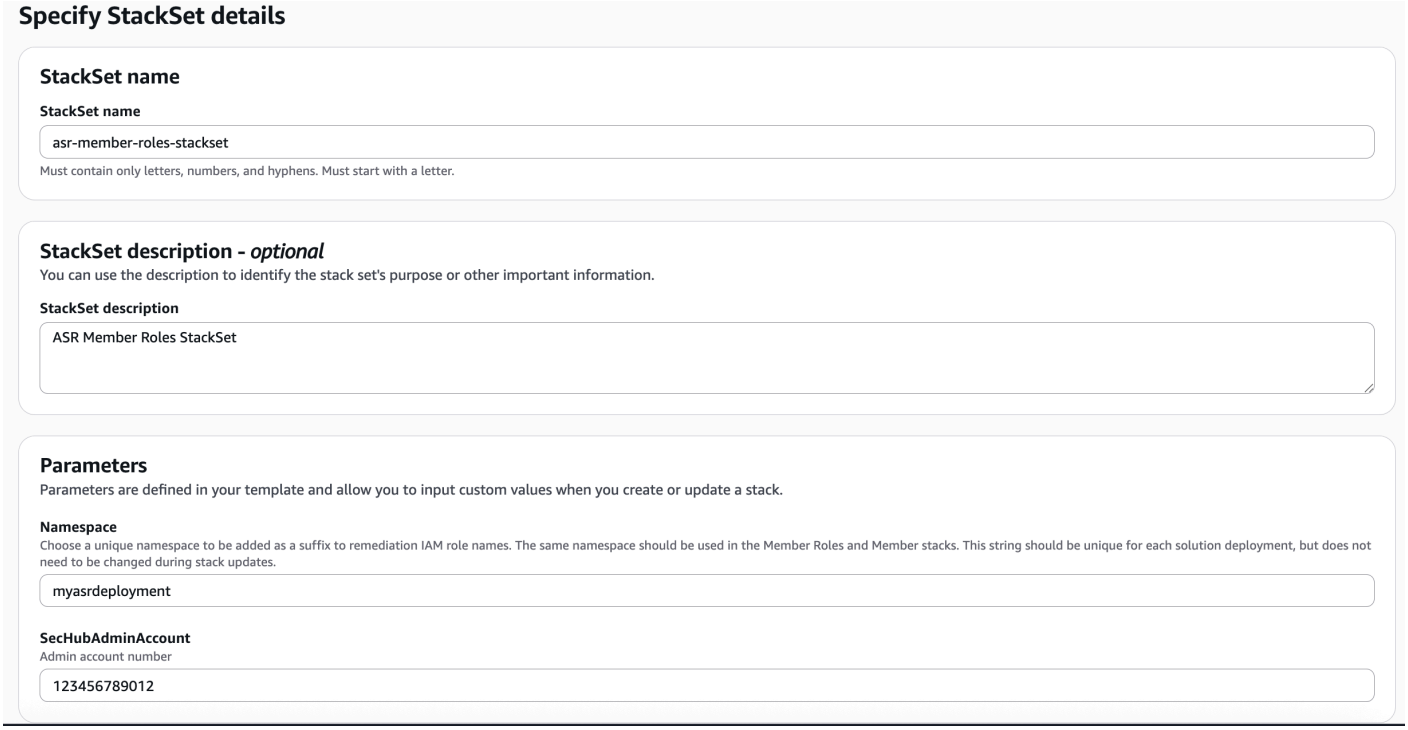
Parameters

Paramètre	Par défaut	Description
Namespace	*<Requires input>*	Entrez une chaîne de 9 caractères alphanumériques minuscules maximum. Espace de noms unique à ajouter en tant que suffixe aux noms de rôles IAM de correction. Le même espace de noms doit être utilisé dans les rôles des membres et dans les piles de membres. Cette chaîne doit être unique pour chaque déploiement de solution, mais il n'est pas nécessaire de la modifier lors des mises à jour de la pile. Il n'est pas nécessaire que la valeur de l'espace de noms soit unique par compte membre.
Administrateur du compte Sec Hub	*<Requires input>*	Entrez l'ID de compte à 12 chiffres du compte administrateur AWS Security Hub. Cette valeur accorde des autorisations au rôle de solution du compte administrateur.

1. Déployez dans l'ensemble de l'organisation (standard) ou dans les unités organisationnelles, conformément aux politiques de votre organisation.
2. Activez le déploiement automatique afin que les nouveaux comptes des organisations AWS reçoivent ces autorisations.

3. Pour le paramètre Spécifier les régions, sélectionnez une seule région. Les rôles IAM sont globaux. Vous pouvez passer à l'étape 3 pendant le StackSet déploiement.

Spécifiez StackSet les détails



Étape 3 : Lancez la pile de membres dans chaque compte membre et région d'AWS Security Hub

Comme la pile de membres utilise des piles imbriquées, vous devez effectuer le déploiement en tant que solution autogérée. StackSet Cela ne prend pas en charge le déploiement automatique vers de nouveaux comptes dans l'organisation AWS.

Parameters

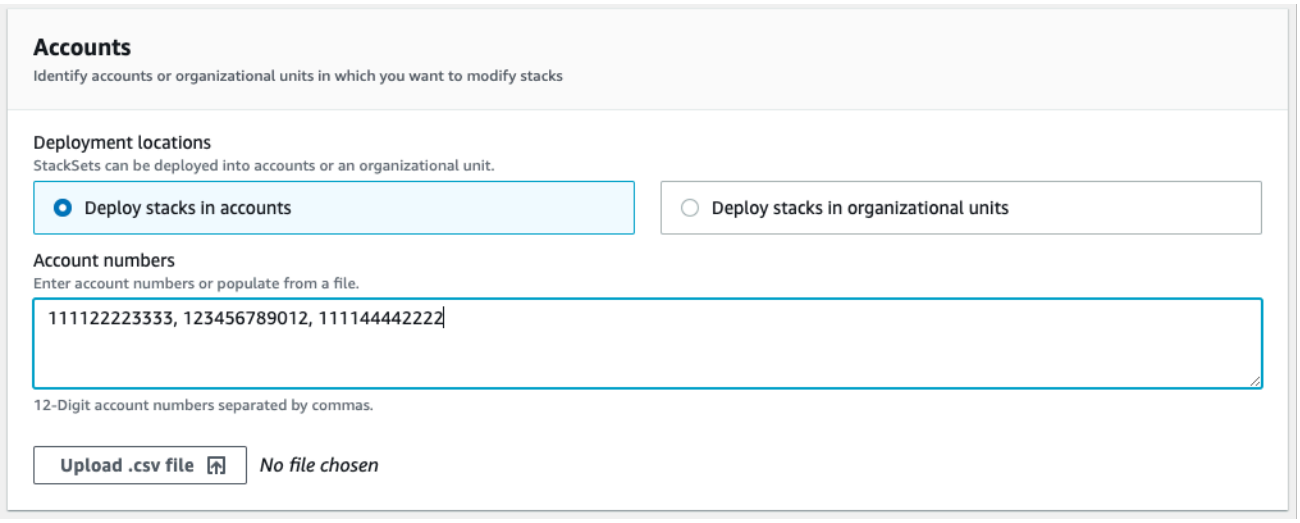
Paramètre	Par défaut	Description
Indiquez le nom du LogGroup à utiliser pour créer des filtres métriques et des alarmes	`<Requires input>`	Spécifiez le nom d'un groupe CloudWatch Logs dans lequel sont CloudTrail enregistrés les appels d'API. Ceci est

Paramètre	Par défaut	Description
		utilisé pour les corrections CIS 3.1-3.14.
Load SC Member Stack	`yes`	Spécifiez s'il faut installer les composants membres pour la correction automatique des contrôles SC.
Charger la pile de membres de l'AFSBP	no	Spécifiez s'il faut installer les composants membres pour la correction automatique des contrôles FSBP.
Charger la pile de CIS120 membres	no	Spécifiez s'il faut installer les composants membres pour la correction automatique des CIS120 contrôles.
Charger la pile de CIS140 membres	no	Spécifiez s'il faut installer les composants membres pour la correction automatique des CIS140 contrôles.
Charger la pile de CIS300 membres	no	Spécifiez s'il faut installer les composants membres pour la correction automatique des CIS300 contrôles.
Charger la pile de PC1321 membres	no	Spécifiez s'il faut installer les composants membres pour la correction automatique des PC1321 contrôles.
Charger la pile de membres du NIST	no	Spécifiez s'il faut installer les composants membres pour la correction automatique des contrôles NIST.

Paramètre	Par défaut	Description
Création d'un compartiment S3 pour la journalisation des audits Redshift	no	Indiquez `yes` si le compartiment S3 doit être créé pour la correction FSBP RedShift .4. Pour plus de détails sur le compartiment S3 et la correction, consultez la correction Redshift.4 dans le guide de l'utilisateur d'AWS Security Hub.
Compte administrateur Sec Hub	*<Requires input>*	Entrez l'ID de compte à 12 chiffres du compte administrateur AWS Security Hub.
Namespace	*<Requires input>*	Entrez une chaîne de 9 caractères alphanumériques minuscules maximum. Cette chaîne fait partie des noms de rôles IAM et du compartiment Action Log S3. Utilisez la même valeur pour le déploiement de la pile de membres et le déploiement de la pile de rôles des membres. La chaîne doit être unique pour chaque déploiement de solution, mais il n'est pas nécessaire de la modifier lors des mises à jour de la pile.

Paramètre	Par défaut	Description
EnableCloudTrailForASRActionJournal	no	Indiquez `yes` si vous souhaitez surveiller les événements de gestion menés par la solution sur le CloudWatch tableau de bord. La solution crée une CloudTrail trace dans chaque compte membre que vous sélectionnez`yes`. Vous devez déployer la solution dans une organisation AWS pour activer cette fonctionnalité. En outre, vous ne pouvez activer cette fonctionnalité que dans une seule région au sein du même compte. Consultez la section Coût pour comprendre les coûts supplémentaires que cela entraîne.

Comptes



Lieux de déploiement : vous pouvez spécifier une liste de numéros de compte ou d'unités organisationnelles.

Spécifiez les régions : sélectionnez toutes les régions dans lesquelles vous souhaitez corriger les résultats. Vous pouvez ajuster les options de déploiement en fonction du nombre de comptes et de régions. La simultanéité des régions peut être parallèle.

Déploiement automatisé - Stacks

> **Note**
>
> Pour les clients ayant plusieurs comptes, nous recommandons vivement le déploiement avec StackSets.

Avant de lancer la solution, passez en revue l'architecture, les composants de la solution, la sécurité et les considérations de conception abordées dans ce guide. Suivez les step-by-step instructions de cette section pour configurer et déployer la solution dans votre compte.

Temps de déploiement : environ 30 minutes

Conditions préalables

Avant de déployer cette solution, assurez-vous qu'AWS Security Hub se trouve dans la même région AWS que vos comptes principal et secondaire. Si vous avez déjà déployé cette solution, vous devez désinstaller la solution existante. Pour plus d'informations, reportez-vous à la section Mettre à jour la solution.

Vue d'ensemble du déploiement

Suivez les étapes ci-dessous pour déployer cette solution sur AWS.

(Facultatif) Étape 0 : Lancer une pile d'intégration d'un système de tickets

- Si vous avez l'intention d'utiliser la fonctionnalité de billetterie, déployez d'abord la pile d'intégration de billetterie dans votre compte administrateur Security Hub.
- Copiez le nom de la fonction Lambda depuis cette pile et fournissez-le comme entrée à la pile d'administration (voir Étape 1).

Étape 1 : Lancez la pile d'administration

- Lancez le CloudFormation modèle `automated-security-response-admin.template` AWS sur votre compte d'administrateur AWS Security Hub.
- Choisissez les normes de sécurité à installer.
- Choisissez un groupe de journaux Orchestrator existant à utiliser (sélectionnez `Yes` s'il existe `SO0111-ASR-Orchestrator` déjà depuis une installation précédente).

Étape 2 : installer les rôles de correction dans chaque compte membre d'AWS Security Hub

- Lancez le CloudFormation modèle `automated-security-response-member-roles.template` AWS dans une région par compte membre.
- Entrez l'IG de compte à 12 chiffres pour le compte administrateur AWS Security Hub.

Étape 3 : Lancez la pile de membres

- Spécifiez le nom du groupe de CloudWatch journaux à utiliser avec les corrections CIS 3.1-3.14. Il doit s'agir du nom du groupe de CloudWatch journaux qui reçoit CloudTrail les journaux.
- Choisissez si vous souhaitez installer les rôles de correction. Installez ces rôles une seule fois par compte.
- Sélectionnez les playbooks à installer.
- Entrez l'ID de compte du compte administrateur AWS Security Hub.

Étape 4 : (Facultatif) Ajustez les mesures correctives disponibles

- Supprimez toutes les corrections pour chaque compte membre. Cette étape est facultative.

(Facultatif) Étape 0 : Lancer une pile d'intégration d'un système de tickets

1. Si vous avez l'intention d'utiliser la fonctionnalité de billetterie, lancez d'abord la pile d'intégration correspondante.
2. Choisissez les piles d'intégration fournies pour Jira ou ServiceNow utilisez-les comme modèle pour implémenter votre propre intégration personnalisée.

   Pour déployer la pile Jira, procédez comme suit :

a. Entrez un nom pour votre pile.

b. Fournissez l'URI de votre instance Jira.

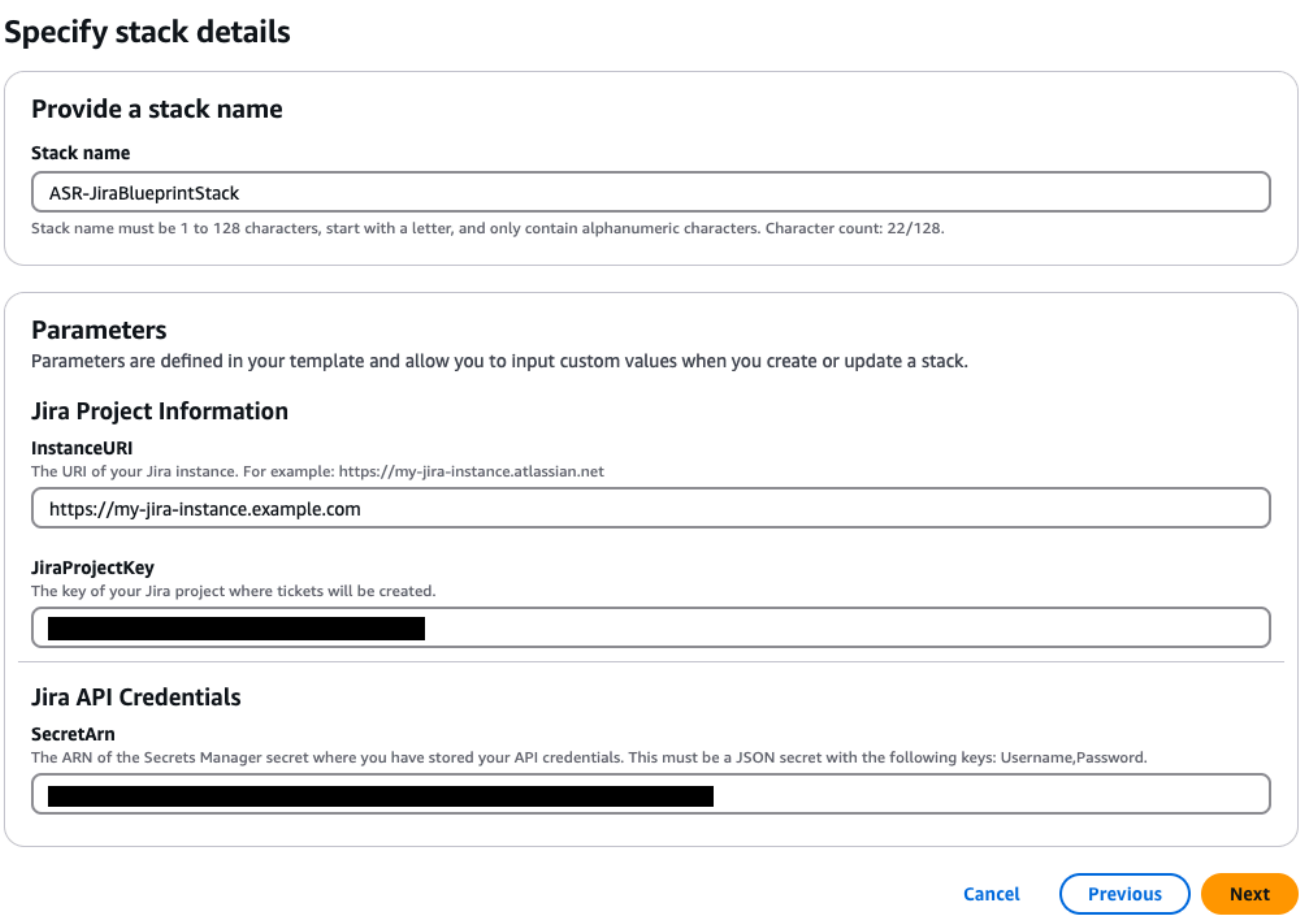
c. Fournissez la clé de projet pour le projet Jira auquel vous souhaitez envoyer des tickets.

d. Créez un nouveau secret clé-valeur dans Secrets Manager qui contient votre `Username` Jira et. `Password`

> **Note**
>
> Vous pouvez choisir d'utiliser une clé d'API Jira à la place de votre mot de passe en fournissant votre nom d'utilisateur `Username` et votre clé API en tant que. `Password`

e. Ajoutez l'ARN de ce secret comme entrée à la pile.

« Fournissez un nom de pile, des informations sur le projet Jira et des informations d'identification de l'API Jira.



Configuration du champ Jira :

Pour plus d'informations sur la personnalisation des champs de ticket Jira, reportez-vous à la section Configuration des champs Jira à l'étape 0 du déploiement. StackSet

Pour déployer la ServiceNow pile :

f. Entrez un nom pour votre pile.

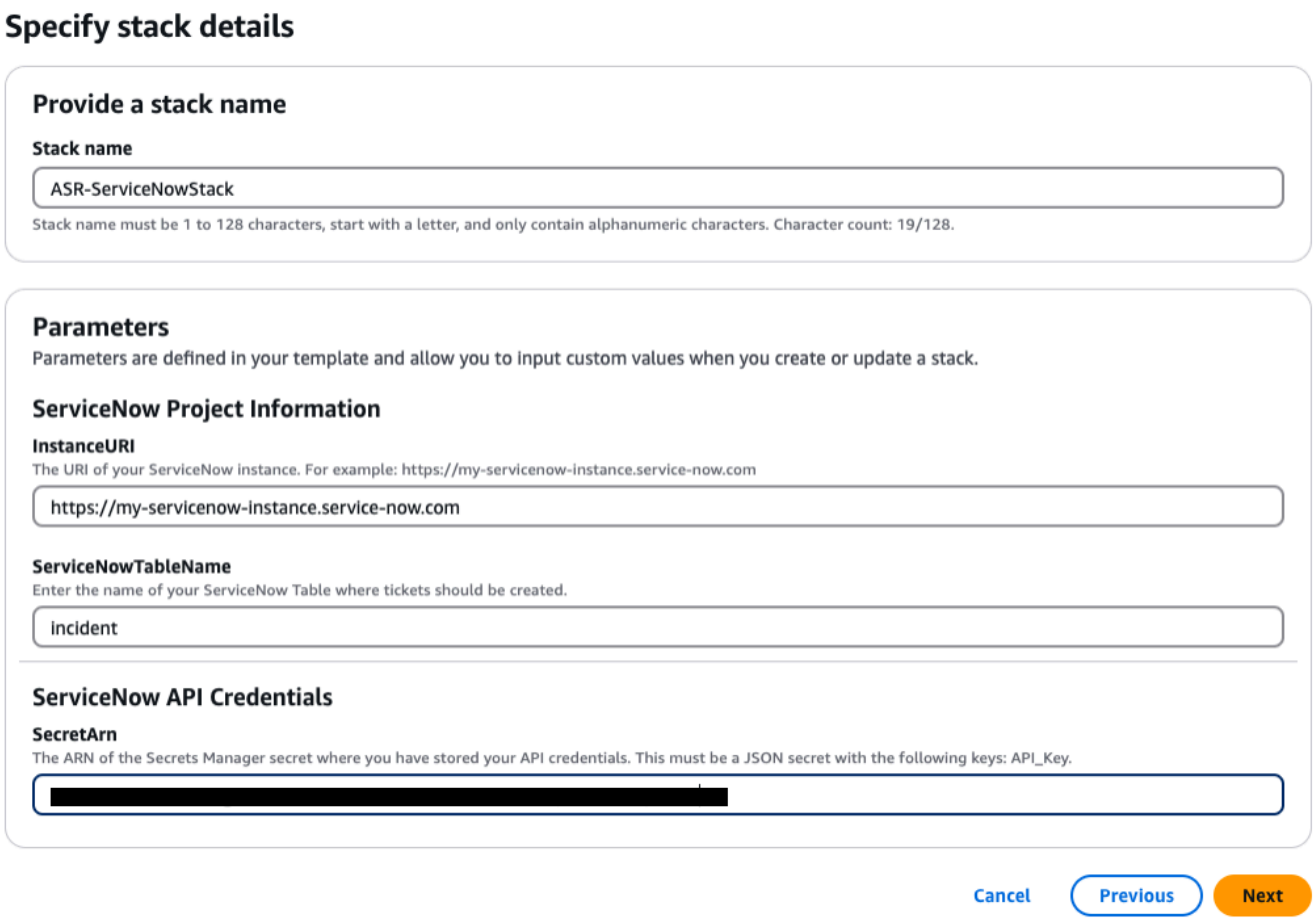
g. Indiquez l'URI de votre ServiceNow instance.

h. Entrez le nom ServiceNow de votre table.

i. Créez une clé d'API ServiceNow avec l'autorisation de modifier la table dans laquelle vous souhaitez écrire.

j. Créez un secret dans Secrets Manager avec la clé `API_Key` et fournissez l'ARN secret en entrée de la pile.

Fournissez un nom de pile, des informations sur le ServiceNow projet et des informations d'identification de ServiceNow l'API.



Pour créer une pile d'intégration personnalisée : incluez une fonction Lambda que l'orchestrateur de solutions Step Functions peut appeler pour chaque correction. La fonction Lambda doit prendre les données fournies par Step Functions, construire une charge utile conformément aux exigences de votre système de billetterie et demander à votre système de créer le ticket.

Étape 1 : Lancez la pile d'administration

> **Important**
>
> Cette solution inclut la collecte de données. Nous utilisons ces données pour mieux comprendre la façon dont les clients utilisent cette solution et les services et produits associés. AWS est propriétaire des données recueillies dans le cadre de cette enquête. La collecte de données est soumise à l'avis de confidentialité d'AWS.

Ce CloudFormation modèle AWS automatisé déploie la solution Automated Security Response on AWS dans le cloud AWS. Avant de lancer la pile, vous devez activer Security Hub et remplir les conditions requises.

> **Note**
>
> Vous êtes responsable du coût des services AWS utilisés lors de l'exécution de cette solution. Pour plus de détails, consultez la section Coût de ce guide et consultez la page Web de tarification de chaque service AWS utilisé dans cette solution.

1. Connectez-vous à l'AWS Management Console depuis le compte sur lequel l'AWS Security Hub est actuellement configuré, puis utilisez le bouton ci-dessous pour lancer le CloudFormation modèle `automated-security-response-admin.template` AWS.

   Launch solution

   Vous pouvez également télécharger le modèle comme point de départ pour votre propre implémentation.

2. Le modèle est lancé par défaut dans la région USA Est (Virginie du Nord). Pour lancer cette solution dans une autre région AWS, utilisez le sélecteur de région dans la barre de navigation de l'AWS Management Console.

> **Note**
>
> Cette solution utilise AWS Systems Manager, qui n'est actuellement disponible que dans certaines régions AWS. La solution fonctionne dans toutes les régions qui prennent en charge ce service. Pour connaître la disponibilité la plus récente par région, consultez la liste des services régionaux AWS.

3. Sur la page Create stack, vérifiez que l'URL du modèle est correcte dans la zone de texte URL Amazon S3, puis choisissez Next.
4. Sur la page Spécifier les détails de la pile, attribuez un nom à votre pile de solutions. Pour plus d'informations sur les limites relatives aux caractères de dénomination, reportez-vous aux limites IAM et STS dans le guide de l'utilisateur d'AWS Identity and Access Management.
5. Sur la page Paramètres, choisissez Next.

Paramètre	Par défaut	Description
Charger SC Admin Stack	`yes`	Spécifiez s'il faut installer les composants d'administration pour la correction automatiq ue des contrôles SC.
Charger la pile d'adminis tration AFSBP	no	Spécifiez s'il faut installer les composants d'administration pour la correction automatiq ue des contrôles FSBP.
Charger CIS120 Admin Stack	no	Spécifiez s'il faut installer les composants d'administration pour la correction automatiq ue des CIS120 contrôles.
Charger CIS140 Admin Stack	no	Spécifiez s'il faut installer les composants d'administration

Paramètre	Par défaut	Description
		pour la correction automatiq ue des CIS140 contrôles.
Charger CIS300 Admin Stack	no	Spécifiez s'il faut installer les composants d'administration pour la correction automatiq ue des CIS300 contrôles.
Charger PC1321 Admin Stack	no	Spécifiez s'il faut installer les composants d'administration pour la correction automatiq ue des PC1321 contrôles.
Charger le NIST Admin Stack	no	Spécifiez s'il faut installer les composants d'administration pour la correction automatiq ue des contrôles NIST.

Paramètre	Par défaut	Description
Réutiliser le groupe de journaux Orchestrator	no	Choisissez de réutiliser ou non un groupe de `S00111-ASR-Orchestrator` CloudWatch journaux existant. Cela simplifie la réinstallation et les mises à niveau sans perdre les données du journal d'une version précédente. Réutilise z l'existant, `Orchestrator Log Group` choisissez `yes` s'il existe `Orchestrator Log Group` toujours depuis un déploiement antérieur dans ce compte, sinonno. Si vous effectuez une mise à jour de la pile à partir d'une version antérieure à la version 2.3.0, choisissez no
ShouldDeployWebUI	`yes`	Déployez les composants de l'interface utilisateur Web, notamment API Gateway, les fonctions Lambda et CloudFront la distribution. Sélectionnez « Oui » pour activer le tableau de bord Web permettant de consulter les résultats et l'état des mesures correctives.

Paramètre	Par défaut	Description
AdminUserEmail	(Entrée facultative)	Adresse e-mail de l'utilisateur administrateur initial. Cet utilisateur aura un accès administratif complet à l'interface utilisateur Web d'ASR. Obligatoire uniquement lorsque l'interface utilisateur Web est activée.
Utiliser CloudWatch les métriques	`yes`	Spécifiez si vous souhaitez activer CloudWatch les métriques pour surveiller la solution. Cela créera un CloudWatch tableau de bord pour consulter les statistiques.
Utiliser les alarmes CloudWatch métriques	`yes`	Spécifiez si vous souhaitez activer CloudWatch les alarmes métriques pour la solution. Cela créera des alarmes pour certaines métriques collectées par la solution.

Paramètre	Par défaut	Description
RemediationFailure AlarmThreshold	5	Spécifiez le seuil pour le pourcentage d'échecs de correction par ID de contrôle. Par exemple, si vous entrez5, vous recevez une alarme si un ID de contrôle échoue dans plus de 5 % des cas de correction au cours d'une journée donnée. Ce paramètre ne fonctionn e que si des alarmes sont créées (voir le paramètre Utiliser CloudWatch les alarmes métriques).
EnableEnhancedClou dWatchMetrics	no	Siyes, crée des CloudWatc h métriques supplémentaires pour suivre tous les contrôles IDs individuellement sur le CloudWatch tableau de bord et sous forme d' CloudWatch alarmes. Consultez la section Coût pour comprendre les coûts supplémentaires que cela entraîne.

Paramètre	Par défaut	Description
TicketGenFunctionName	(Entrée facultative)	Facultatif. Laissez ce champ vide si vous ne souhaitez pas intégrer de système de billetterie. Sinon, fournissez le nom de la fonction Lambda à partir de la sortie de la pile de l'étape 0, par exemple :. `SO0111-ASR-ServiceNow-TicketGenerator`

> **Note**
>
> Vous devez activer manuellement les corrections automatiques dans le compte administrateur après le déploiement ou la mise à jour des CloudFormation piles de la solution.

1. Sur la page Configurer les options de pile, choisissez Suivant.
2. Sur la page Vérification, vérifiez et confirmez les paramètres. Cochez la case indiquant que le modèle créera des ressources AWS Identity and Access Management (IAM).
3. Sélectionnez Create stack (Créer une pile) pour déployer la pile.

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

Étape 2 : installer les rôles de correction dans chaque compte membre d'AWS Security Hub

Ils ne `automated-security-response-member-roles.template` StackSet doivent être déployés que dans une seule région par compte membre. Il définit les rôles globaux qui autorisent les appels d'API entre comptes à partir de la fonction d'étape ASR Orchestrator.

1. Connectez-vous à l'AWS Management Console pour chaque compte membre d'AWS Security Hub (y compris le compte administrateur, qui est également membre). Sélectionnez le bouton

pour lancer le CloudFormation modèle `automated-security-response-member-roles.template` AWS. Vous pouvez également télécharger le modèle comme point de départ pour votre propre implémentation.

2. Le modèle est lancé par défaut dans la région USA Est (Virginie du Nord). Pour lancer cette solution dans une autre région AWS, utilisez le sélecteur de région dans la barre de navigation de l'AWS Management Console.
3. Sur la page Create stack, vérifiez que l'URL du modèle est correcte dans la zone de texte URL Amazon S3, puis choisissez Next.
4. Sur la page Spécifier les détails de la pile, attribuez un nom à votre pile de solutions. Pour plus d'informations sur les limites relatives aux caractères de dénomination, reportez-vous aux limites IAM et STS dans le guide de l'utilisateur d'AWS Identity and Access Management.
5. Sur la page Paramètres, spécifiez les paramètres suivants et choisissez Next.

Paramètre	Par défaut	Description
Namespace	*<Requires input>*	Entrez une chaîne de 9 caractères alphanumé riques minuscules maximum. Espace de noms unique à ajouter en tant que suffixe aux noms de rôles IAM de correction. Le même espace de noms doit être utilisé dans les rôles des membres et dans les piles de membres. Cette chaîne doit être unique pour chaque déploiement de solution, mais il n'est pas nécessaire de la modifier lors des mises à jour de la pile. Il n'est pas nécessaire que la valeur de l'espace de

Paramètre	Par défaut	Description
		noms soit unique par compte membre.
Administrateur du compte Sec Hub	*<Requires input>*	Entrez l'ID de compte à 12 chiffres du compte administrateur AWS Security Hub. Cette valeur accorde des autorisations au rôle de solution du compte administrateur.

6. Sur la page Configurer les options de pile, choisissez Suivant.
7. Sur la page Vérification, vérifiez et confirmez les paramètres. Cochez la case indiquant que le modèle créera des ressources AWS Identity and Access Management (IAM).
8. Sélectionnez Create stack (Créer une pile) pour déployer la pile.

   Vous pouvez consulter l'état de la pile dans la CloudFormation console AWS dans la colonne Status. Vous devriez recevoir le statut CREATE_COMPLETE dans environ 5 minutes. Vous pouvez passer à l'étape suivante pendant le chargement de cette pile.

Étape 3 : Lancez la pile de membres

> **⚠ Important**
>
> Cette solution inclut la collecte de données. Nous utilisons ces données pour mieux comprendre la façon dont les clients utilisent cette solution et les services et produits associés. AWS est propriétaire des données recueillies dans le cadre de cette enquête. La collecte de données est soumise à la politique de confidentialité d'AWS.

La `automated-security-response-member` pile doit être installée sur chaque compte membre du Security Hub. Cette pile définit les runbooks pour la correction automatique. L'administrateur de chaque compte membre peut contrôler les mesures correctives disponibles via cette pile.

1. Connectez-vous à l'AWS Management Console pour chaque compte membre d'AWS Security Hub (y compris le compte administrateur, qui est également membre). Sélectionnez le bouton pour lancer le CloudFormation modèle `automated-security-response-member.template` AWS.

Vous pouvez également télécharger le modèle comme point de départ pour votre propre implémentation. Le modèle est lancé par défaut dans la région USA Est (Virginie du Nord). Pour lancer cette solution dans une autre région AWS, utilisez le sélecteur de région dans la barre de navigation de l'AWS Management Console.

+

> **Note**
>
> Cette solution utilise AWS Systems Manager, qui est actuellement disponible dans la majorité des régions AWS. La solution fonctionne dans toutes les régions qui prennent en charge ces services. Pour connaître la disponibilité la plus récente par région, consultez la liste des services régionaux AWS.

1. Sur la page Create stack, vérifiez que l'URL du modèle est correcte dans la zone de texte URL Amazon S3, puis choisissez Next.
2. Sur la page Spécifier les détails de la pile, attribuez un nom à votre pile de solutions. Pour plus d'informations sur les limites relatives aux caractères de dénomination, reportez-vous aux limites IAM et STS dans le guide de l'utilisateur d'AWS Identity and Access Management.
3. Sur la page Paramètres, spécifiez les paramètres suivants et choisissez Next.

Paramètre	Par défaut	Description
Indiquez le nom du LogGroup à utiliser pour créer des filtres métriques et des alarmes	*<Requires input>*	Spécifiez le nom d'un groupe CloudWatch Logs dans lequel sont CloudTrail enregistrés les appels d'API. Ceci est

Paramètre	Par défaut	Description
		utilisé pour les corrections CIS 3.1-3.14.
Load SC Member Stack	`yes`	Spécifiez s'il faut installer les composants membres pour la correction automatique des contrôles SC.
Charger la pile de membres de l'AFSBP	no	Spécifiez s'il faut installer les composants membres pour la correction automatique des contrôles FSBP.
Charger la pile de CIS120 membres	no	Spécifiez s'il faut installer les composants membres pour la correction automatique des CIS120 contrôles.
Charger la pile de CIS140 membres	no	Spécifiez s'il faut installer les composants membres pour la correction automatique des CIS140 contrôles.
Charger la pile de CIS300 membres	no	Spécifiez s'il faut installer les composants membres pour la correction automatique des CIS300 contrôles.
Charger la pile de PC1321 membres	no	Spécifiez s'il faut installer les composants membres pour la correction automatique des PC1321 contrôles.
Charger la pile de membres du NIST	no	Spécifiez s'il faut installer les composants membres pour la correction automatique des contrôles NIST.

Paramètre	Par défaut	Description
Création d'un compartiment S3 pour la journalisation des audits Redshift	no	Indiquez `yes` si le compartiment S3 doit être créé pour la correction FSBP RedShift .4. Pour plus de détails sur le compartiment S3 et la correction, consultez la correction Redshift.4 dans le guide de l'utilisateur d'AWS Security Hub.
Compte administrateur Sec Hub	*<Requires input>*	Entrez l'ID de compte à 12 chiffres du compte administrateur AWS Security Hub.
Namespace	*<Requires input>*	Entrez une chaîne de 9 caractères alphanumériques minuscules maximum. Cette chaîne fait partie des noms de rôles IAM et du compartiment Action Log S3. Utilisez la même valeur pour le déploiement de la pile de membres et le déploiement de la pile de rôles des membres. La chaîne doit être unique pour chaque déploiement de solution, mais il n'est pas nécessaire de la modifier lors des mises à jour de la pile.

Paramètre	Par défaut	Description
EnableCloudTrailForASRActionJournal	no	Indiquez `yes` si vous souhaitez surveiller les événements de gestion menés par la solution sur le CloudWatch tableau de bord. La solution crée une CloudTrail trace dans chaque compte membre que vous sélectionnez`yes`. Vous devez déployer la solution dans une organisation AWS pour activer cette fonctionnalité. En outre, vous ne pouvez activer cette fonctionnalité que dans une seule région au sein du même compte. Consultez la section Coût pour comprendre les coûts supplémentaires que cela entraîne.

4. Sur la page Configurer les options de pile, choisissez Suivant.
5. Sur la page Vérification, vérifiez et confirmez les paramètres. Cochez la case indiquant que le modèle créera des ressources AWS Identity and Access Management (IAM).
6. Sélectionnez Create stack (Créer une pile) pour déployer la pile.

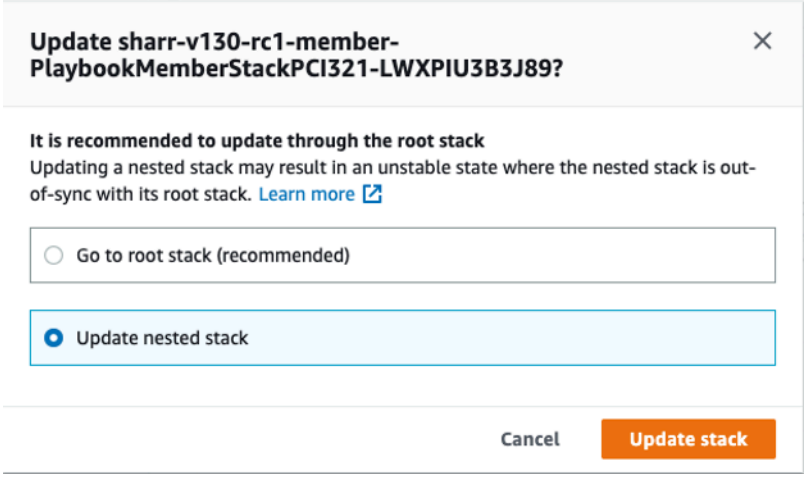
Vous pouvez consulter l'état de la pile dans la CloudFormation console AWS dans la colonne Status. Vous devriez recevoir le statut CREATE_COMPLETE dans 15 minutes environ.

Étape 4 : (Facultatif) Ajustez les mesures correctives disponibles

Si vous souhaitez supprimer des corrections spécifiques d'un compte membre, vous pouvez le faire en mettant à jour la pile imbriquée pour la norme de sécurité. Pour des raisons de simplicité, les options de pile imbriquée ne sont pas propagées à la pile racine.

1. Connectez-vous à la CloudFormation console AWS et sélectionnez la pile imbriquée.
2. Choisissez Mettre à jour.
3. Sélectionnez Mettre à jour la pile imbriquée, puis Mettre à jour la pile.

   Mettre à jour la pile imbriquée



4. Sélectionnez Utiliser le modèle actuel, puis Suivant.
5. Ajustez les mesures correctives disponibles. Modifiez les valeurs des commandes souhaitées par `Available` et des commandes indésirables par. `Not available`

> **Note**
>
> La désactivation d'une correction supprime le manuel de correction des solutions pour la norme et le contrôle de sécurité.

6. Sur la page Configurer les options de pile, choisissez Suivant.
7. Sur la page Vérification, vérifiez et confirmez les paramètres. Cochez la case indiquant que le modèle créera des ressources AWS Identity and Access Management (IAM).
8. Choisissez Mettre à jour la pile.

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

Déploiement de la Control Tower (CT)

Le guide Customizations for AWS Control Tower (CfCT) s'adresse aux administrateurs, aux DevOps professionnels, aux fournisseurs 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.

Temps de déploiement : environ 30 minutes

Conditions préalables

Avant de déployer cette solution, assurez-vous qu'elle est destinée aux administrateurs d'AWS Control Tower.

Lorsque vous êtes prêt à configurer votre zone de landing zone à l'aide de la console AWS Control Tower APIs, ou suivez ces étapes :

Pour commencer à utiliser AWS Control Tower, consultez : Getting Started with AWS Control Tower

Pour savoir comment personnaliser votre zone d'atterrissage, reportez-vous à : Personnalisation de votre zone d'atterrissage

Pour lancer et déployer votre zone d'atterrissage, voir : Guide de déploiement de la zone d'atterrissage

Vue d'ensemble du déploiement

Suivez les étapes ci-dessous pour déployer cette solution sur AWS.

Étape 1 : créer et déployer un compartiment S3

> **Note**
>
> Configuration du compartiment S3 — pour ADMIN uniquement. Il s'agit d'une étape de configuration unique qui ne doit pas être répétée par les utilisateurs finaux. Les compartiments S3 stockent le package de déploiement, y compris le CloudFormation modèle AWS et le code Lambda requis pour l'exécution d'ASR. Ces ressources sont déployées à l'aide de CfCt ou StackSet.

1. Configuration du compartiment S3

Configurez le compartiment S3 qui sera utilisé pour stocker et distribuer vos packages de déploiement.

2. Configuration de l'environnement

Préparez les variables d'environnement, les informations d'identification et les outils nécessaires au processus de création et de déploiement.

3. Configuration des politiques relatives aux compartiments S3

Définissez et appliquez les politiques de compartiment appropriées pour contrôler l'accès et les autorisations.

4. Préparez le build

Compilez, empaquetez ou préparez de toute autre manière votre application ou vos actifs pour le déploiement.

5. Déployer des packages sur S3

Téléchargez les artefacts de construction préparés dans le compartiment S3 désigné.

Étape 2 : déploiement de Stacks sur AWS Control Tower

1. Créer un manifeste de compilation pour les composants ASR

Définissez un manifeste de compilation répertoriant tous les composants ASR, leurs versions, leurs dépendances et leurs instructions de génération.

2. Mettez à jour le CodePipeline

Modifiez la CodePipeline configuration AWS pour inclure les nouvelles étapes de construction, les nouveaux artefacts ou les nouvelles étapes nécessaires au déploiement des composants ASR.

Étape 1 : Création et déploiement dans le compartiment S3

Les solutions AWS utilisent deux compartiments : un compartiment pour l'accès global aux modèles, accessible via HTTPS, et des compartiments régionaux pour accéder aux ressources de la région, comme le code Lambda.

1. Configuration du compartiment S3

Choisissez un nom de compartiment unique, par exemple asr-staging. Définissez deux variables d'environnement sur votre terminal, l'une doit être le nom du bucket de base avec -reference comme suffixe, l'autre avec la région de déploiement prévue comme suffixe :

```
export BASE_BUCKET_NAME=asr-staging-$(date +%s)
export TEMPLATE_BUCKET_NAME=$BASE_BUCKET_NAME-reference
export REGION=us-east-1
export ASSET_BUCKET_NAME=$BASE_BUCKET_NAME-$REGION
```

2. Configuration de l'environnement

Dans votre compte AWS, créez deux compartiments portant ces noms, par exemple asr-staging-reference et asr-staging-us-east -1. (Le compartiment de référence contiendra les CloudFormation modèles, le compartiment régional contiendra tous les autres actifs, comme le bundle de code Lambda.) Vos buckets doivent être chiffrés et interdire l'accès public

```
aws s3 mb s3://$TEMPLATE_BUCKET_NAME/
aws s3 mb s3://$ASSET_BUCKET_NAME/
```

> **Note**
>
> Lorsque vous créez vos buckets, assurez-vous qu'ils ne sont pas accessibles au public. Utilisez des noms de compartiments aléatoires. Désactivez l'accès public. Utilisez le chiffrement KMS. Et vérifiez la propriété du bucket avant de le télécharger.

3. Configuration de la politique des buckets S3

Mettez à jour la politique du compartiment S3 $TEMPLATE_BUCKET_NAME afin d'inclure des autorisations pour l'ID de compte d'exécution PutObject . Attribuez cette autorisation à un rôle IAM au sein du compte d'exécution autorisé à écrire dans le compartiment. Cette configuration vous permet d'éviter de créer le bucket dans le compte de gestion.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
```

```
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::template-bucket-name/*",
                "arn:aws:s3:::template-bucket-name"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "org-id"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::template-bucket-name/*",
                "arn:aws:s3:::template-bucket-name"
            ],
            "Condition": {
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::account-id:role/iam-role-name"
                }
            }
        }
    ]
}
```

Modifiez la politique du compartiment S3 de l'actif pour inclure les autorisations. Attribuez cette autorisation à un rôle IAM au sein du compte d'exécution autorisé à écrire dans le compartiment. Répétez cette configuration pour chaque compartiment d'actifs régional (par exemple, asr-staging-us-east -1, asr-staging-eu-west -1, etc.), en autorisant les déploiements dans plusieurs régions sans avoir à créer les compartiments dans le compte de gestion.

4. Préparation de la construction

- Prérequis :
  - AWS CLI v2
  - Python 3.11+ avec pip
  - AWS CDK 2.171.1+
  - Node.js 20+ avec npm

  - Poetry v2 avec plugin pour exporter
- Clonage de Git https://github.com/aws-solutions/automated-security-response-on-aws.git

Assurez-vous d'abord d'avoir exécuté npm install dans le dossier source.

Ensuite, depuis le dossier de déploiement de votre dépôt cloné, exécutez build-s3-dist.sh en transmettant le nom racine de votre bucket (par exemple mybucket) et la version que vous créez (par exemple v1.0.0). Nous vous recommandons d'utiliser une version semver basée sur la version téléchargée depuis GitHub (ex. GitHub: v1.0.0, votre build : v1.0.0.mybuild)

```
chmod +x build-s3-dist.sh
export SOLUTION_NAME=automated-security-response-on-aws
export SOLUTION_VERSION=v1.0.0.mybuild
./build-s3-dist.sh -b $BASE_BUCKET_NAME -v $SOLUTION_VERSION
```

5. Déployer des packages sur S3

```
cd deployment
aws s3 cp global-s3-assets/  s3://$TEMPLATE_BUCKET_NAME/$SOLUTION_NAME/
$SOLUTION_VERSION/ --recursive --acl bucket-owner-full-control
aws s3 cp regional-s3-assets/  s3://$ASSET_BUCKET_NAME/$SOLUTION_NAME/
$SOLUTION_VERSION/ --recursive --acl bucket-owner-full-control
```

Étape 2 : déploiement de Stacks sur AWS Control Tower

1. Générer un manifeste pour les composants ASR

Après avoir déployé des artefacts ASR dans les compartiments S3, mettez à jour le manifeste du pipeline Control Tower pour faire référence à la nouvelle version, puis déclenchez l'exécution du pipeline. Reportez-vous à : déploiement de la tour de contrôle

> **Important**
>
> Pour garantir le déploiement correct de la solution ASR, consultez la documentation officielle d'AWS pour obtenir des informations détaillées sur la présentation des CloudFormation modèles et la description des paramètres. Liens d'information ci-dessous : Guide de présentation des paramètres des CloudFormation modèles

Le manifeste des composants ASR se présente comme suit :

```
region: us-east-1 #<HOME_REGION_NAME>
version: 2021-03-15

# Control Tower Custom CloudFormation Resources
resources:
  - name: <ADMIN STACK NAME>
    resource_file: s3://<ADMIN TEMPLATE BUCKET path>
    parameters:
      - parameter_key: UseCloudWatchMetricsAlarms
        parameter_value: "yes"
      - parameter_key: TicketGenFunctionName
        parameter_value: ""
      - parameter_key: ShouldDeployWebUI
        parameter_value: "yes"
      - parameter_key: AdminUserEmail
        parameter_value: "<YOUR EMAIL ADDRESS>"
      - parameter_key: LoadSCAdminStack
        parameter_value: "yes"
      - parameter_key: LoadCIS120AdminStack
        parameter_value: "no"
      - parameter_key: LoadCIS300AdminStack
        parameter_value: "no"
      - parameter_key: UseCloudWatchMetrics
        parameter_value: "yes"
      - parameter_key: LoadNIST80053AdminStack
        parameter_value: "no"
      - parameter_key: LoadCIS140AdminStack
        parameter_value: "no"
      - parameter_key: ReuseOrchestratorLogGroup
        parameter_value: "yes"
      - parameter_key: LoadPCI321AdminStack
        parameter_value: "no"
      - parameter_key: RemediationFailureAlarmThreshold
        parameter_value: "5"
      - parameter_key: LoadAFSBPAdminStack
        parameter_value: "no"
      - parameter_key: EnableEnhancedCloudWatchMetrics
        parameter_value: "no"
    deploy_method: stack_set
    deployment_targets:
     accounts: # :type: list
        - <ACCOUNT_NAME> # and/or
```

```
      - <ACCOUNT_NUMBER>
    regions:
      - <REGION_NAME>

  - name:  <ROLE MEMBER STACK NAME>
    resource_file: s3://<ROLE MEMBER TEMPLATE BUCKET path>
    parameters:
      - parameter_key: SecHubAdminAccount
        parameter_value: <ADMIN_ACCOUNT_NAME>
      - parameter_key: Namespace
        parameter_value: <NAMESPACE>
    deploy_method: stack_set
    deployment_targets:
      organizational_units:
        - <ORG UNIT>

  - name:  <MEMBER STACK NAME>
    resource_file: s3://<MEMBER TEMPLATE BUCKET path>
    parameters:
      - parameter_key: SecHubAdminAccount
        parameter_value: <ADMIN_ACCOUNT_NAME>
      - parameter_key: LoadCIS120MemberStack
        parameter_value: "no"
      - parameter_key: LoadNIST80053MemberStack
        parameter_value: "no"
      - parameter_key: Namespace
        parameter_value: <NAMESPACE>
      - parameter_key: CreateS3BucketForRedshiftAuditLogging
        parameter_value: "no"
      - parameter_key: LoadAFSBPMemberStack
        parameter_value: "no"
      - parameter_key: LoadSCMemberStack
        parameter_value: "yes"
      - parameter_key: LoadPCI321MemberStack
        parameter_value: "no"
      - parameter_key: LoadCIS140MemberStack
        parameter_value: "no"
      - parameter_key: EnableCloudTrailForASRActionLog
        parameter_value: "no"
      - parameter_key: LogGroupName
        parameter_value: <LOG_GROUP_NAME>
      - parameter_key: LoadCIS300MemberStack
        parameter_value: "no"
    deploy_method: stack_set
```

```
    deployment_targets:
     accounts: # :type: list
        - <ACCOUNT_NAME> # and/or
        - <ACCOUNT_NUMBER>
    organizational_units:
      - <ORG UNIT>
    regions: # :type: list
      - <REGION_NAME>
```

2. Mise à jour du pipeline de code

Ajoutez un fichier manifeste à un fichier custom-control-tower-configuration .zip et exécutez un CodePipeline, voir : présentation du pipeline de code

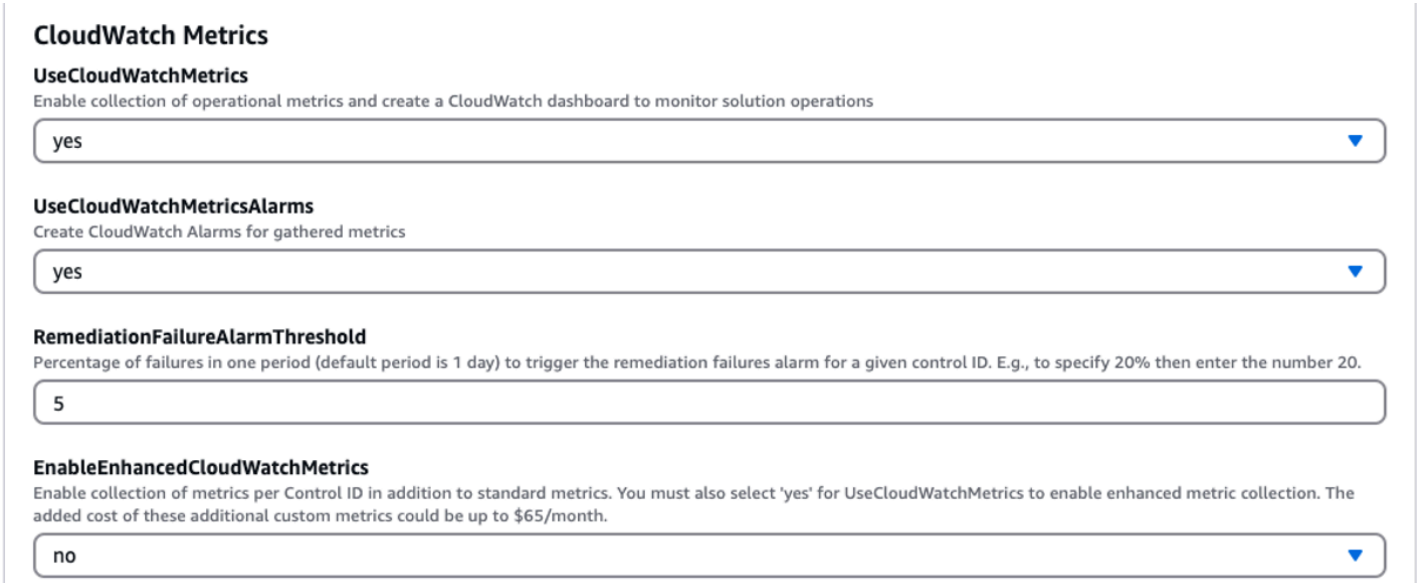
Surveillez les opérations de la solution à l'aide d'un CloudWatch tableau de bord Amazon

Cette solution inclut des métriques personnalisées et des alarmes affichées sur un CloudWatch tableau de bord Amazon.

Le CloudWatch tableau de bord et les alarmes surveillent le fonctionnement de la solution et alertent en cas de problème potentiel.

Activation CloudWatch des métriques, des alarmes et du tableau de bord

Il existe quatre paramètres CloudFormation de modèle pour les CloudWatch fonctionnalités.



1. UseCloudWatchMetrics- Le paramétrage de cette option `yes` permet de collecter des métriques opérationnelles et crée un CloudWatch tableau de bord pour visualiser ces métriques.
2. UseCloudWatchAlarms- Réglez ce paramètre pour `yes` activer les alarmes par défaut de la solution.
3. RemediationFailureAlarmThreshold- Le pourcentage de mesures correctives défaillantes au cours d'une période pendant laquelle une alarme a été déclenchée.
4. EnableEnhancedCloudWatchMetrics- Définissez ce paramètre sur `yes` pour collecter des métriques individuelles par ID de contrôle. Par défaut, ce paramètre est défini surno, de sorte que

seules les mesures relatives au nombre total de mesures correctives pour l'ensemble du contrôle IDs sont collectées. Les mesures et alarmes individuelles par ID de contrôle entraînent un coût supplémentaire.

Utilisation du CloudWatch tableau de bord

Pour consulter le tableau de bord :

1. Accédez à Amazon, CloudWatch puis à Dashboards.
2. Sélectionnez le tableau de bord nommé « ASR-Remediation-Metrics-Dashboard ».

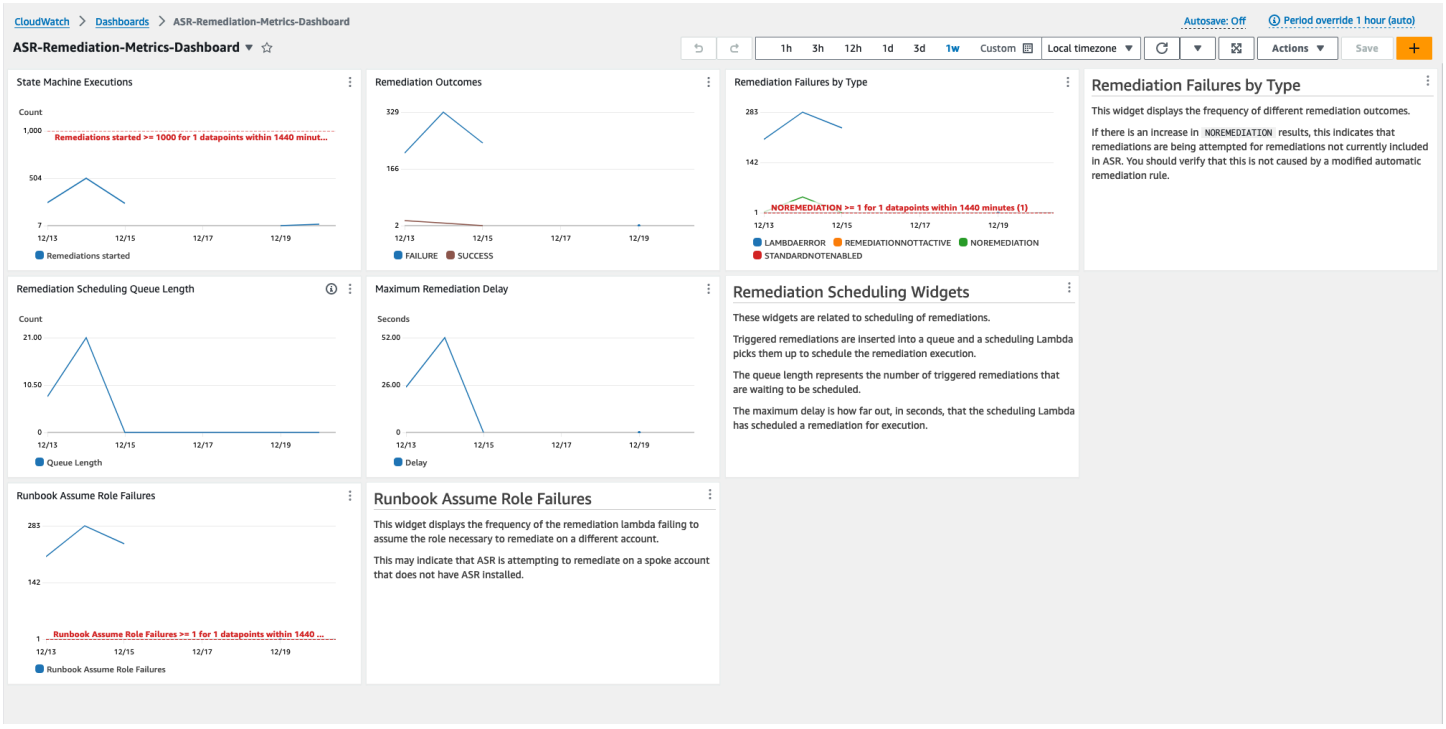
Le CloudWatch tableau de bord contient les sections suivantes :

1. Nombre total de corrections réussies : vous donne un aperçu du nombre de conclusions du Security Hub qui ont été corrigées avec succès par la solution.
2. Défaillances de correction : indique le nombre de mesures correctives qui ont échoué, au total et en pourcentage, ainsi que la cause de l'échec. Un nombre élevé de défaillances peut indiquer un problème technique lié à la solution que vous devrez peut-être étudier plus en détail.
3. Succès ou échec de la correction par ID de contrôle : si vous avez activé les métriques améliorées au moment du déploiement, cette section répertorie les résultats de la correction par ID de contrôle. Lorsque la section Défaillances de correction indique un taux d'échec élevé en général, cette section vous indique si les défaillances sont réparties entre de nombreux contrôles IDs ou si seuls certains contrôles IDs échouent.
4. Runbook Assume Role Failures : indique le nombre d'échecs survenus à la suite de tentatives de correction sur des comptes sur lesquels le rôle de membre de la solution n'est pas installé. Les échecs répétés dus à des tentatives de correction automatisées en raison de rôles manquants entraînent des coûts inutiles. Atténuez ce problème en installant la pile de rôles de membre dans les comptes concernés, en désactivant toutes les EventBridge règles créées par la solution ou en dissociant le compte dans Security Hub.
5. Actions de gestion des traces dans le cloud par ASR : répertorie les actions de gestion effectuées par la solution sur tous les comptes membres pour lesquels vous avez activé les journaux d'actions avec le paramètre EnableCloudTrailForASRActionLog au moment du déploiement. Lorsque vous observez des modifications inattendues des ressources dans l'un de vos comptes AWS, ce widget peut vous aider à comprendre si les ressources ont été modifiées par la solution.

Le CloudWatch tableau de bord est également doté d'alarmes prédéfinies qui signalent les erreurs opérationnelles courantes.

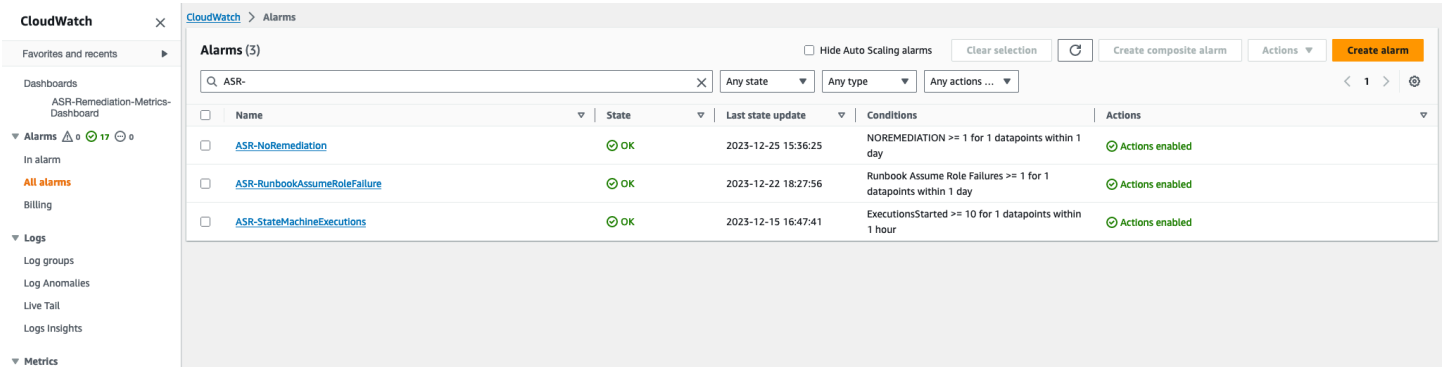
1. Exécutions par State Machine > 1 000 sur une période de 24 heures.
   a. Une forte augmentation du nombre d'exécutions de mesures correctives peut indiquer qu'une règle événementielle est déclenchée plus souvent que prévu.
   b. Le seuil peut être modifié à l'aide du CloudFormation paramètre.
2. Défaillances de correction par type = NOREMEDIATION > 0
   a. Des mesures correctives sont en cours de tentative pour les mesures correctives qui ne sont pas incluses dans l'ASR. Cela peut indiquer qu'une règle d'événement a été modifiée pour inclure plus que les corrections prévues.
3. Défaillances du rôle Runbook Assume > 0
   a. Des mesures correctives sont en cours de tentative sur des comptes ou des régions où la solution n'est pas correctement déployée. Cela peut indiquer qu'une règle d'événement a été modifiée pour inclure plus de comptes que prévu.

Tous les seuils d'alarme peuvent être modifiés en fonction des besoins de déploiement individuels.

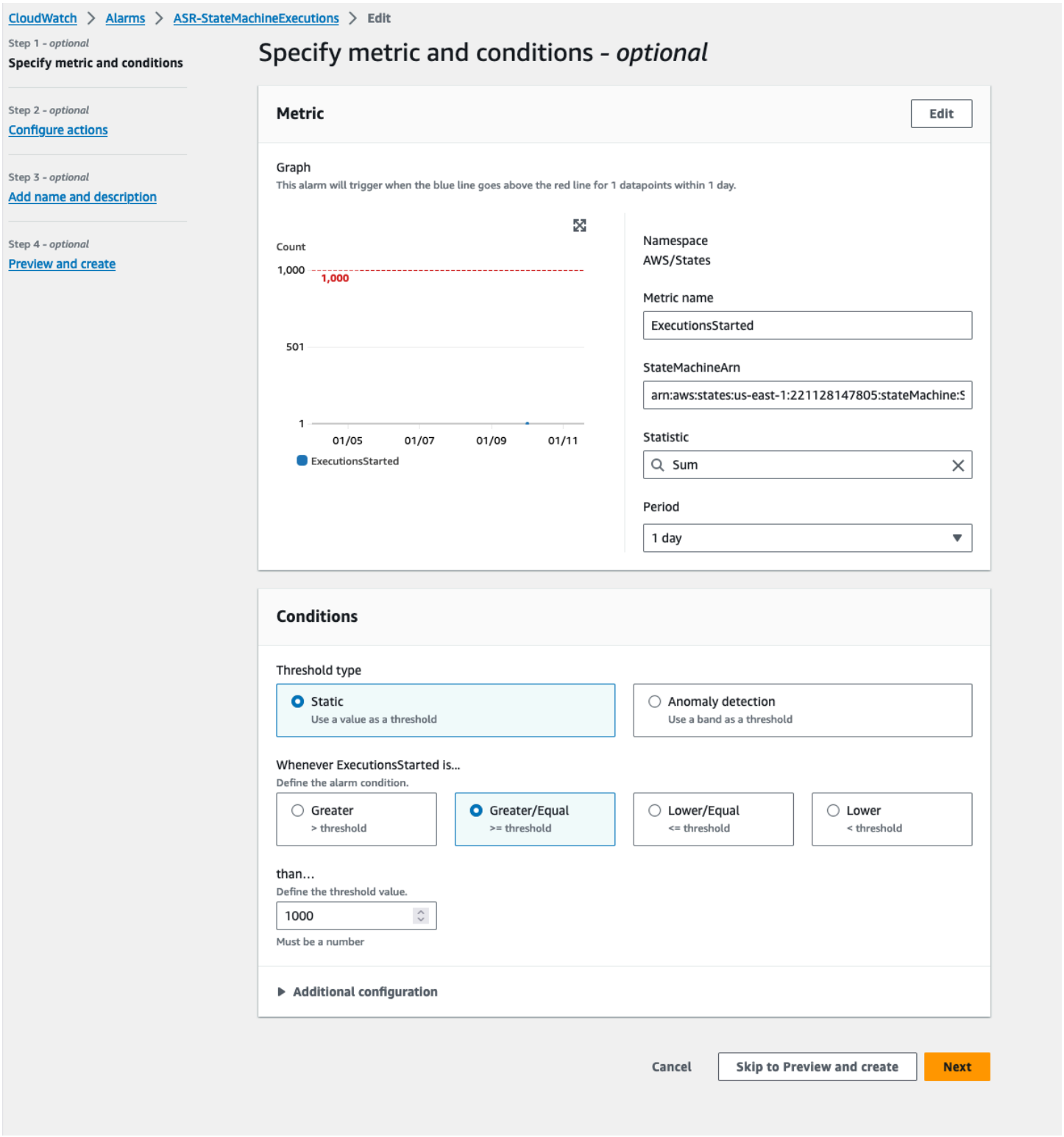


Modification des seuils d'alarme

1. Accédez à Amazon CloudWatch → Alarmes → Toutes les alarmes.
2. Choisissez l'alarme que vous souhaitez modifier, puis sélectionnez Actions → Modifier.



1. Modifiez le seuil à la valeur souhaitée et enregistrez.



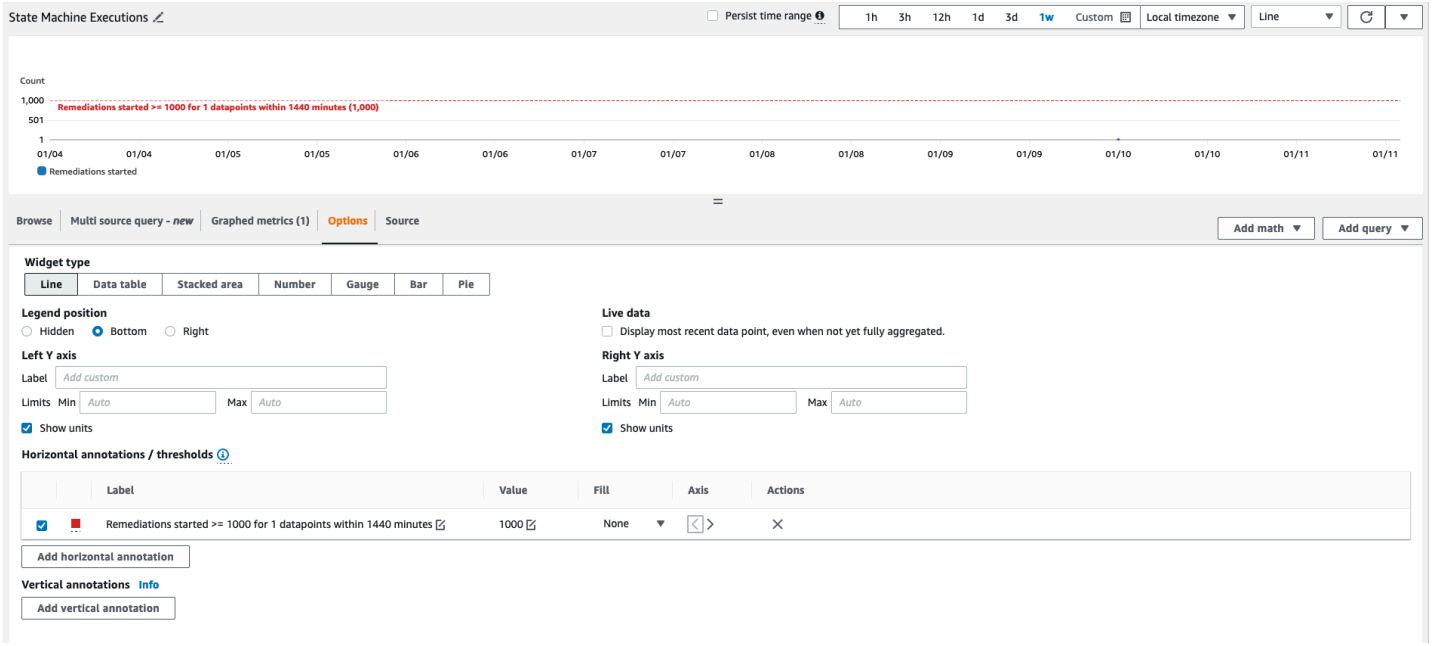
1. Accédez au CloudWatch tableau de bord pour modifier les graphiques qui s'y trouvent afin qu'ils correspondent aux nouveaux paramètres.

   a. Sélectionnez les points de suspension en haut à droite du widget correspondant.

b. Tâche de sélection Modifier.

c. Accédez à l'onglet Options.

d. Modifiez l'annotation d'alarme pour qu'elle corresponde aux nouveaux paramètres.



Abonnement aux notifications d'alarme

Dans le compte administrateur, abonnez-vous à la rubrique Amazon SNS créée par la pile d'administrateurs, SO0111-ASR_Alarm_Topic. Cela vous avertira lorsqu'une alarme passe à l'état ALARM.

Mettre à jour la solution

Important

- Lors de la mise à jour de la solution, il peut être nécessaire de réactiver manuellement les règles de correction automatisées dans le compte administrateur. Reportez-vous à la section Activer les corrections entièrement automatisées.
- Si vous utilisez le `Reuse Orchestrator Log Group` paramètre pour conserver les journaux, assurez-vous qu'il est correctement défini lors de la mise à jour de la pile afin d'éviter la recréation de groupes de journaux ou la perte des paramètres de conservation des journaux. Reportez-vous à la section Déployer la solution. Si vous effectuez une mise à jour de la pile vers la version 2.3.0+ à partir d'une version antérieure, choisissez « non »

Mise à niveau à partir de versions antérieures à la v1.4

Si vous avez déjà déployé la solution avant la version v1.4.x, désinstallez-la, puis installez la dernière version :

1. Désinstallez la solution précédemment déployée. Reportez-vous à la section Désinstaller la solution.
2. Lancez le dernier modèle. Reportez-vous à la section Déployer la solution.

Note

Si vous effectuez une mise à niveau de la version v1.2.1 ou antérieure vers la version v1.3.0 ou ultérieure, définissez Use existing Orchestrator Log Group sur. No Si vous réinstallez la version v1.3.0 ou une version ultérieure, vous pouvez sélectionner `Yes` cette option. Cette option vous permet de continuer à vous connecter au même groupe de journaux pour Orchestrator Step Functions.

Mise à niveau depuis la version 1.4 et les versions ultérieures

Si vous effectuez une mise à niveau depuis la version v1.4.x, mettez à jour toutes les piles ou StackSets procédez comme suit :

1. Mettez à jour la pile du compte administrateur du Security Hub à l'aide du dernier modèle.
2. Dans chaque compte membre, mettez à jour les autorisations à partir du dernier modèle.
3. Dans chaque compte membre, dans toutes les régions où il est actuellement déployé, mettez à jour la pile de membres à partir du dernier modèle.
4. Si l'interface utilisateur Web est activée et que vous avez mis à jour des paramètres tels que `TicketGenFunctionName` l'invalidation du CloudFront cache pour refléter immédiatement les modifications :

```
aws cloudfront create-invalidation \
  --distribution-id <distribution-id> \
  --paths "/aws-exports.json"
```

Mise à niveau depuis la version 2.0.x

Si vous effectuez une mise à niveau depuis la version 2.0.x, passez à la version 2.1.2 ou ultérieure. La mise à jour vers v2.1.0 - v2.1.1 échouera. CloudFormation

Mise à niveau depuis la version 2.1.4 ou antérieure

Si vous effectuez une mise à niveau depuis la version 2.1.4 ou une version antérieure, vous devez effectuer la mise à niveau vers la version 2.3.0 avant de passer à une version supérieure à la version 2.3.0. Dans le cas contraire, l'opération de mise à jour de la pile échouera. Vous pouvez également supprimer et redéployer les piles de la solution plutôt que d'effectuer une mise à jour des piles.

Résolution des problèmes

La résolution des problèmes connus fournit des instructions pour atténuer les erreurs connues. Si ces instructions ne répondent pas à votre problème, contactez le support AWS fournit des instructions pour ouvrir un dossier de support AWS pour cette solution.

Journaux de solutions

Cette section contient des informations de résolution des problèmes pour cette solution, voir la navigation de gauche pour les rubriques.

Cette solution collecte les résultats des runbooks de correction, qui s'exécutent sous AWS Systems Manager, et enregistre le résultat `S00111-ASR` dans le groupe CloudWatch Logs du compte administrateur AWS Security Hub. Il y a un flux par contrôle et par jour.

The Orchestrator Step Functions enregistre toutes les transitions par étapes dans le groupe `S00111-ASR-Orchestrator` CloudWatch Logs du compte administrateur AWS Security Hub. Ce journal est une piste d'audit permettant d'enregistrer les transitions d'état pour chaque instance des Step Functions. Il existe un flux de log par exécution de Step Functions.

Les deux groupes de journaux sont chiffrés à l'aide d'une clé AWS KMS Customer-Manager (CMK).

Les informations de dépannage suivantes utilisent le groupe de `S00111-ASR` journaux. Utilisez ce journal, ainsi que la console AWS Systems Manager Automation, les journaux Automation Executions, la console Step Function et les journaux Lambda pour résoudre les problèmes.

Si une correction échoue, un message similaire au suivant sera enregistré `S00111-ASR` dans le flux de journal pour la norme, le contrôle et la date. Par exemple : CIS-2.9-2021-08-12

```
ERROR: a4cbb9bb-24cc-492b-a30f-1123b407a6253: Remediation failed for CIS control
 2.9 in account 123412341234: See Automation Execution output for details (AwsEc2Vpc
 vpc-0e92bbe911cf08acb)
```

Les messages suivants fournissent des informations supplémentaires. Cette sortie provient du runbook ASR pour la norme et le contrôle de sécurité. Par exemple : ASR-CIS_1.2.0_2.9

```
Step fails when it is Execution complete: verified. Failed to run automation with
 executionId: eecdef79-9111-4532-921a-e098549f5259 Failed :
```

```
{Status=[Failed], Output=[No output available yet because the step is not successfully
 executed], ExecutionId=[eecdef79-9111-4532-921a-e098549f5259]}. Please refer to
 Automation Service Troubleshooting Guide for more diagnosis details.
```

Ces informations vous indiquent l'échec, qui dans ce cas était dû à une automatisation secondaire exécutée sur le compte du membre. Pour résoudre ce problème, vous devez vous connecter à l'AWS Management Console depuis le compte membre (à partir du message ci-dessus), accéder à AWS Systems Manager, accéder à Automation et examiner le résultat du journal pour l'ID `eecdef79-9111-4532-921a-e098549f525` d'exécution.

Résolution des problèmes connus

- Problème : Le déploiement de la solution échoue avec un message d'erreur indiquant que les ressources sont déjà disponibles sur Amazon CloudWatch.

  Solution : recherchez un message d'erreur dans la section CloudFormation ressources/ événements indiquant que des groupes de journaux existent déjà. Les modèles de déploiement ASR permettent de réutiliser les groupes de journaux existants. Vérifiez que vous avez sélectionné Réutiliser.

- Problème : la solution ne parvient pas à être déployée avec une erreur dans une pile imbriquée de playbooks où une EventBridge règle ne parvient pas à être créée

  Résolution : vous avez probablement atteint le quota de EventBridge règles compte tenu du nombre de playbooks déployés. Vous pouvez éviter cela en utilisant les résultats de contrôle consolidés dans Security Hub associés au playbook SC de cette solution, en déployant uniquement les playbooks correspondant aux normes utilisées ou en demandant une augmentation du quota de EventBridge règles.

- Problème : J'utilise Security Hub dans plusieurs régions avec le même compte. Je souhaite déployer cette solution dans plusieurs régions.

  Solution : déployez la pile d'administrateurs dans le même compte et dans la même région que votre administrateur Security Hub. Installez le modèle de membre dans chaque compte et région dans lesquels un membre du Security Hub est configuré. Activez l'agrégation dans le Security Hub.

- Problème : Immédiatement après le déploiement, le SO0111-ASR-Orchestrator échoue dans l'état du document Get Automation avec une erreur 502 : « `Lambda n'a pas pu déchiffrer les variables d'environnement car l'accès KMS a été refusé. Vérifiez les paramètres des touches KMS de la fonction. Exception UnrecognizedClientException KMS : message KMS : le jeton de sécurité inclus

dans la demande n'est pas valide. (Service : AWSLambda ; Code d'état : 502 ; Code d'erreur : KMSAccess DeniedException ; ID de demande :... `»

Résolution : attendez environ 10 minutes pour que la solution se stabilise avant d'exécuter les corrections. Si le problème persiste, ouvrez un ticket d'assistance ou un GitHub problème.

- Problème : J'ai essayé de corriger une constatation, mais rien ne s'est passé.

  Résolution : Consultez les notes relatives à la constatation pour connaître les raisons pour lesquelles elle n'a pas été corrigée. L'une des causes les plus fréquentes est qu'aucune correction automatique n'est apportée au résultat. À l'heure actuelle, il n'existe aucun moyen de fournir un feedback direct à l'utilisateur lorsqu'il n'existe aucune correction autre que par le biais des notes. Consultez les journaux des solutions. Ouvrez CloudWatch Logs dans la console. Trouvez le groupe de CloudWatch journaux SO0111 -ASR. Triez la liste de manière à ce que les derniers streams mis à jour apparaissent en premier. Sélectionnez le flux de journal correspondant à la recherche que vous avez tenté d'exécuter. Vous devriez y trouver des erreurs. L'échec peut s'expliquer notamment par une inadéquation entre le contrôle des résultats et le contrôle des mesures correctives, par la correction entre comptes (non encore prise en charge) ou par le fait que le résultat a déjà été corrigé. Si vous ne parvenez pas à déterminer la raison de l'échec, collectez les journaux et ouvrez un ticket d'assistance.
- Problème : Après le lancement d'une correction, l'état de la console Security Hub n'est pas mis à jour.

  Résolution : La console Security Hub ne se met pas à jour automatiquement. Rafraîchissez la vue actuelle. L'état de la découverte doit être mis à jour. Plusieurs heures peuvent être nécessaires pour que le résultat passe du statut d'échec à celui de réussite. Les résultats sont créés à partir des données d'événements envoyées par d'autres services, tels qu'AWS Config, à AWS Security Hub. Le délai avant la réévaluation d'une règle dépend du service sous-jacent. Si cela ne résout pas le problème, reportez-vous à la résolution précédente car « J'ai essayé de corriger une constatation mais rien ne s'est passé. `»
- Problème : La fonction d'étape de l'orchestrateur échoue dans Get Automation Document State : une erreur s'est produite (AccessDenied) lors de l'appel de l' AssumeRole opération.

  Résolution : Le modèle de membre n'a pas été installé dans le compte membre sur lequel ASR tente de remédier à une constatation. Suivez les instructions de déploiement du modèle de membre.
- Problème : le runbook Config.1 échoue car l'enregistreur ou le canal de diffusion existent déjà.

Résolution : inspectez soigneusement vos paramètres AWS Config pour vous assurer que Config est correctement configuré. La correction automatique ne permet pas de corriger les paramètres AWS Config existants dans certains cas.

- Problème : la correction a réussi mais renvoie le message `"No output available yet because the step is not successfully executed."`

  Résolution : il s'agit d'un problème connu dans cette version, à savoir que certains runbooks de correction ne renvoient pas de réponse. Les runbooks de correction échoueront correctement et signaleront la solution s'ils ne fonctionnent pas.

- Problème : La résolution a échoué et a envoyé une trace de pile.

  Solution : Nous manquons parfois l'occasion de gérer une condition d'erreur qui entraîne un suivi de la pile plutôt qu'un message d'erreur. Essayez de résoudre le problème à partir des données de suivi. Ouvrez un ticket d'assistance si vous avez besoin d'aide.

- Problème : la suppression de la pile v1.3.0 a échoué sur la ressource Custom Action.

  Résolution : La suppression du modèle d'administration peut échouer lors de la suppression de l'action personnalisée. Il s'agit d'un problème connu qui sera résolu dans la prochaine version. Si cela se produit :

  a. Connectez-vous à la console de gestion AWS Security Hub.

  b. Dans le compte administrateur, allez dans Réglages.

  c. Sélectionnez l'onglet Actions personnalisées

  d. Supprimez manuellement l'entrée Remediate with ASR.

  e. Supprimez à nouveau la pile.

- Problème : Après le redéploiement de la pile d'administration, la fonction step échoue. `AssumeRole`

  Résolution : le redéploiement de la pile d'administrateurs rompt le lien de confiance entre le rôle d'administrateur dans le compte d'administrateur et le rôle de membre dans les comptes de membres. Vous devez redéployer la pile des rôles des membres dans tous les comptes membres.

- Problème : les corrections de CIS 3.x ne s'affichent pas `PASSED` après plus de 24 heures.

  Solution : Cela se produit fréquemment si vous n'êtes pas abonné à la rubrique `SO0111-ASR_LocalAlarmNotification` SNS dans le compte membre.

Problèmes liés à des mesures correctives spécifiques

SSLBucketLa définition de la politique échoue avec une AccessDenied erreur

Contrôles associés : AWS FSBP v1.0.0 S3.5, PCI v3.2.1 PCI.S3.5, CIS v1.4.0 2.1.2, SC v2.0.0 S3.5

Problème : L'opération Set SSLBucket Policy échoue avec un AccessDenied message d'erreur :

Une erreur s'est produite (AccessDenied) lors de l'appel de l' PutBucketPolicy opération : Accès refusé

Si le paramètre Bloquer l'accès public a été activé pour un bucket, les tentatives de mise en place d'une politique de bucket incluant des instructions autorisant l'accès public échoueront avec cette erreur. Cet état peut être atteint en définissant une politique de compartiment contenant de telles instructions, puis en activant le blocage de l'accès public pour ce compartiment.

La correction ConfigureS3 BucketPublicAccessBlock (contrôles associés : AWS FSBP v1.0.0 S3.2, PCI v3.2.1 PCI.S3.2, CIS v1.4.0 2.1.5.2, SC v2.0.0 S3.2) peut également placer un bucket dans cet état car il définit le paramètre de blocage de l'accès public sans modifier la politique du bucket.

La règle Set SSLBucket Policy ajoute une instruction à la politique de compartiment pour refuser les demandes qui n'utilisent pas le protocole SSL. Cela ne modifie pas les autres instructions de la politique. Ainsi, si certaines instructions autorisent l'accès du public, la correction échouera en tentant de mettre en place la politique de compartiment modifiée qui inclut toujours ces instructions.

Résolution : modifiez la politique du compartiment pour supprimer les instructions qui autorisent l'accès public en conflit avec le paramètre de blocage de l'accès public sur le compartiment.

PuTS3 échoue BucketPolicyDeny

Contrôles associés : AWS FSBP v1.0.0 S3.6, NIST.800-53.r5 CA-9 (1), NIST.800-53.R5 CM-2

Problème : le PuTS3 BucketPolicyDeny avec l'erreur suivante :

```
Unable to create an explicit deny statement for {bucket_name}.
```

Si les principes de toutes les politiques du compartiment cible sont « * », la solution ne peut pas ajouter la politique de refus au compartiment cible car cela bloquerait toutes les actions du compartiment pour tous les principaux.

Solution : modifiez la politique des compartiments pour autoriser les actions sur des comptes spécifiques au lieu d'utiliser des principes « * » et limitez les actions refusées.

Comment désactiver la solution

En cas d'incident, il se peut que vous deviez désactiver la solution sans supprimer aucune infrastructure. Ces scénarios expliquent comment désactiver les différents composants de la solution.

Scénario 1 : désactiver la correction automatique pour un seul contrôle

1. Dans le compte Admin, accédez à la CloudFormation console AWS.
2. Localisez la pile d'administration et consultez son onglet Sorties.
3. Copiez la valeur de la `RemediationConfigurationDynamoDBTable` sortie.
4. Accédez à la console DynamoDB et ouvrez le tableau de configuration de correction.
5. Sélectionnez Explore Table Items (Explorer les éléments de la table).
6. Sous Numériser ou interroger des éléments, sélectionnez Requête.
7. Entrez l'ID de contrôle (par exemple,`Lambda.1`) dans le champ Clé de partition : ControlID et cliquez sur Exécuter.
8. Sélectionnez l'article renvoyé, puis cliquez sur Actions > Modifier l'article.
9. Remplacez la valeur de `automatedRemediationEnabled` l'attribut par False.
10. Cliquez sur Enregistrer et fermer.

Scénario 2 : désactiver la correction automatique pour tous les contrôles

1. Suivez les étapes 1 à 5 du scénario 1 pour accéder aux éléments du tableau de configuration de la correction.
2. Sous Numériser ou interroger des éléments, sélectionnez Numériser pour afficher toutes les commandes.
3. Pour chaque contrôle `automatedRemediationEnabled` défini sur True, sélectionnez l'élément et cliquez sur Actions > Modifier l'élément.
4. Modifiez la valeur de `automatedRemediationEnabled` l'attribut sur False et cliquez sur Enregistrer et fermer.
5. Répétez l'opération pour toutes les commandes que vous souhaitez désactiver.

Scénario 3 : désactiver la correction manuelle pour un compte

1. Accédez à la console EventBridge .
2. Sélectionnez Règles dans la barre latérale.
3. Sélectionnez le bus d'événements par défaut et recherchez`Remediate_with_ASR_CustomAction`.
4. Sélectionnez la règle et cliquez sur le bouton Désactiver.

Contacter AWS Support

Si vous disposez d'AWS Business Support+, d'AWS Enterprise Support ou d'Unified Operations, vous pouvez utiliser le centre de support AWS pour obtenir l'assistance d'experts concernant cette solution. Les sections suivantes fournissent des instructions.

Créer un dossier

1. Connectez-vous au Centre de Support.
2. Choisissez Create case (Créer une demande).

Comment pouvons-nous vous aider ?

1. Choisissez Technique.
2. Dans le champ Service, sélectionnez Solutions.
3. Dans Catégorie, sélectionnez Autres solutions.
4. Pour Severity, sélectionnez l'option qui correspond le mieux à votre cas d'utilisation.
5. Lorsque vous entrez le service, la catégorie et la gravité, l'interface contient des liens vers des questions de dépannage courantes. Si vous ne parvenez pas à résoudre votre question à l'aide de ces liens, sélectionnez Étape suivante : Informations supplémentaires.

Informations supplémentaires

1. Dans le champ Objet, saisissez un texte résumant votre question ou problème.
2. Pour la description, décrivez le problème en détail, notamment le nom de cette solution et la version que vous utilisez, par exemple : Automated Security Response on AWS Vx.y.z.

3. Choisissez Joindre des fichiers.
4. Joignez les informations dont le Support a besoin pour traiter la demande.

Aidez-nous à résoudre votre cas plus rapidement

1. Entrez les informations demandées.
2. Cliquez sur Étape suivante : résoudre maintenant ou nous contacter.

Résolvez maintenant ou contactez-nous

1. Passez en revue les solutions Solve now.
2. Si vous ne parvenez pas à résoudre votre problème avec ces solutions, choisissez Contactez-nous, entrez les informations demandées, puis cliquez sur Soumettre.

Désinstallez la solution

Utilisez la procédure suivante pour désinstaller la solution à l'aide de l'AWS Management Console.

V1.0.0-V1.2.1

Pour les versions v1.0.0 à v1.2.1, utilisez Service Catalog pour désinstaller les playbooks CIS and/or FSBP. Avec la version v1.3.0, Service Catalog n'est plus utilisé.

1. Connectez-vous à la CloudFormation console AWS et accédez au compte principal Security Hub.
2. Choisissez Service Catalog pour mettre fin à tous les playbooks provisionnés, supprimer les groupes de sécurité, les rôles ou les utilisateurs.
3. Supprimez le `CISPermissions.template` modèle Spoke des comptes membres du Security Hub.
4. Supprimez le `AFSBPMemberStack.template` modèle Spoke des comptes d'administrateur et de membre du Security Hub.
5. Accédez au compte principal Security Hub, sélectionnez la pile d'installation de la solution, puis choisissez Supprimer.

> **Note**
>
> CloudWatch Les journaux des groupes de journaux sont conservés. Nous vous recommandons de conserver ces journaux conformément à la politique de conservation des journaux de votre organisation.

V1.3.x

1. `automated-security-response-member.template`Supprimez-le de chaque compte membre.
2. `automated-security-response-admin.template`Supprimez-le du compte administrateur.

> **Note**
>
> La suppression du modèle d'administration dans la version v1.3.0 échouera probablement lors de la suppression de l'action personnalisée. Il s'agit d'un problème connu qui sera résolu dans la prochaine version. Suivez les instructions suivantes pour résoudre ce problème :
>
> 1. Connectez-vous à la console de gestion AWS Security Hub.
> 2. Dans le compte administrateur, allez dans Réglages.
> 3. Sélectionnez l'onglet Actions personnalisées.
> 4. Supprimez manuellement l'entrée Remediate with ASR.
> 5. Supprimez à nouveau la pile.

V1.4.0 et versions ultérieures

Déploiement en pile

1. `automated-security-response-member.template`Supprimez-le de chaque compte membre.
2. `automated-security-response-admin.template`Supprimez-le du compte administrateur.

StackSet déploiement

Pour chacun StackSet, supprimez les piles, puis retirez-les StackSet dans l'ordre inverse du déploiement.

Notez que les rôles IAM du `automated-security-response-member-roles.template` sont conservés même si le modèle est supprimé. Cela permet aux correctifs utilisant ces rôles de continuer à fonctionner. Ces rôles SO0111-* peuvent être supprimés manuellement après avoir vérifié qu'ils ne sont plus utilisés par les mesures correctives actives, telles que la CloudWatch journalisation ou la surveillance CloudTrail améliorée RDS.

Guide de l'administrateur

Activation et désactivation de certaines parties de la solution

En tant qu'administrateur de solution, vous disposez des contrôles suivants pour déterminer quelles fonctionnalités de la solution sont activées.

Où les piles de rôles des membres et des membres sont déployées :

- La pile d'administrateurs ne pourra initier des corrections (par le biais d'actions personnalisées ou entièrement automatisées) que dans les comptes dans lesquels les piles de membres et de rôles de membre ont été déployées avec le numéro de compte administrateur indiqué comme valeur de paramètre.
- Pour exempter complètement les comptes ou les régions du contrôle de la solution, ne déployez pas les piles de rôles des membres ou des membres sur ces comptes ou régions.

Configuration de l'agrégation de recherche de comptes et de régions dans Security Hub :

- La pile d'administrateurs ne pourra initier des corrections (par le biais d'actions personnalisées ou entièrement automatisées) que pour les résultats qui arrivent dans le compte administrateur et dans la région.
- Pour exempter complètement les comptes ou les régions du contrôle de la solution, n'incluez pas ces comptes ou régions pour envoyer les résultats au même compte administrateur et à la même région dans lesquels la pile d'administrateurs est déployée.

Quelles piles imbriquées standard sont déployées :

- La pile d'administrateurs ne pourra initier des corrections (par le biais d'actions personnalisées ou entièrement automatisées) que pour les contrôles dotés d'un manuel de contrôle déployé dans le compte membre et la région cibles. Ils sont déployés par la pile de membres pour chaque norme.
- La pile d'administrateurs ne pourra lancer des corrections entièrement automatisées que pour les contrôles activés dans la table DynamoDB de configuration des mesures correctives. Cette table est déployée sur le compte administrateur.
- Pour des raisons de simplicité, nous vous recommandons de déployer les normes de manière cohérente sur l'ensemble de vos comptes d'administrateur et de membre. Si AWS FSBP et

CIS v1.2.0 vous intéressent, déployez ces deux piles d'administration imbriquées sur le compte administrateur, puis déployez ces deux piles de membres imbriquées sur chaque compte membre et région.

Quels runbooks Control sont déployés dans chaque pile de membres imbriquée :

- La pile d'administrateurs ne pourra initier des corrections (par le biais d'actions personnalisées ou entièrement automatisées) que pour les contrôles dotés d'un manuel de contrôle déployé dans le compte membre cible et dans la région par la pile de membres pour chaque norme.
- Pour exercer un contrôle plus précis sur les contrôles activés pour une norme donnée, chaque pile imbriquée d'une norme possède des paramètres pour lesquels les runbooks de contrôle sont déployés. Définissez le paramètre d'un contrôle sur la valeur « NON disponible » pour annuler le déploiement de ce runbook de contrôle.

Paramètres SSM pour activer et désactiver les normes :

- La pile d'administration ne pourra initier des corrections (par le biais d'actions personnalisées ou entièrement automatisées) que pour les normes activées via le paramètre SSM déployé par la pile d'administration standard.
- <standard_version>Pour désactiver une norme, définissez la valeur du paramètre SSM avec le chemin « /Solutions/SO0111/<standard_name>//status » sur « Non ».

Accès à l'interface utilisateur Web de la solution :

- Lorsque la pile d'administrateurs sera déployée, vous recevrez un e-mail contenant des informations d'identification temporaires vous permettant de vous connecter à l'interface utilisateur Web à l'aide de l'adresse e-mail que vous avez fournie lors du déploiement.
- À l'aide de la page Inviter des utilisateurs, les administrateurs et les administrateurs délégués peuvent inviter des utilisateurs supplémentaires à accéder à l'interface utilisateur Web et à déléguer l'accès à la solution.
- La page Afficher les utilisateurs permet aux administrateurs et aux administrateurs délégués de consulter et de gérer les utilisateurs existants.
- Pour en savoir plus sur les autorisations et sur l'utilisation de l'interface utilisateur Web de la solution, consultez lethe section called “Interface utilisateur Web”.

Exemples de notifications SNS

Lorsqu'une correction est initiée

```
{
 "severity": "INFO",
 "message": "00000000-0000-0000-0000-000000000000: Remediation queued for SC control
 RDS.13 in account 111111111111",
 "finding": {
 "finding_id": "22222222-2222-2222-2222-222222222222",
 "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
 "standard_name": "security-control",
 "standard_version": "2.0.0",
 "standard_control": "RDS.13",
 "title": "RDS automatic minor version upgrades should be enabled",
 "region": "us-east-1",
 "account": "111111111111",
 "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
 }
}
```

En cas de réussite d'une correction

```
{
 "severity": "INFO",
 "message": "00000000-0000-0000-0000-000000000000: Remediation succeeded for SC
 control RDS.13 in account 111111111111: See Automation Execution output for details
 (AwsRdsDbInstance arn:aws:rds:us-east-1:111111111111:db:database-1)",
 "finding": {
 "finding_id": "22222222-2222-2222-2222-222222222222",
 "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
 "standard_name": "security-control",
 "standard_version": "2.0.0",
 "standard_control": "RDS.13",
 "title": "RDS automatic minor version upgrades should be enabled",
 "region": "us-east-1",
 "account": "111111111111",
 "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
 }
```

```
}
```

En cas d'échec d'une correction

```
{
 "severity": "ERROR",
 "message": "00000000-0000-0000-0000-000000000000: Remediation failed for SC
 control RDS.13 in account 111111111111: See Automation Execution output for details
 (AwsRdsDbInstance arn:aws:rds:us-east-1:111111111111:db:database-1)",
 "finding": {
 "finding_id": "22222222-2222-2222-2222-222222222222",
 "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
 "standard_name": "security-control",
 "standard_version": "2.0.0",
 "standard_control": "RDS.13",
 "title": "RDS automatic minor version upgrades should be enabled",
 "region": "us-east-1",
 "account": "111111111111",
 "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
 }
}
```

didacticiel

Il s'agit d'un didacticiel qui vous guidera tout au long de votre premier déploiement d'ASR. Cela commencera par les conditions préalables au déploiement de la solution et se terminera par la correction des exemples trouvés dans un compte membre.

Tutoriel : Démarrage avec Automated Security Response sur AWS

Il s'agit d'un didacticiel qui vous guidera tout au long de votre premier déploiement. Cela commencera par les conditions préalables au déploiement de la solution et se terminera par la correction des exemples trouvés dans un compte membre.

Préparez les comptes

Afin de démontrer les capacités de correction entre comptes et entre régions de la solution, ce didacticiel utilisera deux comptes. Vous pouvez également déployer la solution sur un seul compte.

Les exemples suivants utilisent `111111111111` des comptes `222222222222` pour démontrer la solution. `111111111111`sera le compte administrateur et `222222222222` sera le compte membre. Nous mettrons en place la solution pour remédier aux problèmes liés aux ressources dans les régions `us-east-1` et`us-west-2`.

Le tableau ci-dessous est un exemple illustrant les actions que nous entreprendrons pour chaque étape dans chaque compte et région.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
`111111111111`	Admin	Aucune	Aucune
`222222222222`	Membre	Aucune	Aucune

Le compte administrateur est le compte qui exécutera les actions d'administration de la solution, notamment le lancement manuel des corrections ou l'activation d'une correction entièrement automatisée à l'aide de la table DynamoDB de configuration des corrections. Ce compte doit également être le compte d'administrateur délégué de Security Hub pour tous les comptes dans lesquels vous souhaitez corriger les résultats, mais il n'est pas nécessaire et il ne doit pas être le

compte administrateur AWS Organizations de l'organisation AWS à laquelle appartiennent vos comptes.

Activation d'AWS Config

Consultez la documentation suivante :

- Documentation AWS Config
- Tarification d'AWS Config
- Activation d'AWS Config

Activez AWS Config dans les deux comptes et dans les deux régions. Cela entraînera des frais.

> **Important**
>
> Assurez-vous de sélectionner l'option « Inclure les ressources globales (par exemple, les ressources AWS IAM) ». Si vous ne sélectionnez pas cette option lors de l'activation d'AWS Config, vous ne verrez pas les résultats relatifs aux ressources globales (par exemple, les ressources AWS IAM)

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Admin	Activation d'AWS Config	Activation d'AWS Config
222222222222	Membre	Activation d'AWS Config	Activation d'AWS Config

Activer le hub de sécurité AWS

Consultez la documentation suivante :

- Documentation d'AWS Security Hub
- Tarification d'AWS Security Hub
- Activation d'AWS Security Hub

Activez AWS Security Hub dans les deux comptes et dans les deux régions. Cela entraînera des frais.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Admin	Activer AWS Security Hub	Activer AWS Security Hub
222222222222	Membre	Activer AWS Security Hub	Activer AWS Security Hub

Permettre des résultats de contrôle consolidés

Consultez la documentation suivante :

- Génération et mise à jour des résultats de contrôle

Dans le cadre de ce didacticiel, nous allons démontrer l'utilisation de la solution en activant la fonctionnalité de résultats de contrôle consolidés d'AWS Security Hub, qui est la configuration recommandée. Dans les partitions qui ne prennent pas en charge cette fonctionnalité au moment de la rédaction, vous devrez déployer les playbooks spécifiques au standard plutôt que le SC (Security Control).

Activez les résultats de contrôle consolidés dans les deux comptes et dans les deux régions.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Admin	Permettre des résultats de contrôle consolidés	Permettre des résultats de contrôle consolidés
222222222222	Membre	Permettre des résultats de contrôle consolidés	Permettre des résultats de contrôle consolidés

La génération des résultats avec la nouvelle fonctionnalité peut prendre un certain temps. Vous pouvez poursuivre le didacticiel, mais vous ne pourrez pas corriger les résultats générés sans la

nouvelle fonctionnalité. Les résultats générés avec la nouvelle fonctionnalité peuvent être identifiés par la valeur du `GeneratorId` champ`security-control/<control_id>`.

Configurer l'agrégation de recherche entre régions

Consultez la documentation suivante :

- Agrégation entre régions
- Activation de l'agrégation entre régions

Configurez l'agrégation de recherche entre us-west-2 et us-east-1 dans les deux comptes.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Admin	Configurer l'agrégation depuis us-west-2	Aucune
222222222222	Membre	Configurer l'agrégation depuis us-west-2	Aucune

La propagation des résultats dans la région d'agrégation peut prendre un certain temps. Vous pouvez poursuivre le didacticiel, mais vous ne pourrez pas corriger les résultats provenant d'autres régions tant qu'ils ne commenceront pas à apparaître dans la région d'agrégation.

Désignez un compte administrateur Security Hub

Consultez la documentation suivante :

- Gestion des comptes dans AWS Security Hub
- Gestion des comptes des membres de l'organisation
- Gérer les comptes des membres sur invitation

Dans l'exemple suivant, nous utiliserons la méthode d'invitation manuelle. Pour un ensemble de comptes de production, nous recommandons de gérer l'administration déléguée de Security Hub via AWS Organizations.

Depuis la console AWS Security Hub, dans le compte administrateur (111111111111), invitez le compte membre (222222222222) à accepter le compte administrateur en tant qu'administrateur délégué du Security Hub. Depuis le compte membre, acceptez l'invitation.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Admin	Inviter le compte membre	Aucune
222222222222	Membre	Acceptez l'invitation	Aucune

La propagation des résultats vers le compte administrateur peut prendre un certain temps. Vous pouvez poursuivre le didacticiel, mais vous ne pourrez pas corriger les résultats des comptes des membres tant qu'ils ne commenceront pas à apparaître dans le compte administrateur.

Création des rôles pour les autorisations autogérées StackSets

Consultez la documentation suivante :

- AWS CloudFormation StackSets
- Accorder des autorisations autogérées

Nous allons déployer des CloudFormation stacks sur plusieurs comptes, nous allons donc utiliser StackSets. Nous ne pouvons pas utiliser les autorisations gérées par le service car la pile d'administrateurs et la pile de membres ont des piles imbriquées, qui ne sont pas prises en charge par le service. Nous devons donc utiliser des autorisations autogérées.

Déployez les piles pour obtenir des autorisations de base pour les StackSet opérations. Pour les comptes de production, vous souhaiterez peut-être restreindre les autorisations conformément à la documentation sur les « options d'autorisations avancées ».

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Admin	Déployer la pile de rôles d' StackSet administrateur	Aucune

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
		Déployer la pile de rôles StackSet d'exécution	
222222222222	Membre	Déployer la pile de rôles StackSet d'exécution	Aucune

Créez les ressources non sécurisées qui généreront des exemples de résultats

Consultez la documentation suivante :

- Référence des contrôles Security Hub
- Contrôles AWS Lambda

L'exemple de ressource suivant avec une configuration non sécurisée afin de démontrer une correction. L'exemple de contrôle est Lambda.1 : les politiques relatives aux fonctions Lambda doivent interdire l'accès public.

> **Important**
>
> Nous allons créer intentionnellement une ressource avec une configuration non sécurisée. Passez en revue la nature du contrôle et évaluez le risque lié à la création d'une telle ressource dans votre environnement pour vous-même. Renseignez-vous sur les outils dont dispose votre organisation pour détecter et signaler de telles ressources et demandez une exception le cas échéant. Si l'exemple de contrôle que nous avons sélectionné ne vous convient pas, sélectionnez un autre contrôle pris en charge par la solution.

Dans la deuxième région du compte membre, accédez à la console AWS Lambda et créez une fonction dans le dernier environnement d'exécution Python. Sous Configuration → Autorisations, ajoutez une déclaration de politique permettant d'appeler la fonction depuis l'URL sans authentification.

Vérifiez sur la page de console que la fonction autorise l'accès public. Une fois que la solution a résolu ce problème, comparez les autorisations pour confirmer que l'accès public a été révoqué.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
`111111111111`	Admin	Aucune	Aucune
`222222222222`	Membre	Aucune	Création d'une fonction Lambda avec une configuration non sécurisée

AWS Config peut mettre un certain temps à détecter la configuration non sécurisée. Vous pouvez poursuivre le didacticiel, mais vous ne pourrez pas corriger le résultat tant que Config ne l'aura pas détecté.

Création de groupes de CloudWatch journaux pour les contrôles associés

Consultez la documentation suivante :

- Surveillance des fichiers CloudTrail journaux avec Amazon CloudWatch Logs
- CloudTrail commandes

CloudTrail Les différents contrôles pris en charge par la solution nécessitent qu'un groupe de CloudWatch journaux soit la destination d'une multirégion. CloudTrail Dans l'exemple suivant, nous allons créer un groupe de journaux à espace réservé. Pour les comptes de production, vous devez configurer correctement CloudTrail l'intégration avec CloudWatch Logs.

Créez un groupe de journaux dans chaque compte et région avec le même nom, par exemple :`asr-log-group`.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
`111111111111`	Admin	Création d'un groupe de journaux	Création d'un groupe de journaux

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
222222222222	Membre	Création d'un groupe de journaux	Création d'un groupe de journaux

Déployer la solution sur des comptes de didacticiel

Rassemblez les trois Amazon S3 URLs pour la pile des rôles d'administrateur, de membre et de membre.

Déployer la pile d'administration

View template

automa

security-response-admin.modèle

Dans le compte administrateur, accédez à la CloudFormation console et déployez la pile d'administrateurs dans la région d'agrégation de recherche du Security Hub.

Choisissez No la valeur de tous les paramètres de chargement des piles d'administration imbriquées, à l'exception de la pile « SC » ou « Security Control ». Cette pile contient les ressources nécessaires aux résultats de contrôle consolidés que nous avons configurés dans nos comptes.

Choisissez No de réutiliser le groupe de journaux de l'orchestrateur, sauf si vous avez déjà déployé cette solution dans ce compte et cette région.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Admin	Déployer la pile d'administration	Aucune
222222222222	Membre	Aucune	Aucune

Attendez que la pile d'administrateurs ait terminé le déploiement avant de continuer afin qu'une relation de confiance puisse être créée entre les comptes membres et le compte administrateur.

Déployer la pile de membres

automa

security-response-member.modèle

Dans le compte administrateur, accédez à la CloudFormation StackSets console et déployez la pile de membres sur chaque compte et région. Utilisez les rôles StackSets d'administration et d'exécution créés dans ce didacticiel.

Entrez le nom du groupe de journaux que vous avez créé comme valeur du paramètre pour le nom du groupe de journaux.

Choisissez No la valeur de tous les paramètres de chargement des piles de membres imbriquées, à l'exception de la pile « SC » ou « Security Control ». Cette pile contient les ressources nécessaires aux résultats de contrôle consolidés que nous avons configurés dans nos comptes.

Entrez l'ID du compte administrateur comme valeur du paramètre du numéro de compte administrateur. Dans notre exemple, c'est le cas111111111111.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Admin	Déployer le StackSet membre/Confirmer le déploiement de la pile de membres	Confirmer le déploiement de la pile de membres
222222222222	Membre	Confirmer le déploiement de la pile de membres	Confirmer le déploiement de la pile de membres

Déployer la pile de rôles des membres

automated-security-response-memberbouton de modèle -roles.template -roles.template automated-security-response-member

Dans le compte administrateur, accédez à la CloudFormation StackSets console et déployez la pile de membres sur chaque compte. Utilisez les rôles StackSets d'administration et d'exécution créés

dans ce didacticiel. Entrez l'ID du compte administrateur comme valeur du paramètre du numéro de compte administrateur. Dans notre exemple, c'est le cas111111111111.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Admin	Déployer le StackSet membre/Confirmer le déploiement de la pile de membres	Aucune
222222222222	Membre	Confirmer le déploiement de la pile de membres	Aucune

Vous pouvez continuer, mais vous ne pourrez pas corriger les résultats tant que le déploiement n'aura pas CloudFormation StackSets été terminé.

Abonnez-vous à la rubrique SNS

Mises à jour des mesures correctives

Sujet - {https---us-east-1-console-aws-amazon-com-sns-v3- home-region-us-east -1— topic-arn-aws-sns -US-East-1-221128147805-SO0111-ASR-Topic} [SO0111-ASR_Topic]

Dans le compte administrateur, abonnez-vous à la rubrique Amazon SNS créée par la pile d'administrateurs. Cela vous avertira lorsque les mesures correctives seront initiées et en cas de réussite ou d'échec.

Alarmes

Sujet - {https---us-east-1-console-aws-amazon-com-sns-v3- home-region-us-east -1— -US-East-1-221128147805-SO0111-ASR-Alarm-Topic} [SO0111-ASR_Alarm_Topictopic-arn-aws-sns]

Dans le compte administrateur, abonnez-vous à la rubrique Amazon SNS créée par la pile d'administrateurs. Cela vous avertira lorsque des alarmes métriques se déclenchent.

Corriger les résultats des exemples

> **Important**
>
> Cet exemple nécessite l'utilisation de la console Security Hub CSPM. La console Security Hub (non CSPM) ne prend actuellement pas en charge les corrections manuelles via une action personnalisée. Pour corriger les résultats sans utiliser la console Security Hub CSPM, consultez la section Corriger à l'aide de l'interface utilisateur Web.

Dans le compte administrateur, accédez à la console Security Hub CSPM et recherchez la ressource dont la configuration n'est pas sécurisée que vous avez créée dans le cadre de ce didacticiel.

Cela peut se faire de plusieurs manières :

1. Dans les partitions qui prennent en charge la fonctionnalité des résultats de contrôle consolidés, une page intitulée « Contrôles » vous permet de localiser le résultat à l'aide de l'ID de contrôle consolidé.
2. Dans la page « Normes de sécurité », vous pouvez localiser le contrôle en fonction de la norme à laquelle il appartient.
3. Vous pouvez consulter tous les résultats sur la page « Résultats » et effectuer une recherche par attribut.

L'ID de contrôle consolidé pour la fonction Lambda publique que nous avons créée est Lambda.1.

Lancer la correction

Cochez la case située à gauche de la constatation relative à la ressource que nous avons créée. Dans le menu déroulant « Actions », sélectionnez « Corriger avec ASR ». Vous verrez une notification indiquant que le résultat a été envoyé à Amazon EventBridge.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Admin	Lancer la correction	Aucune
222222222222	Membre	Aucune	Aucune

Confirmez que la correction a résolu le problème

Vous devriez recevoir deux notifications SNS. Le premier indiquera qu'une correction a été initiée, et le second indiquera que la correction a réussi. Après avoir reçu la deuxième notification, accédez à la console Lambda dans le compte membre et confirmez que l'accès public a été révoqué.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Admin	Aucune	Aucune
222222222222	Membre	Aucune	Confirmez que la correction a réussi

Corriger à l'aide de l'interface utilisateur Web

Vous pouvez également utiliser l'interface utilisateur Web de la solution pour corriger les résultats d'AWS Security Hub et consulter les correctifs antérieurs.

> **Note**
>
> Vous devez définir le `ShouldDeployWebUI` paramètre sur « yes » lors du déploiement de la pile d'administration afin d'utiliser l'interface utilisateur Web de la solution.

Connectez-vous à l'interface utilisateur Web

Après le déploiement de la solution, vous recevrez un e-mail contenant des informations d'identification temporaires et un lien vers l'interface utilisateur Web de la solution de la part de no-reply@verificationemail.com. Il sera envoyé à l'adresse e-mail que vous avez fournie lors du déploiement de la pile d'administrateurs.

Localisez l'e-mail, copiez les informations d'identification temporaires et cliquez sur le lien de l'interface utilisateur Web. Ce lien vous mènera directement à la page de connexion, où vous devrez saisir vos informations d'identification temporaires et définir un nouveau mot de passe.

Localisez la découverte de Lambda.1

Une fois connecté, la page des résultats s'affichera. Cette page affiche tous les résultats relatifs au Security Hub enregistrés dans votre compte administrateur Security Hub qui sont pris en charge pour la correction, y compris les résultats relatifs aux comptes membres intégrés à AWS Security Hub.

Sur la page Résultats, utilisez la barre de recherche pour filtrer par ID de ressource en saisissant l'ARN de la fonction Lambda que vous avez créée dans le cadre de ce didacticiel et en effectuant une recherche à l'aide de l'opérateur « = ». Cela affichera toutes les conclusions d'AWS Security Hub prises en charge par la solution pour la fonction Lambda que vous avez créée.

Pour `Lambda.1` trouver le résultat généré dans ce didacticiel, appliquez un autre filtre sur Type de recherche. Cliquez sur la barre de recherche, sélectionnez Type de recherche, puis sélectionnez l'opérateur « = ». Si les résultats de contrôle consolidés sont activés dans votre environnement, entrez`security-control/Lambda.1`. Sinon, choisissez une norme de sécurité compatible avec le contrôle Lambda.1 et entrez l'ID du générateur, par exemple. `aws-foundational-security-best-practices/v/1.0.0/Lambda.1`

Après avoir appliqué les filtres Resource ID et Finding Type, vous ne verrez que le résultat Lambda.1 généré par AWS Security Hub pour votre ressource de test répertorié dans le tableau.

> **Note**
>
> AWS Security Hub peut mettre un certain temps à générer le résultat Lambda.1 pour la ressource que vous avez créée. Si vous ne voyez pas le résultat après avoir appliqué les deux filtres, attendez 5 à 10 minutes et recherchez à nouveau le résultat.

Lancer la correction

Sélectionnez le résultat que vous avez trouvé à l'étape précédente, puis cliquez sur Actions > Corriger. Cela permettra de commencer à corriger le résultat que vous avez sélectionné.

Vous pouvez consulter la progression de cette correction sur la page Historique des exécutions. Après quelques minutes d'attente, actualisez la page Historique des exécutions en cliquant sur l'icône d'actualisation en haut à droite. Vous devriez voir que le statut est passé de `In progress` à`Success`.

Confirmez que la correction a résolu le problème

Lorsque le résultat est marqué comme provenant `Resolved` d'AWS Security Hub, il est automatiquement supprimé de la page Résultats de l'interface utilisateur Web.

Pour vérifier que la correction a résolu le problème, accédez à la console Lambda dans le compte membre et confirmez que l'accès public a été révoqué.

> **Note**
>
> Certains résultats peuvent toujours apparaître sur la page Résultats, même avec un statut de correction de`Success`. Cela est dû au fait qu'AWS Security Hub met jusqu'à 24 heures pour marquer un résultat comme résolu après la mise à jour de la ressource. Vous pouvez supprimer les résultats que vous ne souhaitez plus voir sur la page Résultats en sélectionnant le résultat et en cliquant sur Actions > Supprimer.

Suivez l'exécution de la remédiation

Pour mieux comprendre le fonctionnement de la solution, vous pouvez suivre l'exécution de la correction.

EventBridge règle

Dans le compte administrateur, recherchez une EventBridge règle nommée CustomActionRemediate_with_ASR_. Cette règle correspond au résultat que vous avez envoyé depuis Security Hub et l'envoie à Orchestrator Step Functions.

Step Functions : exécution

Dans le compte administrateur, recherchez les fonctions AWS Step Functions nommées « SO0111-ASR-Orchestrator ». Cette fonction d'étape appelle le document SSM Automation dans le compte et la région cibles. Vous pouvez suivre l'exécution de la correction dans l'historique d'exécution de cet AWS Step Functions.

Automatisation SSM

Dans le compte membre, accédez à la console SSM Automation. Vous trouverez deux exécutions d'un document nommé « ASR-SC_2.0.0_Lambda.1 » et une exécution d'un document nommé « ASR- ». RemoveLambdaPublicAccess

La première exécution provient de la fonction d'étape de l'orchestrateur dans le compte cible. La deuxième exécution a lieu dans la région cible, qui peut ne pas être la région d'où provient la découverte. L'exécution finale est la correction qui révoque la politique d'accès public de la fonction Lambda.

CloudWatch Groupe de journaux

Dans le compte administrateur, accédez à la console CloudWatch Logs et recherchez un groupe de journaux nommé « SO0111-ASR ». Ce groupe de journaux est la destination des journaux de haut niveau provenant d'Orchestrator Step Functions.

Activez des mesures correctives entièrement automatisées

L'autre mode de fonctionnement de la solution consiste à corriger automatiquement les résultats dès leur arrivée dans Security Hub.

> **Important**
>
> Avant d'activer les corrections entièrement automatisées, assurez-vous que la solution est configurée dans les comptes et les régions où vous êtes conforme aux modifications automatisées apportées par la solution. Si vous souhaitez réduire la portée des corrections automatisées de la solution, consultez la section ci-dessous sur le filtrage des corrections entièrement automatisées.

Exemple : activer les corrections entièrement automatisées pour Lambda.1

L'activation des corrections automatiques initiera des corrections sur toutes les ressources correspondant au contrôle que vous activez (Lambda.1).

> **Important**
>
> Confirmez que vous souhaitez que cette autorisation soit révoquée pour toutes les fonctions Lambda publiques incluses dans le cadre de la solution. La portée des corrections entièrement automatisées ne sera pas limitée à la fonction que vous avez créée. La solution corrigera ce contrôle s'il est détecté dans l'un des comptes ou régions dans lesquels il est installé.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Admin	Confirmez qu'aucune fonction publique n'est souhaitée	Confirmez qu'aucune fonction publique n'est souhaitée
222222222222	Membre	Confirmez qu'aucune fonction publique n'est souhaitée	Confirmez qu'aucune fonction publique n'est souhaitée

Localisez la table DynamoDB de configuration de correction

Dans le compte administrateur, consultez la pile `Outputs` réservée aux administrateurs dans la CloudFormation console. Vous verrez une sortie intituléeRemediationConfigurationDynamoDBTable.

Il s'agit du nom de la table DynamoDB de configuration de correction, qui contrôle les configurations de correction automatisées pour la solution. Copiez la valeur de cette sortie et recherchez la table DynamoDB correspondante dans la console DynamoDB.

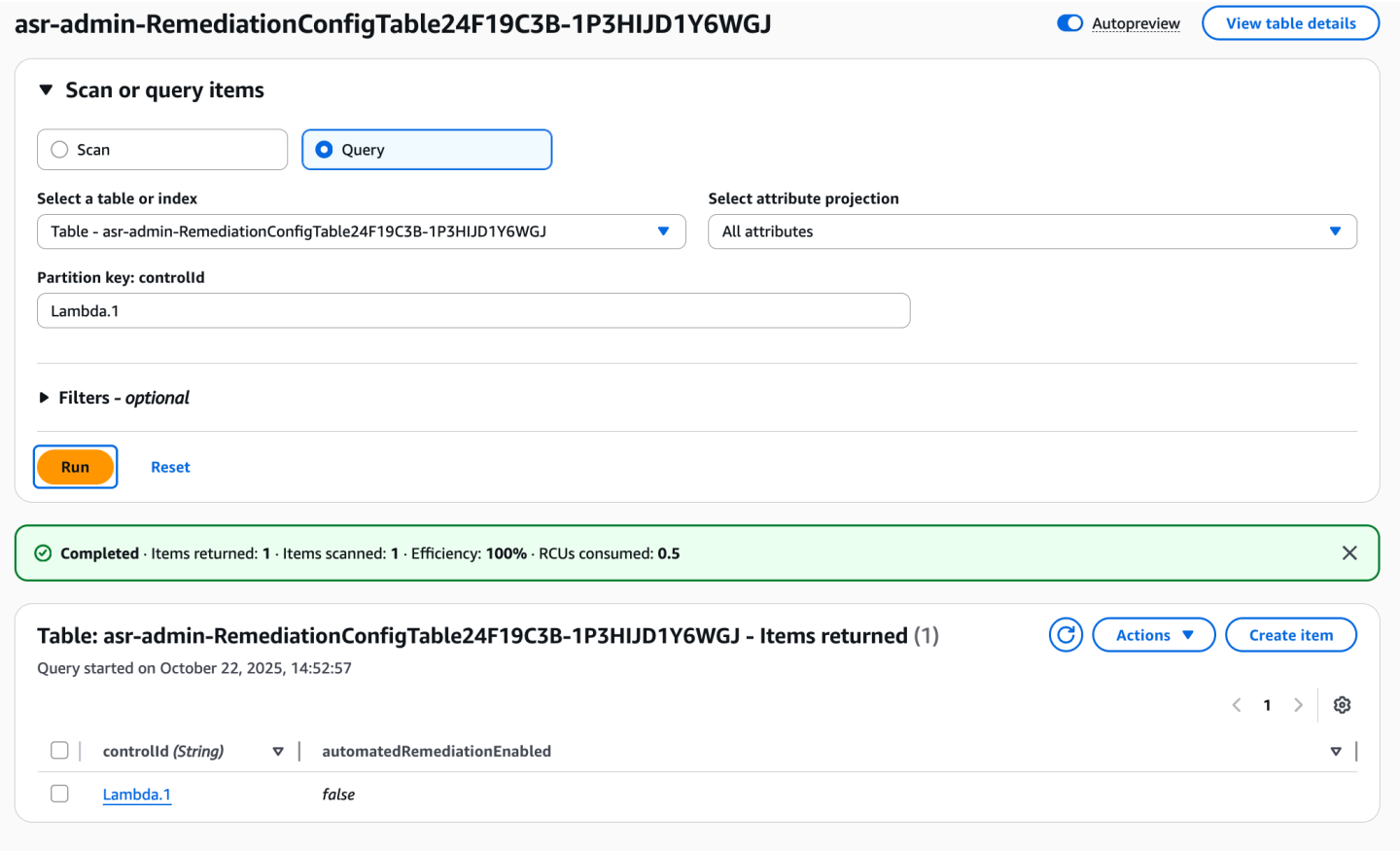
Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Admin	Localisez la table DynamoDB de configuration de correction.	Aucune
222222222222	Membre	Aucune	Aucune

Modifier le tableau de configuration de la correction

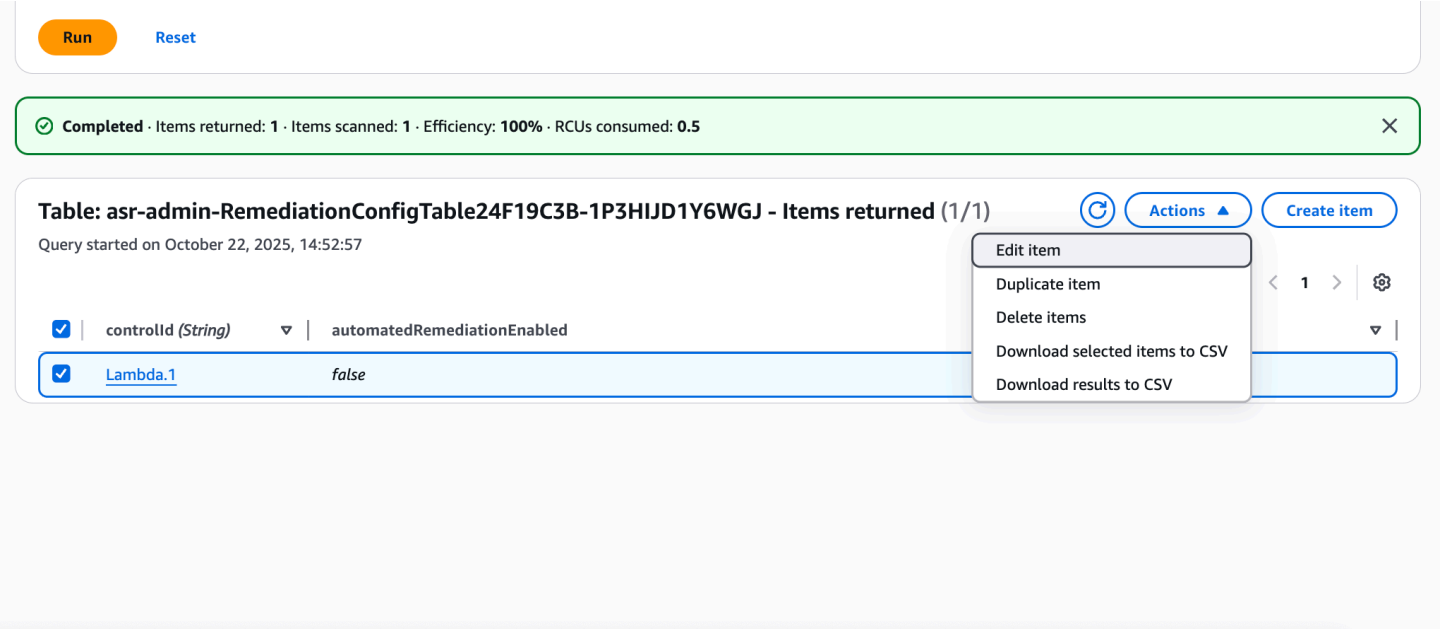
Dans la console DynamoDB où se trouve le tableau de configuration de correction, sélectionnez Explorer les éléments du tableau.

Chaque élément du tableau correspond à un contrôle Security Hub pris en charge par la solution. Chaque élément possède un `automatedRemediationEnabled` attribut qui peut être modifié pour permettre des corrections entièrement automatisées pour le contrôle associé.

Pour activer Lambda.1, sous Numériser ou interroger des éléments, sélectionnez Requête. Sous Clé de partition : ControlID, entrez `Lambda.1` et cliquez sur Exécuter. Vous verrez un seul article retourné correspondant au contrôle Lambda.1.



Maintenant, sélectionnez l'`Lambda.1`élément, puis cliquez sur Actions > Modifier l'élément.



Enfin, remplacez la valeur de `automatedRemediationEnabled` l'attribut par True. Cliquez sur Enregistrer et fermer.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Admin	Modifiez le tableau DynamoDB de configuration de correction.	Aucune
222222222222	Membre	Aucune	Aucune

Configuration de la ressource

Dans le compte membre, reconfigurez la fonction Lambda pour autoriser l'accès public.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Admin	Aucune	Aucune
222222222222	Membre	Aucune	Configurer la fonction Lambda pour

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
			autoriser l'accès public

Confirmez que la correction a résolu le problème

Config peut mettre un certain temps à détecter à nouveau la configuration non sécurisée. Vous devriez recevoir deux notifications SNS. Le premier indiquera qu'une correction a été initiée. Le second indiquera que la correction a réussi. Après avoir reçu la deuxième notification, accédez à la console Lambda dans le compte membre et confirmez que l'accès public a été révoqué.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
`111111111111`	Admin	Aucune	Aucune
`222222222222`	Membre	Aucune	Confirmez que la correction a réussi

(Facultatif) Configurer le filtrage pour des corrections entièrement automatisées

Si vous souhaitez limiter l'étendue dans laquelle la solution exécute les corrections, vous pouvez appliquer des filtres. Ces filtres ne s'appliqueront qu'aux corrections entièrement automatisées et n'auront aucun impact sur les corrections invoquées manuellement.

La solution propose un filtrage sur les dimensions suivantes :

1. Identifiants de compte
2. Unités organisationnelles (OUs)
3. Balises des ressources

Chaque dimension est configurable en modifiant les paramètres de Systems Manager déployés par la solution correspondant à la dimension donnée. Tous les paramètres de filtrage du Parameter Store se trouvent dans le compte Admin, sous le `/ASR/Filters/` chemin.

Chaque dimension possède deux paramètres de configuration, l'un pour la valeur du filtre et l'autre pour le mode de filtre. Par exemple, la dimension Account Ids comporte deux paramètres nommés `/ASR/Filters/AccountFilters` et`/ASR/Filters/AccountFilterMode`. Les deux doivent être modifiés pour configurer le filtrage sur les identifiants de compte.

Par exemple, pour limiter les corrections entièrement automatisées à l'exécution uniquement sur les comptes `111111111111222222222222`, vous devez remplacer la valeur par « 111111111111, `/ASR/Filters/AccountFilters` 222222222222 ». Changez ensuite la valeur de `/ASR/Filters/AccountFilterMode` en « Inclure ». La solution ignorera alors les résultats générés pour des comptes autres que 1111111111 ou 222222222222.

Chaque paramètre de filtre utilise une liste de valeurs séparées par des virgules à filtrer, et chaque paramètre de « mode » peut être défini sur Inclure, Exclure ou Désactivé.

Nettoyage

Supprimer les exemples de ressources

Dans le compte membre, supprimez l'exemple de fonction Lambda que vous avez créé.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
`111111111111`	Admin	Aucune	Aucune
`222222222222`	Membre	Aucune	Supprimer l'exemple de fonction Lambda

Supprimer la pile d'administrateurs

Dans le compte administrateur, supprimez la pile d'administrateurs.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
`111111111111`	Admin	Supprimer la pile d'administrateurs	Aucune
`222222222222`	Membre	Aucune	Aucune

Supprimer la pile de membres

Dans le compte Admin, supprimez le membre StackSet.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Admin	Supprimer le membre StackSet Confirmer la suppression de la pile de membres	Confirmer la suppression de la pile de membres
222222222222	Membre	Confirmer la suppression de la pile de membres	Confirmer la suppression de la pile de membres

Supprimer la pile de rôles des membres

Dans le compte administrateur, supprimez les rôles des membres StackSet.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Admin	Supprimer les rôles des membres StackSet Confirmez que la pile de rôles des membres a été supprimée	Aucune
222222222222	Membre	Confirmer la suppression de la pile des rôles des membres	Aucune

Supprimer les rôles conservés

Dans chaque compte, supprimez les rôles IAM conservés.

Important : Ces rôles sont conservés pour les corrections qui nécessitent un rôle pour que la correction continue de fonctionner (par exemple, journalisation des flux VPC). Vérifiez que vous n'avez pas besoin du fonctionnement continu d'aucun de ces rôles avant de les supprimer.

Supprimez tous les rôles préfixés par SO0111-.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Admin	Supprimer les rôles conservés	Aucune
222222222222	Membre	Supprimer les rôles conservés	Aucune

Planifiez la suppression des clés KMS conservées

Les piles d'administrateurs et de membres créent et conservent une clé KMS. Des frais vous seront facturés si vous conservez ces clés.

Ces clés sont conservées afin de vous donner accès à toutes les ressources cryptées par la solution. Vérifiez que vous n'en avez pas besoin avant de planifier leur suppression.

Identifiez les clés déployées par la solution à l'aide des alias créés par la solution ou à partir de l' CloudFormation historique. Programmez-les pour leur suppression.

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Admin	Identifier et planifier la suppression de la clé d'administration Identifier et planifier la suppression de la clé de membre	Identifier et planifier la suppression de la clé de membre

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
222222222222	Membre	Identifier et planifier la suppression de la clé de membre	Identifier et planifier la suppression de la clé de membre

Supprimer les piles pour les autorisations autogérées StackSets

Supprimer les piles créées pour autoriser les autorisations autogérées StackSets

Compte	Objectif	Action dans us-east-1	Action dans us-west-2
111111111111	Admin	Supprimer la pile de rôles d' StackSet administrateur	Aucune
222222222222	Membre	Supprimer la pile de rôles StackSet d'exécution	Aucune

Guide du développeur

Cette section fournit le code source de la solution ainsi que des personnalisations supplémentaires.

Code source

Consultez notre GitHub référentiel pour télécharger les modèles et les scripts de cette solution et pour partager vos personnalisations avec d'autres utilisateurs.

Playbooks

Cette solution inclut les correctifs relatifs aux normes de sécurité définies dans le cadre du Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v3.0.0, AWS Foundational Security Best Practices (FSBP) v.1.0.0,Payment Card Industry Data Security Standard (PCI-DSS) v3.2.1 et National Institute ofStandards and Technology (NIST).

Si vous avez activé les résultats des contrôles consolidés, ces contrôles sont pris en charge dans toutes les normes. Si cette fonctionnalité est activée, seul le playbook SC doit être déployé. Si ce n'est pas le cas, les playbooks sont compatibles avec les normes répertoriées précédemment.

> **Important**
>
> Déployez uniquement les playbooks correspondant aux normes activées afin d'éviter d'atteindre les quotas de service.

Pour plus de détails sur une correction spécifique, reportez-vous au document d'automatisation de Systems Manager portant le nom déployé par la solution dans votre compte. Accédez à la console AWS Systems Manager, puis dans le volet de navigation, sélectionnez Documents.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
Nombre total de mesures correctives	63	34	29	33	65	19	90
ASR-EnableAutoScalingGroup ELBHealthVérifier Les groupes Auto Scaling associés à un équilibreur de charge doivent utiliser des contrôles de santé de l'équilibreur de charge	Mise à l'échelle automatique.1		Mise à l'échelle automatique.1		Mise à l'échelle automatique.1		Mise à l'échelle automatique.1

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-ConfigureAutoScalingLaunchConfigToRequireIMDSv2 Les configurations de lancement du groupe Auto Scaling doivent configurer les EC2 instances de manière à ce qu'elles nécessitent la version 2 du service de métadonnées					Mise à l'échelle automatique.3		Mise à l'échelle automatique.3

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
d'instance (IMDSv2)							
ASR-CreateCloudTrailMultiRegionTrail CloudTrail doit être activé et configuré avec au moins un parcours multirégional	CloudTrail1.	2.1	CloudTrail2.	3.1	CloudTrail1.	3.1	CloudTrail1.
ASR-EnableEncryption CloudTrail le chiffrement au repos doit être activé	CloudTrail2.	2.7	CloudTrail1.	3.7	CloudTrail2.	3,5	CloudTrail2.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-EnableLogFileValidation Assurez-vous que la validation du fichier CloudTrail journal est activée	CloudTrail4.	2.2	CloudTrail3.	3.2	CloudTrail4.		CloudTrail4.
ASR-EnableCloudTrailToCloudWatchLogging Assurez-vous que les CloudTrail sentiers sont intégrés à Amazon CloudWatch Logs	CloudTrail5.	2,4	CloudTrail4.	3.4	CloudTrail5.		CloudTrail5.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR - Configure 3 BucketLogging Assurez-vous que la journalisation des accès au compartiment S3 est activée sur le compartiment CloudTrail S3		2.6		3.6		3.4	CloudTrail7.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-ReplaceCodeBuildClearTextCredentials CodeBuild les variables d'environnement du projet ne doivent pas contenir d'informations d'identification en texte clair	CodeBuild 2.		CodeBuild 2.		CodeBuild 2.		CodeBuild 2.
Activation ASR AWSConfig Assurez-vous qu'AWS Config est activé	Config.1	2,5	Config.1	3,5	Config.1	3.3	Config.1

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-Make Private EBSSnapshots Les instantanés Amazon EBS ne doivent pas être restaurables publiquement	EC21.		EC21.		EC21.		EC21.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-Supprimer VPCDefaultSecurityGroupRules Le groupe de sécurité VPC par défaut doit interdire le trafic entrant et sortant	EC22.	4.3	EC22.	5.3	EC22.	5.4	EC22.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
Journaux compatibles avec l'ASR VPCFlow La journalisation des flux VPC doit être activée dans tous les cas VPCs	EC26.	2.9	EC26.	3.9	EC26.	3.7	EC26.
ASR-EnableEbsEncryptionByDefault Le chiffrement par défaut EBS doit être activé	EC27.	2.2.1			EC27.	2.2.1	EC27.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-RevokeUnrotatedKeys Les clés d'accès des utilisateurs doivent être renouvelées tous les 90 jours ou moins	IAM.3	1.4		1.14	IAM.3	1.14	IAM.3
Politique IAMPassword ASR-Set Politique de mot de passe par défaut d'IAM	IAM.7	1,5-1,11	IAM.8	1.8	IAM.7	1.8	IAM.7

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
RevokeUnusedIAMUserACCRÉDITATIONS ASR Les informations d'identification de l'utilisateur doivent être désactivées si elles ne sont pas utilisées dans les 90 jours	IAM.8	1.3	IAM.7		IAM.8		IAM.8

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
RevokeUnusedIAMUserACCRÉDITATIONS ASR Les informations d'identification de l'utilisateur doivent être désactivées si elles ne sont pas utilisées dans les 45 jours.				1.12		1.12	IAM.22

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-RemoveLambdaPublicAccess Les fonctions Lambda devraient interdire l'accès public	Lambda.1		Lambda.1		Lambda.1		Lambda.1
ASR-MakePrivateRDSSnapshot Les instantanés RDS doivent interdire l'accès public	RDS.1		RDS.1		RDS.1		RDS.1

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-DisablePublicAccessToRDSInstance Les instances de base de données RDS doivent interdire l'accès public	RDS.2		RDS.2		RDS.2	2.3.3	RDS.2

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
Cryptage ASR RDSSnapshot Les instantanés du cluster RDS et les instantanés de base de données doivent être chiffrés au repos	RDS.4				RDS.4		RDS.4

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-EnableMulti AZOnRDSInstance Les instances de base de données RDS doivent être configurées avec plusieurs zones de disponibilité	RDS.5				RDS.5		RDS.5

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-EnableEnhancedMonitoringOnRDSInstance Une surveillance améliorée doit être configurée pour les instances et les clusters de base de données RDS	RDS.6				RDS.6		RDS.6

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
Activation ASR RDSClusterDeletionProtection La protection contre la suppression des clusters RDS doit être activée	RDS.7				RDS.7		RDS.7

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
Activation ASR RDSInstance DeletionProtection La protection contre la suppression des instances de base de données RDS doit être activée	RDS.8				RDS.8		RDS.8

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-EnableMinorVersionUpgradeOnRDSDBInstance Les mises à niveau automatiques des versions mineures de RDS doivent être activées	RDS.13				RDS.13	2.3.2	RDS.13

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-EnableCopyTagsToSnapshotOnRDSCluster Les clusters de base de données RDS doivent être configurés pour copier des balises dans des instantanés	RDS.16				RDS.16		RDS.16

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-DisablePublicAccessToRedshiftCluster Les clusters Amazon Redshift devraient interdire l'accès public	Redshift.1		Redshift.1		Redshift.1		Redshift.1

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-EnableAutomaticSnapshotsOnRedshiftCluster Les snapshots automatiques doivent être activés sur les clusters Amazon Redshift	Redshift.3				Redshift.3		Redshift.3

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-EnableRedshiftClusterAuditLogging La journalisation des audits doit être activée sur les clusters Amazon Redshift	Redshift.4				Redshift.4		Redshift.4

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-EnableAutomaticVersionUpgradeOnRedshiftCluster Amazon Redshift devrait activer les mises à niveau automatiques vers les versions majeures	Redshift.6				Redshift.6		Redshift.6
ASR - Configure3PublicAccessBlock Le paramètre S3 Block Public Access doit être activé	S3.1	2.3	S3.6	2.1.5.1	S3.1	2.1.4	S3.1

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR - Configure 3 BucketPublicAccessBlock Les compartiments S3 devraient interdire l'accès public à la lecture	S3.2		S3.2	2.1.5.2	S3.2		S3.2
ASR - Configure 3 BucketPublicAccessBlock Les compartiments S3 devraient interdire l'accès public en écriture		S3.3					S3.3

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
EnableDefaultEncryptionASR-S3 Le chiffrement côté serveur doit être activé dans les compartiments S3	S3.4		S3.4	2.1.1	S3.4		S3.4
PolitiqueSSLBucketASR-Set Les compartiments S3 doivent nécessiter des demandes d'utilisation du protocole SSL	S3.5		S3.5	2.1.2	S3.5	2.1.1	S3.5

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-S3 BlockDenylist Les autorisations Amazon S3 accordées à d'autres comptes AWS dans les politiques de compartiment doivent être limitées	S3.6				S3.6		S3.6

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
Le paramètre S3 Block Public Access doit être activé au niveau du bucket	S3.8				S3.8		S3.8
ASR - Configure 3 BucketPublicAccessBlock Assurez-vous que les CloudTrail logs du compartiment S3 ne sont pas accessibles au public		2.3					CloudTrail6.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-CreateAccessLoggingBucket Assurez-vous que la journalisation des accès au compartiment S3 est activée sur le compartiment CloudTrail S3		2.6					CloudTrail7.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-EnableKeyRotation Assurez-vous que la rotation pour les applications créées par le client CMKs est activée		2,8	KMS.1	3.8	KMS.4	3.6	KMS.4

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-CreateLogMetricFilterAndAlarm Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les appels d'API non autorisés		3.1		4.1			Cloudwatch 1

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-CreateLogMetricFilterAndAlarm Assurez-vous qu'un journal, un filtre métrique et une alarme existent pour la connexion à AWS Management Console sans MFA		3.2		4.2			Cloudwatch 2

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-CreateLogMetricFilterAndAlarm Assurez-vous qu'un journal, un filtre métrique et une alarme existent pour l'utilisation de l'utilisateur « root »		3.3	CW.1	4.3			Cloudwatch 3

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-CreateLogMetricFilterAndAlarm Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications de politique IAM		3.4		4,4			Cloudwatch 4

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-CreateLogMetricFilterAndAlarm Assurez-vous qu'un journal, un filtre métrique et une alarme existent pour les modifications CloudTrail de configuration.		3,5		4,5			Cloudwatch 5

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-CreateLogMetricFilterAndAlarm Assurez-vous qu'un journal, un filtre métrique et une alarme existent en cas d'échec de l'authentification de l'AWS Management Console.		3.6		4.6			Cloudwatch 6

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-CreateLogMetricFilterAndAlarm Assurez-vous qu'un journal, un filtre métrique et une alarme existent pour la désactivation ou la suppression planifiée des fichiers créés par le client CMKs		3.7		4,7			Cloudwatch.7

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-CreateLogMetricFilterAndAlarm Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications de politique de compartiment S3		3.8		4.8			Cloudwatch.8

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-CreateLogMetricFilterAndAlarm Assurez-vous qu'un journal, un filtre métrique et une alarme existent pour les modifications de configuration d'AWS Config.		3.9		4,9			Cloudwatch.9

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-CreateLogMetricFilterAndAlarm Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications des groupes de sécurité		3,10		4,10			Cloudwatch.10

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-CreateLogMetricFilterAndAlarm Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications des listes de contrôle d'accès réseau (ACL réseau)		3,11		4,11			Cloudwatch.11

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-CreateLogMetricFilterAndAlarm Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications des passerelles réseau		3,12		4,12			Cloudwatch.12

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-CreateLogMetricFilterAndAlarm Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications des tables de routage		3.13		4,13			Cloudwatch.13

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-CreateLogMetricFilterAndAlarm Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications VPC		3,14		4,14			Cloudwatch.14

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
AWS-DisablePublicAccessForSecurityGroup Assurez-vous qu'aucun groupe de sécurité n'autorise l'entrée entre 0.0.0.0/0 et le port 22		4.1	EC25.		EC2.13		EC2.13

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
AWS-DisablePublicAccessForSecurityGroup Assurez-vous qu'aucun groupe de sécurité n'autorise l'entrée entre 0.0.0.0/0 et le port 3389		4.2			EC2.14		EC2.14
Configuration ASR SNSTopicForStack	CloudFormation1.				CloudFormation1.		CloudFormation1.
Rôle ASR-CreateIAMSupport		1,20		1,17		1,17	IAM.18

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-DisablePublicIPAutoAttribuer EC2 Les sous-réseaux Amazon ne doivent pas attribuer automatiquement d'adresses IP publiques	EC2.15				EC2.15		EC2.15
ASR-EnableCloudTrailLogFileValidation	CloudTrail4.	2.2	CloudTrail3.	3.2			CloudTrail4.
ASR-EnableEncryptionFor SNSTopic	SNS.1				SNS.1		SNS.1

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-EnableDeliveryStatusLoggingForSNSTopic L'enregistrement de l'état de livraison doit être activé pour les messages de notification envoyés à un sujet	SNS.2				SNS.2		SNS.2
ASR-EnableEncryptionFor SQSQueue	SQS.1				SQS.1		SQS.1

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
L'instantané RDS RDSSnapshotprivé d'ASR-Make doit être privé	RDS.1		RDS.1				RDS.1
Bloc ASR SSMDocument PublicAccess Les documents SSM ne doivent pas être publics	SSM.4				SSM.4		SSM.4

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-EnableCloudFrontDefaultRootObject CloudFront les distributions doivent avoir un objet racine par défaut configuré	CloudFront1.				CloudFront1.		CloudFront1.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-SetCloudFrontOriginDomain CloudFront les distributions ne doivent pas pointer vers des origines S3 inexistantes	CloudFront.12				CloudFront.12		CloudFront.12

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-RemoveCodeBuildPrivilegedMode CodeBuild les environnements de projet doivent disposer d'une configuration AWS de journalisation	CodeBuild 5.				CodeBuild 5.		CodeBuild 5.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
Instance ASR Terminer EC2 EC2 Les instances arrêtées doivent être supprimées après une période spécifiée	EC24.				EC24.		EC24.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
Activation ASR IMDSV2 OnInstance EC2 les instances doivent utiliser le service de métadonnées d'instance version 2 (IMDSv2)	EC28.				EC28.	5.6	EC28.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-RevokeUnauthorizedInboudRules Les groupes de sécurité ne doivent autoriser le trafic entrant illimité que pour les ports autorisés	EC2.18				EC2.18		EC2.18

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
INSÉREZ LE TITRE ICI Les groupes de sécurité ne doivent pas autoriser un accès illimité aux ports présentant un risque élevé	EC2.19				EC2.19		EC2.19

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
Désactiver l'ASR TGWAutoAcceptSharedAttachments Amazon EC2 Transit Gateways ne doit pas accepter automatiquement les demandes de pièces jointes VPC	EC2.23				EC2.23		EC2.23

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-EnablePrivateRepositoryScanning La numérisation des images doit être configurée dans les référentiels privés ECR	ECR.1				ECR.1		ECR.1
ASR-EnableGuardDuty GuardDuty doit être activé	GuardDuty 1.		GuardDuty 1.		GuardDuty 1.		GuardDuty 1.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR - Configure 3 BucketLogging La journalisation des accès au serveur de compartiments S3 doit être activée	S3.9				S3.9		S3.9

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-EnableBucketEventNotifications Les notifications d'événements doivent être activées dans les compartiments S3	S3.11				S3.11		S3.11

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
Ensembles ASR 3 Lifecycle Policy Les politiques de cycle de vie des compartiments S3 doivent être configurées	S3.13				S3.13		S3.13

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-EnableAutoSecretRotation La rotation automatique des secrets des secrets du Gestionnaire de secrets doit être activée	SecretsManager1.				SecretsManager1.		SecretsManager1.
ASR-RemoveUnsedSecret Supprimer les secrets inutilisés de Secrets Manager	SecretsManager3.				SecretsManager3.		SecretsManager3.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-UpdateSecretRotationPeriod Les secrets de Secrets Manager doivent faire l'objet d'une rotation dans un délai spécifié	SecretsManager4.				SecretsManager4.		SecretsManager4.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
Activation ASR APIGateway CacheDataEncryption Les données du cache de l'API REST API Gateway doivent être chiffrées au repos					APIGateway5.		APIGateway5.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-SetLogGroupRetentionDays CloudWatch les groupes de journaux doivent être conservés pendant une période spécifiée					CloudWatch.16		CloudWatch.16

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-AttachService VPCEndpoint Amazon EC2 doit être configuré pour utiliser les points de terminaison VPC créés pour le service Amazon EC2	EC2.10				EC2.10		EC2.10
ASR-TagGuardDutyResource GuardDuty les filtres doivent être étiquetés							GuardDuty 2.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-TagGuardDutyResource GuardDuty les détecteurs doivent être étiquetés							GuardDuty 4.
ASR - Attacher SSMPermissions à EC2 EC2 Les instances Amazon doivent être gérées par Systems Manager	SSM.1		SSM.3				SSM.1

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-ConfigureLaunchConfigNoPublicIPDocument EC2 Les instances Amazon lancées à l'aide des configurations de lancement de groupe Auto Scaling ne doivent pas avoir d'adresse IP publique					Autoscaling.5		Autoscaling.5

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
Activation ASR APIGateway Execution Logs	APIGateway1.						APIGateway1.
ASR-EnableMacie Amazon Macie devrait être activé	Macie.1				Macie.1		Macie.1
ASR-EnableAthenaWorkGroupLogging La journalisation des groupes de travail Athena doit être activée	Athéna.4						Athéna.4

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-Enforce LAB HTTPSFor Application Load Balancer doit être configuré pour rediriger toutes les requêtes HTTP vers HTTPS	ELB.1		ELB.1		ELB.1		ELB.1

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
Limite ASR ECSRootFilesystemAccess Les conteneurs ECS doivent être limités à l'accès en lecture seule aux systèmes de fichiers racines	ECS.5				ECS.5		ECS.5

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-EnableElastiCacheBackups ElastiCache Les sauvegardes automatiques des clusters (Redis OSS) doivent être activées	ElastiCache1.				ElastiCache1.		ElastiCache1.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-EnableElastiCacheVersionUpgrades ElastiCache les mises à niveau automatiques des versions mineures doivent être activées sur les clusters	ElastiCache2.				ElastiCache2.		ElastiCache2.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-EnableElastiCacheReplicationGroupFailover ElastiCache le basculement automatique doit être activé pour les groupes de réplication	ElastiCache3.				ElastiCache3.		ElastiCache3.

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
ASR-Configure DynamoDBAuto Mise à l'échelle Les tables DynamoDB doivent automatiquement adapter la capacité à la demande	DynamoDB.1				DynamoDB.1		DynamoDB.1
TagDynamoDBTableResource ASR Les tables DynamoDB doivent être balisées							DynamoDB.5

Description	AWS FSBP	CIS v1.2.0	PCI v3.2.1	CIS v1.4.0	NIST	CIS v3.0.0	ID de contrôle de sécurité
EnableDynamoDBDeletionProtection ASR La protection contre la suppression des tables DynamoDB doit être activée					Dynamo DB.6		Dynamo DB.6

Ajouter de nouvelles mesures correctives

Les corrections peuvent être ajoutées manuellement en mettant à jour les fichiers playbook appropriés, ou par programmation en étendant la solution via des constructions CDK, en fonction de votre flux de travail préféré.

> **Note**
>
> Les instructions qui suivent utilisent les ressources installées par la solution comme point de départ. Par convention, la plupart des noms de ressources de solutions contiennent l'ASR and/or SO0111 afin de faciliter leur localisation et leur identification.

Vue d'ensemble du flux de travail manuel

La réponse de sécurité automatisée sur les runbooks AWS doit suivre la dénomination standard suivante :

ASR- *<standard>* - *<version>* - *<control>*

Standard : Abréviation de la norme de sécurité. Cela doit correspondre aux normes prises en charge par l'ASR. Il doit s'agir de l'une des catégories « CIS », « AFSBP », « PCI », « NIST » ou « SC ».

Version : version de la norme. Encore une fois, cela doit correspondre à la version prise en charge par ASR et à la version figurant dans les données de recherche.

Contrôle : ID du contrôle à corriger. Cela doit correspondre aux données de recherche.

1. Créez un runbook sur le (s) compte (s) membre (s).
2. Créez un rôle IAM dans le (s) compte (s) membre (s).
3. (Facultatif) Créez une règle de correction automatique dans le compte administrateur.

Étape 1. Créez un runbook sur le (s) compte (s) membre (s)

1. Connectez-vous à la console AWS Systems Manager et obtenez un exemple du JSON trouvé.
2. Créez un runbook d'automatisation qui corrige le résultat. Dans l'onglet Owned by me, utilisez l'un des `ASR-` documents de l'onglet Documents comme point de départ.
3. Les AWS Step Functions du compte administrateur exécuteront votre runbook. Votre runbook doit spécifier le rôle de correction afin d'être transmis lors de l'appel du runbook.

Étape 2. Création d'un rôle IAM dans le ou les comptes membres

1. Connectez-vous à la console AWS Identity and Access Management.
2. Obtenez un exemple à partir des rôles IAM SO0111 et créez un nouveau rôle. Le nom du rôle doit commencer par SO0111-Remediate- - -. *<standard>* *<version>* *<control>* Par exemple, si vous ajoutez le contrôle 5.6 CIS v1.2.0, le rôle doit être`SO0111-Remediate-CIS-1.2.0-5.6`.
3. À l'aide de cet exemple, créez un rôle correctement défini qui autorise uniquement les appels d'API nécessaires pour effectuer la correction.

À ce stade, votre correction est active et disponible pour une correction automatique à partir de l'action personnalisée ASR dans AWS Security Hub.

Étape 3 : (Facultatif) Créez une règle de correction automatique dans le compte administrateur

La correction automatique (et non « automatisée ») est l'exécution immédiate de la correction dès que le résultat est reçu par AWS Security Hub. Réfléchissez bien aux risques avant d'utiliser cette option.

1. Consultez un exemple de règle pour la même norme de sécurité dans CloudWatch Events. La norme de dénomination pour les règles est`standard_control_*AutoTrigger*`.
2. Copiez le modèle d'événement de l'exemple à utiliser.
3. Modifiez la `GeneratorId` valeur pour qu'elle corresponde `GeneratorId` à celle de votre Finding JSON.
4. Enregistrez et activez la règle.

Présentation du flux de travail CDK

En résumé, les fichiers suivants du dépôt ASR seront modifiés ou ajoutés. Dans cet exemple, une nouvelle correction pour la version ElastiCache 2 a été ajoutée aux playbooks SC et AFSBP.

> **Note**
>
> Toutes les nouvelles corrections doivent être ajoutées au playbook SC, car il consolide toutes les corrections disponibles dans ASR. Si vous avez l'intention de déployer uniquement un ensemble spécifique de playbooks (par exemple, AFSBP), vous pouvez soit : (1) ajouter la correction uniquement aux playbooks que vous souhaitez, soit (2) ajouter la correction à tous les playbooks pour lesquels elle existe dans le Security Hub Standard correspondant, en plus du playbook SC. La deuxième option est recommandée pour des raisons de flexibilité.

Dans cet exemple, la norme ElastiCache .2 est incluse dans les normes Security Hub suivantes :

- AFSBP
- NIST.800-53.R5 SI-2
- NIST.800-53.R5 SI-2 (2)

- NIST.800-53.R5 SI-2 (4)
- NIST.800-53.R5 SI-2 (5)
- PCI DSS v4.0.1/6.3.3

Étant donné que, par défaut, ASR n'implémente que les playbooks pour AFSBP et NIST.800-53, nous ajouterons cette nouvelle correction à ces playbooks en plus du SC.

Modify

- source/lib/remediation-runbook-stack.ts
- source/playbooks/AFSBP/lib/[nom standard] _remediations.ts
- source/playbooks/NIST80053/lib/control_runbooks-construct.ts
- source/playbooks/NIST80053/lib/[nom standard] _remediations.ts
- source/playbooks/SC/lib/control_runbooks-construct.ts
- source/playbooks/SC/lib/sc_remediations.ts
- source/test/regex_registry.ts

Addition

- source/playbooks/SC/ssmdocs/SC_ ElastiCache .2.ts
- source/playbooks/SC/ssmdocs/descriptions/ElastiCache2.md
- source/remediation_runbooks/EnableElastiCacheVersionUpgrades.yaml

> **Note**
>
> Le nom choisi pour le runbook peut être n'importe quelle chaîne, à condition qu'il soit cohérent avec le reste des modifications apportées.

- source/playbooks/NIST80053/ssmdocs/NIST80053_ 2.ts ElastiCache
- source/playbooks/AFSBP/ssmdocs/AFSBP_ ElastiCache .2.yaml

Étapes de développement

1. Créez le manuel de correction.
2. Créez les Control Runbooks.
3. Intégrez chaque Control Runbook à un Playbook.
4. Création du rôle IAM de correction et intégration du manuel de correction
5. Mettre à jour les tests unitaires

Étape 1 : Création du runbook de correction

Il s'agit du document SSM utilisé pour corriger les ressources. Il doit inclure le `AutomationAssumeRole` paramètre, qui est le rôle IAM autorisé à exécuter la correction. Affichez le fichier existant `source/remediation_runbooks/EnableElastiCacheVersionUpgrades.yaml` comme référence lors de la création de nouveaux runbooks de correction.

Tous les nouveaux runbooks doivent être ajoutés au `source/remediation_runbooks/` répertoire.

Étape 2 : Création des Control Runbooks

Un runbook de contrôle est un runbook spécifique au playbook qui analyse les données de recherche issues de la norme donnée et exécute le runbook de correction approprié. Étant donné que nous ajoutons la correction ElastiCache .2 aux playbooks SC, AFSBP et NIST8 0053, nous devons créer un nouveau runbook de contrôle pour chacun d'eux. Les fichiers suivants sont créés :

- source/playbooks/SC/ssmdocs/SC_ ElastiCache .2.ts
- source/playbooks/NIST80053/ssmdocs/NIST80053_ 2.ts ElastiCache
- source/playbooks/AFSBP/ssmdocs/AFSBP_ ElastiCache .2.yaml

Example

Le nom de ces fichiers est important et doit suivre le format <PLAYBOOK_NAME>_ <CONTROL.ID>.ts/yaml

Certains playbooks en ASR prennent en charge les runbooks de contrôle iAC TypeScript, tandis que d'autres doivent être écrits en YAML brut. Référez-vous aux correctifs existants dans le playbook correspondant à titre d'exemples. Dans cet exemple, nous aborderons le playbook SC, qui utilise IaC.

Dans le playbook SC, votre nouveau runbook de contrôle doit exporter une classe qui étend ControlRunbookDocument et correspond au nom de votre runbook de remédiation. Regardez l'exemple ci-dessous :

```
export class EnableElastiCacheVersionUpgrades extends ControlRunbookDocument {
  constructor(scope: Construct, id: string, props: ControlRunbookProps) {
    super(scope, id, {
      ...props,
      securityControlId: 'ElastiCache.2',
      remediationName: 'EnableElastiCacheVersionUpgrades',
      scope: RemediationScope.REGIONAL,
      resourceIdRegex: <Regex>,
      resourceIdName: 'ClusterId',
      updateDescription: new StringFormat('Automatic minor version upgrades enabled for
 cluster %s.', [
        StringVariable.of(`ParseInput.ClusterId`),
      ]),
    });
  }
}
```

- `securityControlId`est l'ID de contrôle pour la correction que vous ajoutez, tel qu'il est défini dans la vue des contrôles consolidés de Security Hub.
- `remediationName`est le nom que vous avez choisi pour votre manuel de remédiation.
- `scope`représente l'étendue de la ressource que vous êtes en train de corriger, en indiquant si elle existe dans le monde entier ou dans une région spécifique.
- `resourceIdRegex`est l'expression régulière utilisée pour capturer l'ID de ressource que vous souhaitez transmettre au runbook de correction en tant que paramètre. Un seul groupe doit être capturé, tous les autres groupes ne doivent pas être capturés. Si vous souhaitez transmettre l'intégralité de l'ARN, omettez ce champ.
- `resourceIdName`est le nom que vous souhaitez définir pour l'ID de ressource capturé. Il doit correspondre au nom du paramètre d'ID de ressource dans votre manuel de correction. `resourceIdRegex`
- `updateDescription`est la chaîne que vous souhaitez attribuer à la section « notes » de la recherche dans Security Hub une fois la correction réussie.

Vous devez également exporter une fonction appelée `createControlRunbook` qui renvoie une nouvelle instance de votre classe. Pour la ElastiCache version 2, cela ressemble à :

```
export function createControlRunbook(scope: Construct, id: string, props:
 PlaybookProps): ControlRunbookDocument {
  return new EnableElastiCacheVersionUpgrades(scope, id, { ...props, controlId:
 'ElastiCache.2' });
}
```

où `controlId` est l'ID de contrôle tel que défini dans la norme de sécurité associée au playbook sous lequel vous opérez.

Si le contrôle Security Hub contient des paramètres que vous souhaitez transmettre à votre runbook de correction, vous pouvez les transmettre en ajoutant des remplacements aux méthodes suivantes : - `getExtraSteps` : définit les valeurs par défaut pour chaque paramètre implémenté pour le contrôle dans Security Hub

> **Note**
>
> Chaque paramètre de Security Hub doit recevoir une valeur par défaut

- `getInputParamsStepOutput`: définit les sorties pour l' GetInputParams étape du runbook de contrôle
- Chaque sortie possède un `nameoutputType`, et`selector`. `selector`Il doit s'agir du même sélecteur que celui utilisé dans le remplacement de la `getExtraSteps` méthode.
- `getRemediationParams`: définit les paramètres transmis au runbook de correction, extraits des résultats de l' GetInputParams étape.

Pour voir un exemple, accédez au `source/playbooks/SC/ssmdocs/SC_DynamoDB.1.ts` fichier.

Étape 3 : Intégrer chaque Control Runbook à un Playbook

Pour chaque runbook de contrôle créé à l'étape précédente, vous devez désormais l'intégrer aux définitions d'infrastructure du playbook associé. Suivez les étapes ci-dessous pour chaque runbook de contrôle.

> **Important**
>
> Si vous avez créé le runbook de contrôle en utilisant du code YAML brut au lieu du texte dactylographié IAc, passez à la section suivante.

Dans `/<playbook_name>/control_runbooks-construct.ts` Importer votre nouveau fichier runbook de contrôle, tel que :

```
import * as elasticache_2 from '../ssmdocs/SC_ElastiCache.2';
```

Ensuite, accédez au tableau pour

```
const controlRunbooksRecord: Record<string, any>
```

Et ajoutez une nouvelle entrée mappant l'ID de contrôle (spécifique au playbook) à la `createControlRunbook` méthode que vous avez créée :

```
'ElastiCache.2': elasticache_2.createControlRunbook,
```

Ajoutez l'ID de contrôle spécifique au playbook à la liste des corrections comme ci-dessous : `<playbook_name>\_remediations.ts`

```
{ control: 'ElastiCache.2', versionAdded: '2.3.0' },
```

Le `versionAdded` champ doit être la dernière version de la solution. Si l'ajout de la correction dépasse la limite de taille du modèle, augmentez le`versionAdded`. Vous pouvez ajuster le nombre de corrections incluses dans la pile de chaque membre du playbook. `solution_env.sh`

Étape 4 : Création du rôle IAM de correction et intégration du runbook de correction

Chaque correction possède son propre rôle IAM avec des autorisations personnalisées requises pour exécuter le runbook de correction. En outre, la `RunbookFactory.createRemediationRunbook` méthode doit être invoquée pour ajouter le runbook de correction que vous avez créé à l'étape 1 aux modèles de CloudFormation la solution.

Dans le`remediation-runook-stack.ts`, chaque correction possède son propre bloc de code dans la `RemediationRunbookStack` classe. Le bloc de code suivant montre la création d'un nouveau rôle IAM et l'intégration du runbook de correction pour la ElastiCache correction .2 :

```
    //-----------------------
    // EnableElastiCacheVersionUpgrades
    //
    {
      const remediationName = 'EnableElastiCacheVersionUpgrades'; // should match the
 name of your remediation runbook
      const inlinePolicy = new Policy(props.roleStack, `ASR-Remediation-Policy-
${remediationName}`);

      const remediationPolicy = new PolicyStatement();
      remediationPolicy.addActions('elasticache:ModifyCacheCluster');
      remediationPolicy.effect = Effect.ALLOW;
      remediationPolicy.addResources(`arn:${this.partition}:elasticache:*:
${this.account}:cluster:*`);
      inlinePolicy.addStatements(remediationPolicy);

      new SsmRole(props.roleStack, 'RemediationRole ' + remediationName, { // creates
 the remediation IAM role
        solutionId: props.solutionId,
        ssmDocName: remediationName,
        remediationPolicy: inlinePolicy,
        remediationRoleName: `${remediationRoleNameBase}${remediationName}`,
      });

      RunbookFactory.createRemediationRunbook(this, 'ASR ' + remediationName, { // adds
 the remediation runbook to the solution's cloudformation templates
        ssmDocName: remediationName,
        ssmDocPath: ssmdocs,
        ssmDocFileName: `${remediationName}.yaml`,
        scriptPath: `${ssmdocs}/scripts`,
        solutionVersion: props.solutionVersion,
        solutionDistBucket: props.solutionDistBucket,
        solutionId: props.solutionId,
        namespace: namespace,
      });
    }
```

Étape 5 : Mettre à jour les tests unitaires

Nous vous recommandons de mettre à jour et d'exécuter les tests unitaires après avoir ajouté une nouvelle correction.

Tout d'abord, vous devez ajouter de nouvelles expressions régulières (qui ne sont pas déjà ajoutées) dans le `source/test/regex_registry.ts` fichier. Ce fichier impose des tests pour chaque nouvelle expression régulière incluse dans les runbooks de la solution. Examinez l'exemple de la `addElastiCacheClusterTestCases` fonction, qui est utilisée pour tester les expressions régulières utilisées dans ElastiCache les corrections.

Enfin, vous devez mettre à jour les instantanés pour chaque pile. Les instantanés sont des définitions de CloudFormation modèles contrôlées par version qui sont utilisées pour suivre les modifications apportées à l'infrastructure d'ASR. Vous pouvez mettre à jour ces fichiers instantanés en exécutant la commande suivante depuis le `deployment` répertoire :

```
./run-unit-tests.sh update
```

Vous êtes maintenant prêt à déployer votre nouvelle solution ! Accédez à la section Création et déploiement ci-dessous pour obtenir des instructions sur la création et le déploiement de la solution avec vos nouvelles modifications.

Ajouter un nouveau playbook

Téléchargez les manuels de la solution Automated Security Response on AWS et le code source de déploiement depuis le GitHub référentiel.

Les CloudFormation ressources AWS sont créées à partir des composants AWS CDK, et elles contiennent le code du modèle de playbook que vous pouvez utiliser pour créer et configurer de nouveaux playbooks. Pour plus d'informations sur la configuration de votre projet et la personnalisation de vos playbooks, consultez le fichier README.md dans. GitHub

AWS Systems Manager Parameter Store

Automated Security Response sur AWS utilise AWS Systems Manager Parameter Store pour le stockage des données opérationnelles. Les paramètres suivants sont enregistrés dans Parameter Store :

Name	Value	Utilisation
`/Solutions/SO0111/CMK_REMEDIATION_ARN`	Clé AWS KMS qui chiffrera les données pour les corrections du FSBP	Chiffrement des données clients, telles que CloudTrai

Name	Value	Utilisation
		l les journaux, dans le cadre des mesures correctives
/Solutions/SO0111/CMK_ARN	Clé AWS KMS qu'ASR utilisera pour chiffrer les données	Chiffrement des données de solution
/Solutions/SO0111/SNS_Topic_ARN	ARN de la rubrique Amazon SNS relative à la solution	Notification des événements de remédiation
/Solutions/SO0111/SNS_Topic_Config.1	Rubrique SNS pour les mises à jour d'AWS Config	Correction de la configuration 1
/Solutions/SO0111/version	Version de la solution	
/Solutions/SO0111/*<security standard long name>*/*<version>* /statut	enabled	Indique si le standard est actif dans la solution. Une norme peut être désactivée pour une correction automatique en la remplaçant par disabled
/Solutions/SO0111/*<security standard long name>*/shortname	String	Nom abrégé de la norme de sécurité. Par exemple :CIS,AFSBP, PCI
/Solutions/SO0111//*<security standard long name><version>* /*<control>* /remap	String	Lorsqu'un contrôle utilise la même correction qu'un autre, ces paramètres exécutent le remappage
/ASR/Filters/AccountFilterMode	Inclure, exclure ou désactiver	Contrôle le comportement de filtrage des identifiants de compte pour des corrections entièrement automatisées

Name	Value	Utilisation
`/ASR/Filters/AccountFilters`	Liste de comptes AWS séparée par des virgules IDs	Liste des comptes AWS IDs pour lesquels la solution doit filtrer les corrections automatisées.
`/ASR/Filters/OUFilterMode`	Inclure, exclure ou désactiver	Contrôle le comportement de filtrage des unités organisationnelles (OUs) pour des corrections entièrement automatisées
`/ASR/Filters/OUFilters`	Liste d'identifiants d'unités d'organisation séparés par des virgules	Liste des solutions OUs pour lesquelles la solution doit filtrer les corrections automatisées.
`/ASR/Filters/TagFilterMode`	Inclure, exclure ou désactiver	Contrôle le comportement de filtrage des balises de ressource pour des corrections entièrement automatisées
`/ASR/Filters/TagFilters`	Liste de clés de balises de ressources séparées par des virgules	Liste des clés de balise de ressource pour lesquelles la solution doit filtrer les corrections automatisées.

Rubrique Amazon SNS - Progression de la correction

Automated Security Response sur AWS crée une rubrique Amazon SNS, SO0111-ASR_Topic. Cette rubrique est utilisée pour publier des mises à jour sur la progression de la correction. Voici les trois notifications possibles envoyées à ce sujet.

```
Remediation queued for [.replaceable]`<standard>` control [.replaceable]`<control_ID>`
 in account [.replaceable]`<account_ID>`
```

```
Remediation failed for [.replaceable]`<standard>` control [.replaceable]`<control_ID>`
 in account [.replaceable]`<account_ID>`
```

```
[.replaceable]`<control_ID>` remediation was successfully invoke via AWS Systems
 Manager in account [.replaceable]`<account_ID>`
```

Il s'agit du message d'achèvement. Cela indique que la correction s'est terminée sans erreur ; toutefois, le test définitif pour une correction réussie est la validation and/or manuelle d'AWS Config check.

Filtrer un abonnement à une rubrique SNS

Politiques de filtrage des abonnements Amazon SNS :

1. Accédez à l'abonnement à la rubrique SNS.
2. Sous Politique de filtrage des abonnements, sélectionnez « Modifier ».
3. Développez « Politique de filtrage des abonnements » et activez l'option « Politique de filtrage des abonnements » pour activer les filtres.
4. Sélectionnez le champ « Corps du message ».
5. Ajoutez votre politique à l'éditeur JSON.
6. Enregistrez les modifications.

Exemples de politiques :

Filtrer par compte

```
{
"finding": {
"account": [
"111111111111",
"222222222222"
]
}
```

Filtrer les erreurs

```
{
"severity": ["ERROR"]
```

```
}
```

Filtrer par commandes

```
{
"finding": {
"standard_control": ["S3.9","S3.6"]
}
}
```

Rubrique Amazon SNS - Alarmes CloudWatch

Cette solution crée une rubrique Amazon SNS,. `S00111-ASR_Alarm_Topic` Cette rubrique est utilisée pour publier des alertes d'alarme.

Les détails de toutes les alarmes qui passent à l'état ALARM seront envoyés à cette rubrique.

Lancer Runbook sur la base des résultats de configuration

Cette solution peut lancer des runbooks en fonction des résultats personnalisés d'AWS Config. Pour ce faire, vous devez :

1. Trouvez le nom de la règle AWS Config que vous souhaitez corriger. Cela se trouve dans AWS Config ou dans le résultat généré par Security Hub pour cette règle.
2. Accédez à AWS Systems Manager Parameter Store et sélectionnez Create Parameter.
3. Le nom de votre règle doit être `/Solutions/S00111/` [.replaceable] `Rule name from Step 1`
4. La valeur doit être formatée comme suit :

```
{
"RunbookName":"Name of SSM runbook",
"RunbookRole": "Role that Orchestrator will assume"
}
```

1. RunbookName est un champ obligatoire et sera le runbook qui sera exécuté lorsque vous corrigerez cette règle de Config. RunbookRole est le rôle que l'orchestrateur assumera lors de

l'exécution de ce rôle. Ce champ n'est pas obligatoire, et s'il est omis, l'orchestrateur utilisera par défaut le rôle de membre du compte.

2. Une fois que cela est en place, vous pouvez corriger votre règle Config à l'aide de l'action personnalisée « Corriger avec ASR » disponible sur le Security Hub.

Interface utilisateur Web

L'interface utilisateur Web de la solution permet aux utilisateurs de corriger les résultats d'AWS Security Hub en un clic, de consulter et de télécharger les corrections précédentes et de déléguer l'accès à la solution.

L'interface utilisateur Web n'est pas requise pour utiliser la solution ; vous pouvez également configurer des corrections entièrement automatisées pour éviter de devoir les exécuter manuellement, ou utiliser la console AWS Security Hub CSPM pour lancer les corrections à l'aide de l'action personnalisée Remediate with ASR.

> **Note**
>
> Vous devez définir le `ShouldDeployWebUI` paramètre sur « yes » lors du déploiement de la pile d'administration afin d'utiliser l'interface utilisateur Web de la solution.

Comment ça marche

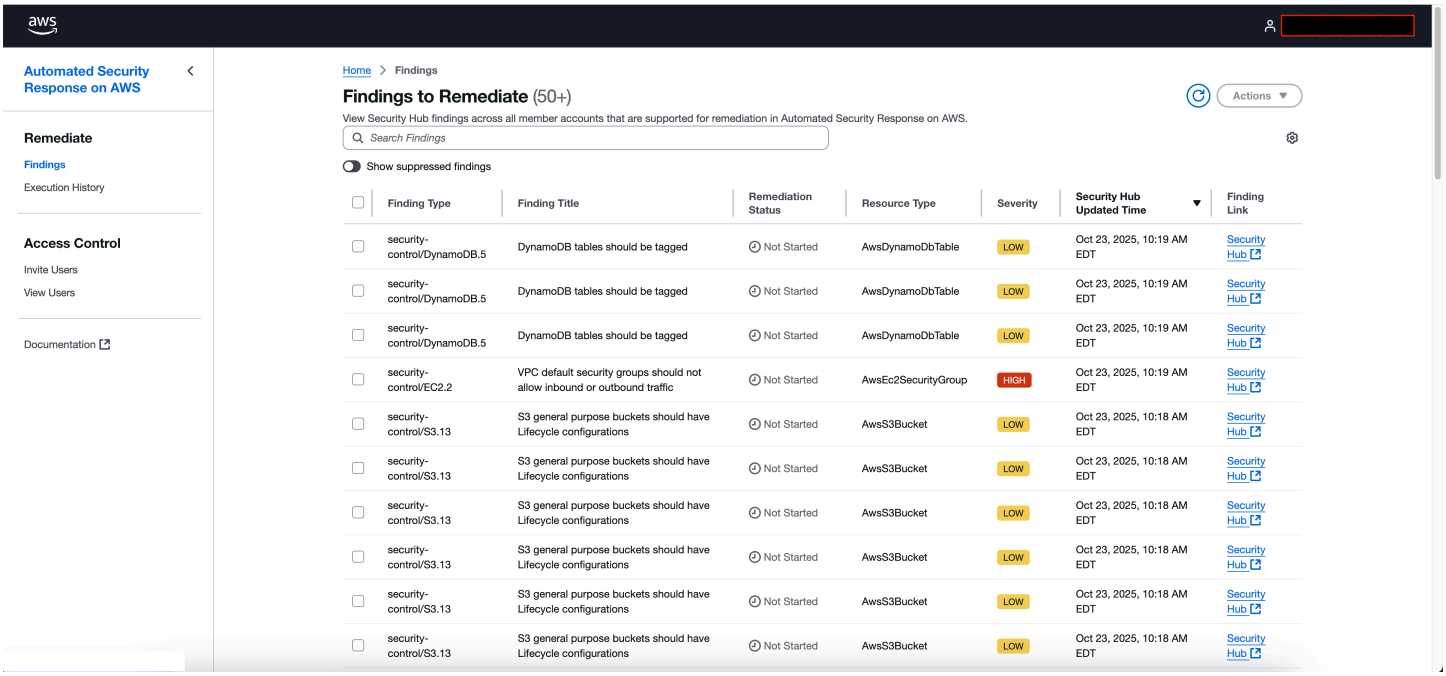
L'interface utilisateur Web de la solution est une application Web d'une seule page hébergée dans votre compte par Amazon S3 et distribuée par Amazon CloudFront. La solution déploie également une API REST à l'aide d'API Gateway pour prendre en charge les opérations dans l'interface utilisateur Web.

Lorsque la pile d'administration est déployée, les fonctions Lambda de la solution commencent à charger dans DynamoDB toutes les conclusions d'AWS Security Hub prises en charge par la solution et présentes dans votre compte d'administrateur. Une fois cette opération terminée, les résultats présentés dans l'interface utilisateur Web sont synchronisés avec Security Hub en temps quasi réel grâce aux EventBridge règles déployées par la solution.

Chaque semaine, les fonctions Lambda de la solution sont déclenchées pour actualiser la table DynamoDB contenant les résultats d'AWS Security Hub affichés dans l'interface utilisateur Web. Cela garantit que les données périmées sont nettoyées et que nos tables DynamoDB

sont conservées. up-to-date Si vous souhaitez configurer cette ligne de base pour qu'elle s'exécute plus ou moins souvent, modifiez la EventBridge règle nommée `SO0111-ASR-SynchronizationFindingsLambdaWeeklyRule` située dans votre compte d'administrateur dans la région où vous avez déployé la solution.

Exécutez les corrections directement dans l'interface utilisateur Web



Sur la page Conclusions, les utilisateurs administrateurs ou administrateurs délégués peuvent consulter toutes les conclusions d'AWS Security Hub prises en charge par la solution à des fins de correction. Cela inclut les résultats relatifs aux comptes membres du Security Hub intégrés au compte principal du Security Hub. Si la solution est également déployée dans la région d'agrégation, les résultats de n'importe quelle région intégrée seront également affichés. Pour consulter la liste des résultats étayés par la solution, consultez la section Playbooks.

Les utilisateurs des opérateurs de compte pourront uniquement consulter les résultats provenant des comptes AWS auxquels ils ont accès, comme indiqué dans leur invitation. En outre, ils ne pourront exécuter des corrections que pour les ressources des comptes auxquels ils sont associés.

Pour exécuter des corrections, sélectionnez autant d'éléments que vous le souhaitez dans le tableau et cliquez sur Actions > Corriger. Vous pouvez également supprimer les résultats en cliquant sur Actions > Supprimer, ce qui masque les résultats sélectionnés dans la vue par défaut. Vous pouvez consulter les résultats supprimés à tout moment en cliquant sur le bouton Afficher les résultats supprimés.

Une fois que vous avez entamé la correction d'une constatation, vous pouvez cliquer sur la colonne État de la correction pendant que la correction est en cours **`In Progress`** ou **`Failed`** pour accéder directement à cette correction sur la page Historique des exécutions.

Filtrer les résultats et les mesures correctives disponibles

Sur les pages Résultats et Historique des exécutions, vous pouvez filtrer les données affichées dans le tableau en fonction de l'une des colonnes présentes dans chaque tableau respectif.

Par exemple, sur la page Résultats, vous pouvez filtrer sur Type de recherche pour rechercher des types spécifiques de résultats AWS Security Hub (par exemple Lambda.1 ou Athena.4) en cliquant sur la barre de recherche et en sélectionnant Type de recherche.

> **Note**
>
> Les valeurs renseignées automatiquement dans la barre de recherche ne représentent pas une liste complète des données disponibles. Les valeurs suggérées pour chaque critère de recherche ne représentent que les données actuellement extraites et affichées dans l'interface utilisateur.

Vous pouvez également combiner plusieurs attributs dans une seule recherche. Par exemple, vous pouvez appliquer à la fois le type de recherche et l'identifiant de ressource à votre recherche pour effectuer une `AND` requête logique. En outre, vous pouvez appliquer plusieurs critères de filtre identiques pour effectuer une `OR` recherche logique, tels que Type de recherche = Lambda.1 et Type de recherche = Athena.4. Les mêmes principes s'appliquent à la page Historique des exécutions

Authentification et autorisation dans l'interface utilisateur Web

L'interface utilisateur Web de la solution est protégée par l'authentification fournie par Amazon Cognito. Lorsque la solution est déployée, un groupe d'utilisateurs Cognito, un client d'application Cognito et un domaine de groupe d'utilisateurs Cognito sont fournis et configurés parallèlement à l'interface utilisateur Web. L'adresse e-mail fournie en tant que paramètre à la pile d'administrateurs se voit attribuer des informations d'identification temporaires et un accès administrateur à l'interface utilisateur Web.

Il existe trois types d'autorisation qui définissent l'accès d'un utilisateur à l'interface utilisateur Web :

Type d'autorisation	Niveau d'accès	Cas d’utilisation
Admin	Contrôle total dans l'interfa ce utilisateur Web ; possibili té de visualiser tous les résultats et mesures correctiv es, d'exécuter n'importe quelle correction et de n' invite/view importe quel utilisateur.	Attribué uniquement à l'utilisa teur qui a déployé la pile d'administrateurs lorsqu'il fournit son adresse e-mail lors CloudFormation du déploieme nt.
Administrateur délégué	Contrôle élevé dans l'interfa ce utilisateur Web ; possibilité de consulter tous les résultats et les mesures correctives, d'exécuter toutes les mesures correctives et de consulter les utilisateurs de l'opérateur de invite/view compte. Impossibl e d'inviter ou de consulter les administrateurs et les administrateurs délégués dans l'interface utilisateur Web.	L'utilisateur administrateur peut déléguer l'accès à la solution en invitant des utilisateurs administrateurs délégués, qui seront en mesure d'exécuter et de gérer toutes les corrections.
Opérateur du compte	Contrôle limité dans l'interfa ce utilisateur Web ; limité à l'affichage et à la correctio n des résultats uniquement dans les comptes auxquels ils sont associés sur invitatio n. Impossible d'inviter ou de consulter d'autres utilisateurs.	Day-to-day utilisateurs qui devraient disposer d'un accès limité pour exécuter des corrections dans un sous-ense mble de comptes intégrés. Les administrateurs ou les administrateurs délégués sont chargés d'inviter ces utilisate urs et de définir leur champ d'application.

Tous les utilisateurs doivent être invités par un administrateur ou un administrateur délégué avant de pouvoir se connecter à l'interface utilisateur Web. Pour inviter des utilisateurs supplémentaires,

un administrateur ou un administrateur délégué peut saisir son adresse e-mail et son niveau d'autorisation sur la page Inviter des utilisateurs de l'interface utilisateur Web.

Les administrateurs et les administrateurs délégués peuvent également consulter, gérer et supprimer les utilisateurs existants. Pour voir la liste de tous les utilisateurs, accédez à la page Afficher les utilisateurs.

Pour gérer un utilisateur existant, sélectionnez-le dans le tableau et cliquez sur Gérer l'utilisateur. Vous pouvez ensuite supprimer l'utilisateur en cliquant sur Supprimer l'utilisateur. Si l'utilisateur est un opérateur de compte, vous pouvez modifier la liste des comptes AWS IDs auxquels il a accès dans le contexte de la solution. La modification du type d'autorisation pour un utilisateur existant n'est actuellement pas prise en charge.

Veuillez noter que les administrateurs délégués ne peuvent consulter et gérer que les utilisateurs des opérateurs de comptes.

Intégration avec des applications externes IdPs

Vous pouvez personnaliser le mécanisme d'authentification fourni par la solution pour permettre aux utilisateurs de se connecter à l'aide de votre propre fournisseur d'identité OIDC ou SAML, tel qu'Okta ou Microsoft Entra ID. Les étapes suivantes pour l'intégration avec des applications externes IdPs nécessitent l'accès au compte AWS sur lequel la pile d'administrateurs est déployée.

> **Important**
>
> Les utilisateurs doivent toujours être invités avant de se connecter à l'aide de tout IdP externe que vous configurez pour utiliser la solution. En outre, l'adresse e-mail associée à leur profil IdP doit correspondre à l'adresse e-mail fournie dans leur invitation.

Étape 1 - Localiser le groupe d'utilisateurs de la solution

Dans la console Amazon Cognito, localisez le groupe d'utilisateurs de la solution nommé SO0111-ASR -. UserPool

Cliquez sur le nom du groupe d'utilisateurs SO0111-ASR- UserPool pour accéder à la page d'aperçu. À partir de là, sélectionnez Fournisseurs sociaux et externes dans la barre de navigation.

Étape 2 - Ajoutez votre fournisseur d'identité

Sur la page Fournisseurs sociaux et externes, cliquez sur le bouton Ajouter un fournisseur d'identité en haut à droite.

Sélectionnez OIDC ou SAML, selon votre fournisseur d'identité.

Une fois que vous aurez sélectionné votre type de fournisseur, vous serez invité à saisir des informations sur votre fournisseur d'identité.

Renseignez les champs suivants pour les fournisseurs SAML :

1. Nom du fournisseur : un nom convivial pour votre fournisseur
2. Connexion SAML initiée par l'IDP : Sélectionnez `Require SP-initiated SAML assertions - Recommended`
3. Source du document de métadonnées : Sélectionnez `Upload metadata document`
4. Document de métadonnées : téléchargez le document de métadonnées SAML fourni par votre IdP.
5. Sous Cartographier les attributs entre votre fournisseur SAML et votre groupe d'utilisateurs, cliquez sur Ajouter un autre attribut. Pour l'attribut du groupe d'utilisateurs, `email` sélectionnez dans la liste déroulante. Pour l'attribut SAML, entrez le nom complet de l'attribut dans lequel l'adresse e-mail de l'utilisateur est enregistrée dans votre fournisseur d'identité SAML. Par exemple, `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`.
6. Cliquez sur Ajouter un fournisseur d'identité pour enregistrer vos modifications.

Remplissez les champs suivants pour les fournisseurs OIDC :

1. Nom du fournisseur : un nom convivial pour votre fournisseur
2. ID client : entrez l'identifiant client fourni par votre fournisseur d'identité OpenID Connect.
3. Secret client : entrez le secret client fourni par le fournisseur d'identité OpenID Connect.
4. Étendue autorisée : Entrez `openid profile email`
5. Méthode de demande d'attribut : sélectionnez `GET` ou `POST` en fonction de la configuration de votre fournisseur d'identité.
6. Méthode de configuration : sélectionnez `Auto fill through issuer URL` et entrez l'URL de l'émetteur de votre fournisseur OIDC. Vous pouvez également saisir les valeurs manuellement.
7. Sous Cartographier les attributs entre votre fournisseur OpenID Connect et votre groupe d'utilisateurs, cliquez sur Ajouter un autre attribut. Pour l'attribut du groupe d'utilisateurs, `email`

sélectionnez dans la liste déroulante. Pour l'attribut OpenID Connect, entrez le nom complet de l'attribut dans lequel l'adresse e-mail de l'utilisateur est enregistrée dans votre fournisseur d'identité OIDC. Par exemple, `email`.

8. Cliquez sur Ajouter un fournisseur d'identité pour enregistrer vos modifications.

> **Important**
>
> Vous devez ajouter un mappage d'attributs pour l'attribut du groupe `email` d'utilisateurs, même si le nom d'attribut de votre fournisseur d'identité l'est également`email`.

Étape 3 - Ajoutez votre fournisseur au client d'application de la solution

Accédez à la page App Clients et sélectionnez le client nommé SO0111-ASR-WebUI -. UserPoolClient

Cliquez sur l'onglet Pages de connexion, puis sous Configuration des pages de connexion gérées, cliquez sur Modifier.

Dans le champ Fournisseurs d'identité, ajoutez le fournisseur d'identité que vous avez créé à l'étape précédente. Cliquez sur Save Changes (Enregistrer les modifications).

Étape 4 - Configuration de votre fournisseur d'identité

Pour permettre à votre fournisseur d'identité de rediriger vers l'interface utilisateur Web de la solution après la connexion, vous devez autoriser les éléments suivants URLs dans la configuration de votre IdP.

En fonction de votre type de fournisseur, autorisez l'un des rappels URLs suivants :

1. URL de rappel SAML : https://so0111-asr - *<your-aws-account-id>* .auth. *<aws-region>*.amazoncognito. com/saml2/idpresponse
2. URL de rappel OIDC : https://so0111-asr - *<your-aws-account-id>* .auth. *<aws-region>*.amazoncognito. com/oauth2/idpresponse

Vous devez le `<your-aws-account-id>` remplacer par l'ID du compte AWS dans lequel vous avez déployé la pile d'administrateurs et `<aws-region>` par la région dans laquelle vous avez déployé la pile d'administrateurs.

Étape 4 - Vérifiez votre intégration

Accédez à la page de connexion de l'interface utilisateur Web. Vérifiez que votre fournisseur d'identité personnalisé est visible sur la page de connexion.

Pour tester l'intégration, invitez un nouvel utilisateur à l'aide de la page Inviter des utilisateurs. Assurez-vous ensuite que l'utilisateur peut s'authentifier en cliquant sur votre fournisseur d'identité personnalisé sur la page de connexion de l'interface utilisateur Web.

Notez que le profil de l'utilisateur dans votre IdP personnalisé doit être lié à la même adresse e-mail que celle indiquée dans son invitation. En d'autres termes, l'adresse e-mail figurant dans les réclamations de votre fournisseur doit correspondre à l'invitation.

Référence

Cette section inclut des informations sur une fonctionnalité facultative de collecte de données, des pointeurs vers des ressources connexes et une liste des créateurs qui ont contribué à cette solution.

Collecte des données

Cette solution envoie des métriques opérationnelles à AWS (les « données ») concernant l'utilisation de cette solution. Nous utilisons ces données pour mieux comprendre comment les clients utilisent cette solution et les services et produits associés. La collecte de ces données par AWS est soumise à l'avis de confidentialité d'AWS.

Ressources connexes

- Réponse et correction automatisées avec AWS Security Hub
- Benchmarks de CIS Amazon Web Services Foundations, version 1.2.0
- Norme relative aux meilleures pratiques de sécurité de base d'AWS
- Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS)
- Institut national des normes et de la technologie (NIST) SP 800-53 Rev. 5

Collaborateurs

Les personnes suivantes ont contribué à ce document :

- Mike O'Brien
- Nikhil Reddy
- Chandini Penmetsa
- Chaitanya Deolankar
- Max Granat
- Tim Mekari
- Aaron Schütter
- Andrew Yankowski
- Josh Moss

- Ryan Garay
- Thiemo Belméga
- Mykhailo Markhain
- Manish Jangid
- Andrew Stephen
- Peter DeVries
- Mukta Dadariya

Révisions

Date de publication : août 2020 (dernière mise à jour : janvier 2025)

Consultez le fichier ChangeLog.md dans notre GitHub référentiel pour suivre les améliorations et les correctifs spécifiques à chaque version.

Notifications

Il incombe aux clients de procéder à une évaluation indépendante des informations contenues dans le présent document. Ce document : (a) est fourni à titre informatif uniquement, (b) représente les offres de produits et les pratiques actuelles d'AWS, qui sont susceptibles d'être modifiées sans préavis, et (c) ne crée aucun engagement ni aucune garantie de la part d'AWS et de ses filiales, fournisseurs ou concédants de licence. Les produits ou services AWS sont fournis « tels quels » sans garanties, déclarations ou conditions d'aucune sorte, qu'elles soient explicites ou implicites. Les responsabilités et obligations d'AWS à l'égard de ses clients sont régies par les accords AWS, et le présent document ne fait partie d'aucun accord conclu entre AWS et ses clients et ne les modifie pas.

Automated Security Response sur AWS est concédé sous licence selon les termes de la licence Apache version 2.0 disponible auprès de l'Apache Software Foundation.

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.