Guide de l’utilisateur

AWS Well-Architected Tool

AWS Well-Architected Tool: Guide de l’utilisateur

Table of Contents

Qu'est-ce que c'est AWS Well-Architected Tool ?

AWS Well-Architected Tool (AWS WA Tool) est un service dans le cloud qui fournit un processus cohérent pour mesurer votre architecture en utilisant les AWS meilleures pratiques. AWS WA Tool vous aide tout au long du cycle de vie du produit en effectuant les opérations suivantes :

- Facilitant la documentation des décisions que vous prenez
- Fournissant des recommandations pour améliorer votre charge de travail en fonction des bonnes pratiques
- Vous guidant dans l'amélioration de la fiabilité, de la sécurité, de l'efficacité et de la rentabilité de vos charges de travail

Vous pouvez l'utiliser AWS WA Tool pour documenter et mesurer votre charge de travail en utilisant les meilleures pratiques du AWS Well-Architected Framework. Ces meilleures pratiques ont été développées par AWS des architectes de solutions sur la base de leurs années d'expérience dans la création de solutions pour une grande variété d'entreprises. La structure offre une approche cohérente pour mesurer les architectures et fournit des conseils quant à l'implémentation de modèles qui s'adaptent à vos besoins au fil du temps.

Outre les AWS meilleures pratiques, vous pouvez utiliser des verres personnalisés pour mesurer votre charge de travail en utilisant vos propres meilleures pratiques. Vous pouvez adapter les questions dans une perspective personnalisée pour qu'elles soient spécifiques à une technologie particulière ou pour vous aider à répondre aux besoins de gouvernance au sein de votre organisation. Les verres personnalisés étendent les indications fournies par les AWS verres.

Intégrations avec AWS Trusted Advisorles AWS Service Catalog AppRegistryinformations nécessaires pour répondre aux questions de AWS Well-Architected Tool révision et les découvrir plus facilement.

Ce service est destiné aux personnes impliquées dans le développement de produits techniques, telles que les directeurs de la technologie (CTOs), les architectes, les développeurs et les membres de l'équipe opérationnelle. AWS les clients l'utilisent AWS WA Tool pour documenter leurs architectures, assurer la gouvernance des lancements de produits et comprendre et gérer les risques liés à leur portefeuille technologique.

Rubriques

- Qu'est-ce que AWS Well-Architected Framework ?

Qu'est-ce que AWS Well-Architected Framework ?

Le AWS Well-Architected Framework documente un ensemble de questions fondamentales qui vous permettent de comprendre comment une architecture spécifique s'aligne sur les meilleures pratiques du cloud. Le cadre fournit une approche cohérente pour évaluer les systèmes par rapport aux qualités attendues des systèmes modernes basés sur le cloud. En fonction de l'état de votre architecture, le cadre suggère des améliorations que vous pouvez apporter pour mieux atteindre ces qualités.

L'utilisation de ce cadre vous permet d'apprendre les bonnes pratiques architecturales permettant de concevoir et de gérer des systèmes fiables, sécurisés, efficaces et rentables dans le cloud. Il vous permet d'évaluer vos architectures par rapport aux bonnes pratiques et d'identifier les points à améliorer. Le cadre repose sur six piliers : excellence opérationnelle, sécurité, fiabilité, efficacité des performances, optimisation des coûts et durabilité.

Lorsque vous concevez des charges de travail, vous établissez des compromis entre ces piliers en fonction des besoins de votre activité. Ces décisions professionnelles peuvent orienter vos priorités en matière d'ingénierie. Dans les environnements de développement, vous pouvez optimiser pour réduire les coûts au détriment de la fiabilité. Dans les solutions stratégiques, vous pouvez optimiser la fiabilité et être prêt à accepter une augmentation des coûts. Dans les solutions d'E-commerce, vous pouvez hiérarchiser les performances, car la satisfaction du client peut donner lieu à une augmentation des revenus. La sécurité et l'excellence opérationnelle ne donnent généralement pas lieu à des compromis avec les autres piliers.

Pour plus d'informations sur le framework, rendez-vous sur le site Web de AWS Well-Architected.

AWS Well-Architected Tool glossaire

Ce qui suit définit les termes courants utilisés dans AWS WA Tool et dans le AWS Well-Architected Framework.

- Une charge de travail identifie un ensemble de composants qui offrent une valeur business. La charge de travail est généralement le niveau de détail communiqué par les leaders technologiques et commerciaux. Les exemples de charges de travail incluent les sites Web marketing, les sites Web d'E-commerce, le backend pour une application mobile ett les plateformes d'analyse. Les charges de travail varient dans leur niveau de complexité d'architecture. Elles peuvent être simples,

comme un site Web statique, ou complexes, tels que les architectures de microservices avec plusieurs magasins de données et de nombreux composants.

- Les jalons marquent les principaux changements apportés à votre architecture au fur et à mesure qu'elle évolue tout au long du cycle de vie du produit : conception, tests, mise en service et production.
- Les cadres vous permettent d'évaluer continuellement vos architectures par rapport aux bonnes pratiques et d'identifier les points à améliorer.

  Outre les objectifs fournis par AWS, vous pouvez également créer et utiliser vos propres objectifs, ou utiliser des objectifs qui ont été partagés avec vous.
- Les problèmes à haut risque (HRIs) sont des choix architecturaux et opérationnels susceptibles d'avoir un impact négatif significatif sur une entreprise. AWS Cela HRIs peut affecter les opérations, les actifs et les individus de l'organisation.
- Les problèmes à risque moyen (MRIs) sont des choix architecturaux et opérationnels dont on AWS a constaté qu'ils pouvaient avoir un impact négatif sur les activités, mais dans une moindre mesureHRIs.

  Pour plus d'informations, consultez Problèmes à risque élevé et problèmes à risque moyen.

Démarrer avec AWS Well-Architected Tool

Pour commencer à utiliser l'AWS Well-Architected Tool, vous devez d'abord fournir les autorisations appropriées à vos utilisateurs, groupes et rôles, puis activer la prise en charge des Services AWS que vous souhaitez utiliser avec l'AWS WA Tool. Ensuite, vous définissez et documentez une charge de travail. Vous pouvez également enregistrer un jalon de l'état actuel d'une charge de travail.

Les rubriques suivantes expliquent comment faire vos premiers pas sur AWS WA Tool. Pour accéder à un didacticiel étape par étape qui explique comment utiliser AWS Well-Architected Tool, consultez Didacticiel : documenter une charge de travail AWS Well-Architected Tool.

Rubriques

Octroi de l'accès à l'AWS WA Tool à des utilisateurs, groupes ou rôles

Vous pouvez accorder aux utilisateurs, groupes ou rôles un accès avec contrôle total ou en lecture seule à l'AWS Well-Architected Tool.

Octroi de l'accès à l'AWS WA Tool

1. Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

   - Utilisateurs et groupes dans AWS IAM Identity Center :

     Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center.
   - Utilisateurs gérés dans IAM par un fournisseur d'identité :

Créez un rôle pour la fédération d'identité. Suivez les instructions de la rubrique Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM.

- Utilisateurs IAM :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique Création d'un rôle pour un utilisateur IAM dans le Guide de l'utilisateur IAM.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique Ajout d'autorisations à un utilisateur (console) du Guide de l'utilisateur IAM.

2. Pour accorder un contrôle total, appliquez la politique gérée WellArchitectedConsoleFullAccess au jeu d'autorisations ou au rôle.

   L'accès complet permet au principal d'effectuer toutes les actions dans l'AWS WA Tool. Cet accès est nécessaire pour définir des charges de travail, supprimer des charges de travail, consulter des charges de travail, mettre à jour des charges de travail, partager des charges de travail, créer des objectifs personnalisés et partager des objectifs personnalisés.

3. Pour accorder un accès en lecture seule, appliquez la politique gérée WellArchitectedConsoleReadOnlyAccess au jeu d'autorisations ou au rôle. Les principaux dotés de ce rôle peuvent uniquement consulter les ressources.

Pour plus d'informations sur ces politiques, consultez Politiques gérées par AWS pour AWS Well-Architected Tool.

Activation dans l'AWS WA Tool de la prise en charge d'autres services AWS

L'activation de l'accès à l'organisation permet à l'AWS Well-Architected Tool de recueillir des informations sur la structure de votre organisation afin de partager les ressources plus facilement (voir the section called "Activation du partage des ressources au sein d'AWS Organizations" pour plus d'informations). L'activation de la prise en charge Discovery permet de recueillir des informations à partir d'AWS Trusted Advisor, d'AWS Service Catalog AppRegistry et des ressources connexes (telles que les piles CloudFormation dans les collections de ressources AppRegistry) afin de vous aider à découvrir plus facilement les informations nécessaires pour répondre aux questions d'examen Well-Architected et adapter les vérifications Trusted Advisor à une charge de travail.

L'activation de la prise en charge pour AWS Organizations ou l'activation de la prise en charge Discovery crée automatiquement un rôle lié à un service pour votre compte.

Pour activer la prise en charge d'autres services avec lesquels l'AWS WA Tool peut interagir, accédez à Paramètres.

1. Pour recueillir des informations auprès d'AWS Organizations, activez l'option Activer la prise en charge AWS Organizations.
2. Activez l'option Activer la prise en charge Discovery pour recueillir des informations auprès d'autres services et ressources AWS.
3. Sélectionnez Afficher les autorisations des rôles pour consulter les autorisations de rôle liées à un service ou les politiques de relations d'approbation.
4. Sélectionnez Enregistrer les paramètres.

Activation d'AppRegistry pour une charge de travail

L'utilisation d'AppRegistry est facultative, et les clients AWS Business Support et Enterprise Support peuvent l'activer pour chaque charge de travail.

Chaque fois que la prise en charge Discovery est activée et qu'AppRegistry est associé à une charge de travail nouvelle ou existante, l'AWS Well-Architected Tool crée un groupe d'attributs géré par le service. Le groupe d'attributs Metadata dans AppRegistry contient l'ARN de la charge de travail, le nom de la charge de travail et les risques associés à la charge de travail.

- Lorsque la prise en charge Discovery est activée, chaque fois que la charge de travail est modifiée, le groupe d'attributs est mis à jour.
- Lorsque la prise en charge Discovery est désactivée ou que l'application est supprimée de la charge de travail, les informations de charge de travail sont supprimées d'AWS Service Catalog.

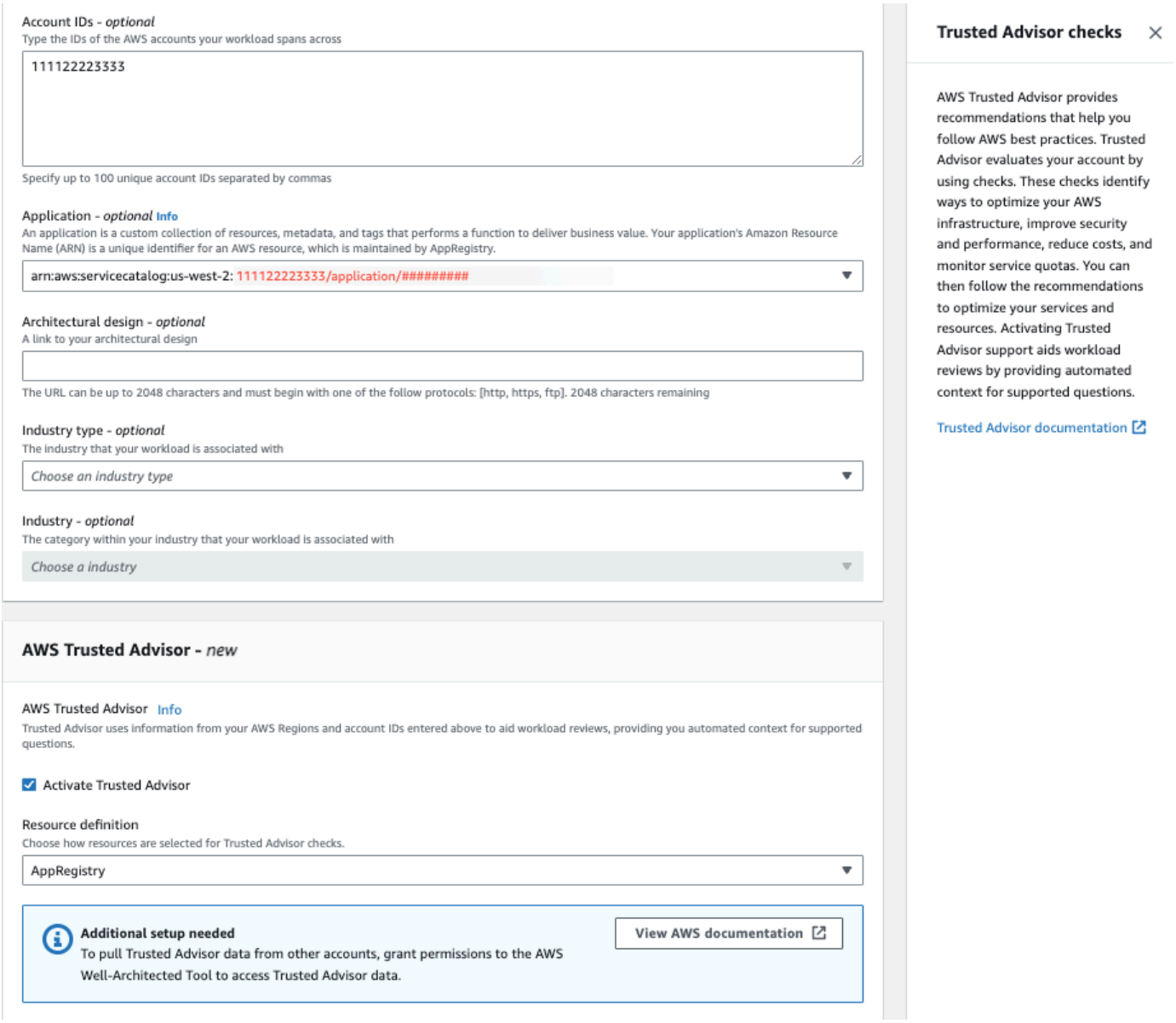
Si vous souhaitez qu'une application AppRegistry gère les données récupérées de Trusted Advisor, définissez le paramètre Définition de ressource de votre charge de travail sur AppRegistry ou Tous. Créez des rôles pour tous les comptes qui possèdent des ressources dans votre application en suivant les instructions fournies dans the section called "Activation de Trusted Advisor dans IAM".

Activation d'AWS Trusted Advisor pour une charge de travail

En option, vous pouvez intégrer AWS Trusted Advisor et l'activer pour chaque charge de travail pour les clients AWS Business Support et Enterprise Support. Aucun coût ne s'applique à l'intégration de Trusted Advisor à l'AWS WA Tool, mais pour connaître les informations de tarification de Trusted Advisor, consultez Plans de support AWS. L'activation de Trusted Advisor pour les charges de travail peut vous fournir une approche automatisée et surveillée plus complète pour examiner et optimiser vos charges de travail AWS. Cela peut vous aider à améliorer la fiabilité, la sécurité, les performances et l'optimisation des coûts de vos charges de travail.

Pour activer Trusted Advisor pour une charge de travail

1. Pour activer Trusted Advisor, les propriétaires de charge de travail peuvent utiliser l'AWS WA Tool pour mettre à jour une charge de travail existante ou créer une nouvelle charge de travail en choisissant Définir une charge de travail.
2. Entrez un identifiant de compte utilisé par Trusted Advisor dans le champ ID de compte, sélectionnez un ARN d'application dans le champ Application, ou effectuez les deux opérations pour activer Trusted Advisor.
3. Dans la section AWS Trusted Advisor, sélectionnez Activer Trusted Advisor.



4. La notification La fonction du service IAM sera créée s'affiche la première fois que Trusted Advisor est activé pour une charge de travail. Si vous choisissez Afficher les autorisations, les autorisations du rôle IAM s'affichent. Vous pouvez voir le Nom du rôle, ainsi que les Autorisations et Relations d'approbation que JSON a automatiquement créées pour vous dans IAM. Une fois le rôle créé, pour les charges de travail suivantes activant Trusted Advisor, seule la notification Configuration supplémentaire requise est affichée.
5. Dans le menu déroulant Définition de ressource, vous pouvez sélectionner Métadonnées de charge de travail, AppRegistry ou Tout. La sélection de Définition de ressource définit les données que l'AWS WA Tool récupère auprès de Trusted Advisor pour fournir les vérifications de statut dans l'examen de la charge de travail qui correspondent aux bonnes pratiques Well-Architected.

Métadonnées de charge de travail : la charge de travail est définie par les ID de compte et les Régions AWS spécifiées dans la charge de travail.

AppRegistry : la charge de travail est définie par les ressources (telles que les piles CloudFormation) présentes dans l'application AppRegistry associée à la charge de travail.

Tous : la charge de travail est définie à la fois par les métadonnées de charge de travail et par les ressources AppRegistry.

6. Choisissez Suivant.
7. Appliquez le cadre AWS Well-Architected à votre charge de travail et choisissez Définir une charge de travail. Les vérifications Trusted Advisor sont liées uniquement au cadre AWS Well-Architected, et non à d'autres objectifs.

L'AWS WA Tool obtient régulièrement des données de Trusted Advisor en utilisant les rôles créés dans IAM. Le rôle IAM est automatiquement créé pour le propriétaire de charge de travail. Toutefois, pour consulter les informations de Trusted Advisor, les propriétaires de tous les comptes associés à la charge de travail doivent accéder à IAM et créer un rôle. Consultez ??? pour plus de détails. Si ce rôle n'existe pas, l'AWS WA Tool ne peut pas obtenir les informations de Trusted Advisor pour ce compte et affiche un message d'erreur.

Pour plus d'informations sur la création d'un rôle dans Gestion des identités et des accès AWS (IAM), consultez Création d'un rôle pour un service AWS (console) dans le Guide de l'utilisateur IAM.

Activation de Trusted Advisor pour une charge de travail dans IAM

> **Note**
>
> Les propriétaires d'une charge de travail doivent activer la prise en charge Discovery pour leur compte avant de créer une charge de travail Trusted Advisor. Le choix d'activer la prise en charge Discovery crée le rôle requis pour le propriétaire de charge de travail. Suivez les étapes ci-dessous pour tous les autres comptes associés.

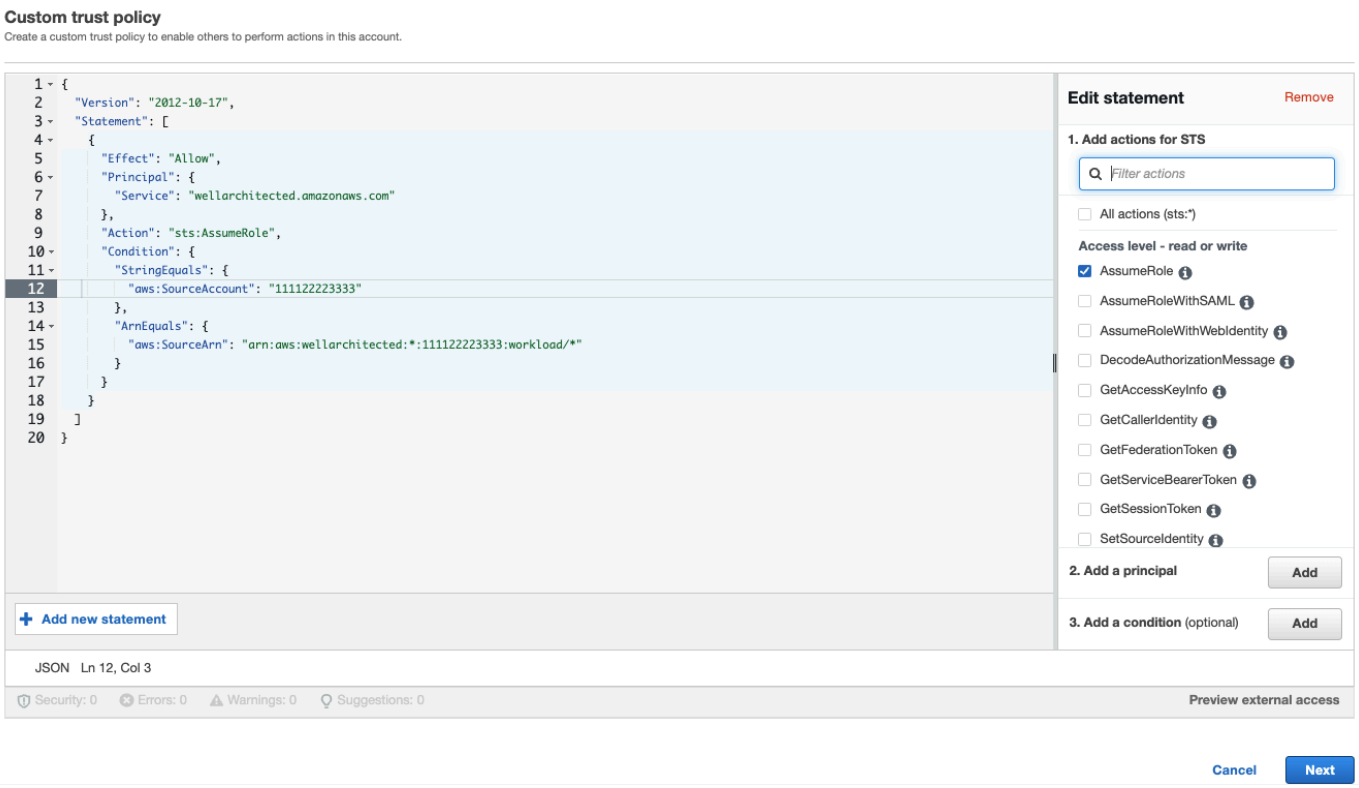
Les propriétaires des comptes associés aux charges de travail qui ont activé Trusted Advisor doivent créer un rôle dans IAM pour voir les informations de Trusted Advisor dans l'AWS Well-Architected Tool.

Pour créer un rôle dans IAM afin que l'AWS WA Tool obtienne des informations auprès de Trusted Advisor

1. Connectez-vous à la AWS Management Console et ouvrez la console IAM sur https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation de la console IAM, choisissez Rôles, puis Créer un rôle.
3. Pour Type d'entité approuvée, choisissez Stratégie d'approbation personnalisée.
4. Copiez et collez la stratégie d'approbation personnalisée suivante dans le champ JSON de la console IAM, comme illustré dans l'image suivante. Remplacez *WORKLOAD_OWNER_ACCOUNT_ID* par l'ID de compte du propriétaire de charge de travail, puis choisissez Suivant.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "wellarchitected.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "WORKLOAD_OWNER_ACCOUNT_ID"
                },
                "ArnEquals": {
                    "aws:SourceArn":
 "arn:aws:wellarchitected:*:111122223333:workload/*"
                }
            }
        }
    ]
}
```



Note

L'élément `aws:sourceArn` dans le bloc conditionnel de la politique d'approbation personnalisée précédente est `"arn:aws:wellarchitected:*:WORKLOAD_OWNER_ACCOUNT_ID:workload/*"`, qui est une condition générique indiquant que ce rôle peut être utilisé par l'AWS WA Tool pour toutes les charges de travail du propriétaire de charge de travail. Toutefois, l'accès peut être réduit à l'ARN d'une charge de travail spécifique ou à un ensemble d'ARN de charges de travail. Pour spécifier plusieurs ARN, consultez l'exemple de politique d'approbation suivant.

JSON

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

```
            "Principal": {
                "Service": "wellarchitected.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                "aws:SourceAccount": "111122223333"
                },
                "ArnEquals": {
                    "aws:SourceArn": [
                    "arn:aws:wellarchitected:us-
east-1:111122223333:workload/WORKLOAD_ID_1",
    "arn:aws:wellarchitected:us-
east-1:111122223333:workload/WORKLOAD_ID_2"
                    ]
                }
            }
        }
    ]
}
```

5. Sur la page Ajouter des autorisations, pour Politiques des autorisations, choisissez Créer une politique pour autoriser l'AWS WA Tool à accéder aux données de lecture de Trusted Advisor. Lorsque vous sélectionnez Créer une politique, une nouvelle fenêtre s'ouvre.

> **Note**
>
> En outre, vous avez la possibilité de ne pas créer les autorisations lors de la création du rôle et de créer une politique en ligne après avoir créé le rôle. Choisissez Afficher le rôle dans le message de création de rôle réussie, puis sélectionnez Créer une politique en ligne dans le menu déroulant Ajouter des autorisations de l'onglet Autorisations.

6. Copiez et collez la politique des autorisations suivante dans le champ JSON. Dans l'ARN `Resource`, remplacez *`YOUR_ACCOUNT_ID`* par votre propre ID de compte, spécifiez la région ou un astérisque (*), puis choisissez Suivant : Balises.

   Pour plus d'informations sur les formats ARN, consultez Amazon Resource Name (ARN) dans le Guide de référence générale AWS.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:DescribeCheckRefreshStatuses",
                "trustedadvisor:DescribeCheckSummaries",
                "trustedadvisor:DescribeRiskResources",
                "trustedadvisor:DescribeAccount",
                "trustedadvisor:DescribeRisk",
                "trustedadvisor:DescribeAccountAccess",
                "trustedadvisor:DescribeRisks",
                "trustedadvisor:DescribeCheckItems"
            ],
            "Resource": [
                "arn:aws:trustedadvisor:*:111122223333:checks/*"
            ]
        }
    ]
}
```

7. Si Trusted Advisor est activé pour une charge de travail et que Définition de ressource a pour valeur AppRegistry ou Tous, tous les comptes qui possèdent une ressource dans l'application AppRegistry attachée à la charge de travail doivent ajouter l'autorisation suivante à la politique des autorisations de leur rôle Trusted Advisor.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DiscoveryPermissions",
            "Effect": "Allow",
            "Action": [
                "servicecatalog:ListAssociatedResources",
                "tag:GetResources",
```

```
                "servicecatalog:GetApplication",
                "resource-groups:ListGroupResources",
                "cloudformation:DescribeStacks",
                "cloudformation:ListStackResources"
            ],
            "Resource": "*"
        }
    ]
}
```

8. (Facultatif) Ajoutez des balises. Choisissez Suivant : Vérification.
9. Examinez la stratégie, attribuez-lui un nom et sélectionnez Créer une politique.
10. Sur la page Ajouter des autorisations pour le rôle, sélectionnez le nom de la politique que vous venez de créer, puis sélectionnez Suivant.
11. Entrez le nom du rôle, qui doit utiliser la syntaxe suivante : `WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`* et choisissez Créer un rôle. Remplacez *`WORKLOAD_OWNER_ACCOUNT_ID`* par l'ID de compte du propriétaire de charge de travail.

    Vous devriez recevoir un message de réussite en haut de la page indiquant que le rôle a été créé.
12. Pour consulter le rôle et la politique d'autorisations associée, dans le volet de navigation de gauche, sous Gestion des accès, choisissez Rôles et recherchez le nom `WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`*. Sélectionnez le nom du rôle pour vérifier que les autorisations et les relations d'approbation sont correctes.

Désactivation de Trusted Advisor pour une charge de travail

Pour désactiver Trusted Advisor pour une charge de travail

Vous pouvez désactiver Trusted Advisor pour n'importe quelle charge de travail depuis l'AWS Well-Architected Tool en modifiant votre charge de travail et en désélectionnant Activer Trusted Advisor. Pour plus d'informations sur la modification des charges de travail, consultez the section called "Modification d'une charge de travail".

La désactivation de Trusted Advisor depuis l'AWS WA Tool ne supprime pas les rôles créés dans IAM. La suppression des rôles dans IAM nécessite une mesure de nettoyage distincte. Les propriétaires de charge de travail ou les propriétaires de comptes associés doivent supprimer les

rôles IAM créés lors de la désactivation de Trusted Advisor dans l'AWS WA Tool, ou pour empêcher l'AWS WA Tool de collecter des données Trusted Advisor pour la charge de travail.

Pour supprimer **`WellArchitectedRoleForTrustedAdvisor`** dans IAM

1. Connectez-vous à la AWS Management Console et ouvrez la console IAM sur https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation de la console IAM, choisissez Rôles.
3. Recherchez `WellArchitectedRoleForTrustedAdvisor-`*`WORKLOAD_OWNER_ACCOUNT_ID`* et sélectionnez le nom du rôle.
4. Sélectionnez Supprimer. Dans la fenêtre contextuelle, saisissez le nom du rôle pour confirmer la suppression, puis sélectionnez à nouveau Supprimer.

Pour plus d'informations sur la suppression d'un rôle dans IAM, consultez Suppression d'un rôle IAM (console) dans le Guide de l'utilisateur IAM.

Définition d'une charge de travail dans l'AWS WA Tool

Une charge de travail est un ensemble de composants qui apportent une valeur ajoutée à l'entreprise. Par exemple, les charges de travail peuvent être des sites Web de marketing, des sites Web de commerce électronique, le backend d'une application mobile et des plateformes d'analyse. Une définition précise de la charge de travail permet de procéder à un examen complet en fonction des piliers du cadre AWS Well-Architected.

Pour définir une charge de travail

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.
2. Si vous utilisez AWS WA Tool pour la première fois, vous voyez une page qui vous présente les fonctions du service. Dans la section Define a workload (Définir une charge de travail), choisissez Define a workload (Définir une charge de travail).

   Sinon, dans le panneau de navigation de gauche, choisissez Workloads (Charges de travail) et choisissez Define a workload (Définir une charge de travail).

   Pour plus d'informations sur la façon dont AWS utilise vos données de charge de travail, choisissez Pourquoi AWS a-t-il besoin de ces données et comment seront-elles utilisées ?

3. Dans la case Nom, saisissez un nom pour votre charge de travail.

> **Note**
>
> Le nom doit avoir entre 3 et 100 caractères. Au moins trois caractères ne doivent pas être des espaces. Les noms de charges de travail doivent être uniques. Les espaces et les majuscules sont ignorés lors du contrôle de l'unicité.

4. Dans la zone Description, saisissez une description de la charge de travail. La description doit comporter entre 3 et 250 caractères.
5. Dans la zone Responsable de la vérification, entrez le nom, l'adresse de messagerie ou l'identificateur du groupe ou de l'individu principal qui est responsable du processus de vérification de la charge de travail.
6. Dans la case Environnement, choisissez l'environnement pour votre charge de travail :
   - Production : la charge de travail s'exécute dans un environnement de production.
   - Pré-production : la charge de travail s'exécute dans un environnement de pré-production.
7. Dans la section Régions, choisissez les régions pour votre charge de travail :
   - Régions AWS : choisissez les Régions AWS où votre charge de travail s'exécute, l'une après l'autre.
   - Régions non AWS : entrez les noms des régions en dehors d'AWS où votre charge de travail s'exécute. Vous pouvez spécifier jusqu'à cinq régions uniques, séparées par des virgules.

   Utilisez les deux options le cas échéant pour votre charge de travail.
8. (Facultatif) Dans la case ID de compte, entrez les ID des Comptes AWS associés à votre charge de travail. Vous pouvez spécifier jusqu'à 100 ID de comptes uniques, séparés par des virgules.

   Si Trusted Advisor est activé, tous les ID de compte spécifiés sont utilisés pour obtenir des données de Trusted Advisor. Consultez Activation de AWS Trusted Advisor pour une charge de travail afin d'accorder à l'AWS WA Tool des autorisations permettant d'obtenir des données Trusted Advisor en votre nom au sein d'IAM.
9. (Facultatif) Dans la zone Application, entrez l'ARN d'une application issue d'AWS Service Catalog AppRegistry que vous souhaitez associer à cette charge de travail. Un seul ARN peut être spécifié par charge de travail, et l'application et la charge de travail doivent se trouver dans la même région.

10. (Facultatif) Dans la zone Conception architecturale saisissez l'URL de votre conception architecturale.
11. (Facultatif) Dans la zone Type de secteur d'activité choisissez le type de secteur associé à votre charge de travail.
12. (Facultatif) Dans la zone Secteur d'activité, choisissez le secteur qui correspond le mieux à votre charge de travail.
13. (Facultatif) Dans la section Trusted Advisor, pour activer les vérifications Trusted Advisor pour votre charge de travail, sélectionnez Activer Trusted Advisor. Une configuration supplémentaire peut être nécessaire pour les comptes associés à votre charge de travail. Consultez the section called "Activation de Trusted Advisor" pour accorder à AWS WA Tool les autorisations nécessaires pour obtenir les données Trusted Advisor en votre nom. Sélectionnez Métadonnées de charge de travail, AppRegistry ou Tous sous Définition de ressource pour définir les ressources utilisées par l'AWS WA Tool pour exécuter les vérifications Trusted Advisor.
14. (Facultatif) Dans la section Jira, pour activer les paramètres de synchronisation Jira au niveau de la charge de travail pour la charge de travail, sélectionnez Remplacer les paramètres au niveau du compte. Une configuration supplémentaire peut être nécessaire pour les comptes associés à votre charge de travail. Consultez Connecteur de l'AWS Well-Architected Tool pour Jira pour commencer à configurer le connecteur. Sélectionnez Ne pas synchroniser la charge de travail, Synchronisation de la charge de travail – Manuelle ou Synchronisation de la charge de travail – Automatique, et entrez éventuellement le paramètre Clé du projet Jira vers lequel effectuer la synchronisation.

    > **Note**
    >
    > Si vous ne remplacez pas les paramètres au niveau du compte, les charges de travail utiliseront par défaut le paramètre de synchronisation Jira au niveau du compte.

15. (Facultatif) Dans la section Balises, ajoutez les balises que vous souhaitez associer à la charge de travail.

    Pour plus d'informations sur les balises, consultez Balisage de vos ressources AWS WA Tool.
16. Choisissez Suivant.

    Si un champ obligatoire est vide ou si une valeur spécifiée n'est pas valide, vous devez corriger le problème avant de continuer.

17. (Facultatif) À l'étape Appliquer le profil, associez un profil à la charge de travail en sélectionnant un profil existant, en recherchant le nom du profil ou en choisissant Créer un profil pour créer un profil. Choisissez Suivant.
18. Choisissez les cadres qui s'appliquent à cette charge de travail. Jusqu'à 20 objectifs peuvent être ajoutés à une charge de travail. Pour accéder aux descriptions des objectifs AWS officiels, consultez Objectifs.

    Les objectifs peuvent être sélectionnés parmi les objectifs personnalisés (objectifs que vous avez créés ou qui ont été partagés avec votre Compte AWS), le catalogue Lens (objectifs officiels AWS disponibles pour tous les utilisateurs), ou les deux.

    > **Note**
    >
    > La section Objectifs personnalisés est vide si vous n'avez pas créé d'objectif personnalisé ou si aucun objectif personnalisé n'a été partagé avec vous.

    > **Exclusion de responsabilité**
    >
    > En accédant et/ou en appliquant des objectifs personnalisés créés par un autre utilisateur ou compte AWS, vous reconnaissez que les objectifs personnalisés créés par d'autres utilisateurs et partagés avec vous constituent un contenu tiers tel que défini dans le contrat client AWS.

19. Choisissez Define workload (Définir une charge de travail).

    Si un champ obligatoire est vide ou si une valeur spécifiée n'est pas valide, vous devez corriger le problème avant que votre charge de travail soit définie.

Documentation d'une charge de travail dans l'AWS WA Tool

Après avoir défini une charge de travail dans l'AWS Well-Architected Tool, vous pouvez documenter son état en ouvrant la page Examiner la charge de travail. Cela vous aide à évaluer votre charge de travail et à suivre son évolution au fil du temps.

Pour documenter l'état d'une charge de travail

1. Une fois la charge de travail définie, vous voyez une page indiquant les détails actuels de votre charge de travail. Choisissez Start reviewing (Démarrer la vérification) pour commencer.

   Sinon, dans le panneau de navigation de gauche, choisissez Workloads (Charges de travail) et sélectionnez le nom de la charge de travail pour ouvrir la page des détails de la charge de travail. Choisissez Continue reviewing (Continuer la vérification).

   (Facultatif) Si un profil est associé à votre charge de travail, le volet de navigation de gauche contient une liste de questions d'examen de charge de travail hiérarchisées que vous pouvez utiliser pour accélérer le processus d'examen de la charge de travail.
2. La première question vous est maintenant présentée. Pour chaque question :

   a. Lisez la question et déterminez si la question s'applique à votre charge de travail.

      Pour plus de conseils, choisissez Informations et consultez les informations dans le volet d'aide.

      - Si la question ne s'applique pas à votre charge de travail, choisissez Question does not apply to this workload (La question ne s'applique pas à cette charge de travail).
      - Dans le cas contraire, sélectionnez les bonnes pratiques de la liste que vous suivez actuellement.

        Si vous ne suivez actuellement aucune des bonnes pratiques, choisissez None of these (Aucune des propositions).

      Pour plus de conseils sur un élément, choisissez Informations et affichez les informations dans le volet droit.

   b. (Facultatif) Si une ou plusieurs bonnes pratiques ne s'appliquent pas à votre charge de travail, choisissez Marquer les bonnes pratiques qui ne s'appliquent pas à cette charge de travail et sélectionnez-les. Pour chaque bonne pratique sélectionnée, vous pouvez éventuellement sélectionner une raison et fournir des informations supplémentaires.

   c. (Facultatif) Utilisez la case Notes pour enregistrer les informations relatives à la question.

      Par exemple, vous pouvez décrire pourquoi la question ne s'applique pas ou fournir des détails supplémentaires sur les bonnes pratiques sélectionnées.

   d. Choisissez Suivant pour continuer vers la question suivante.

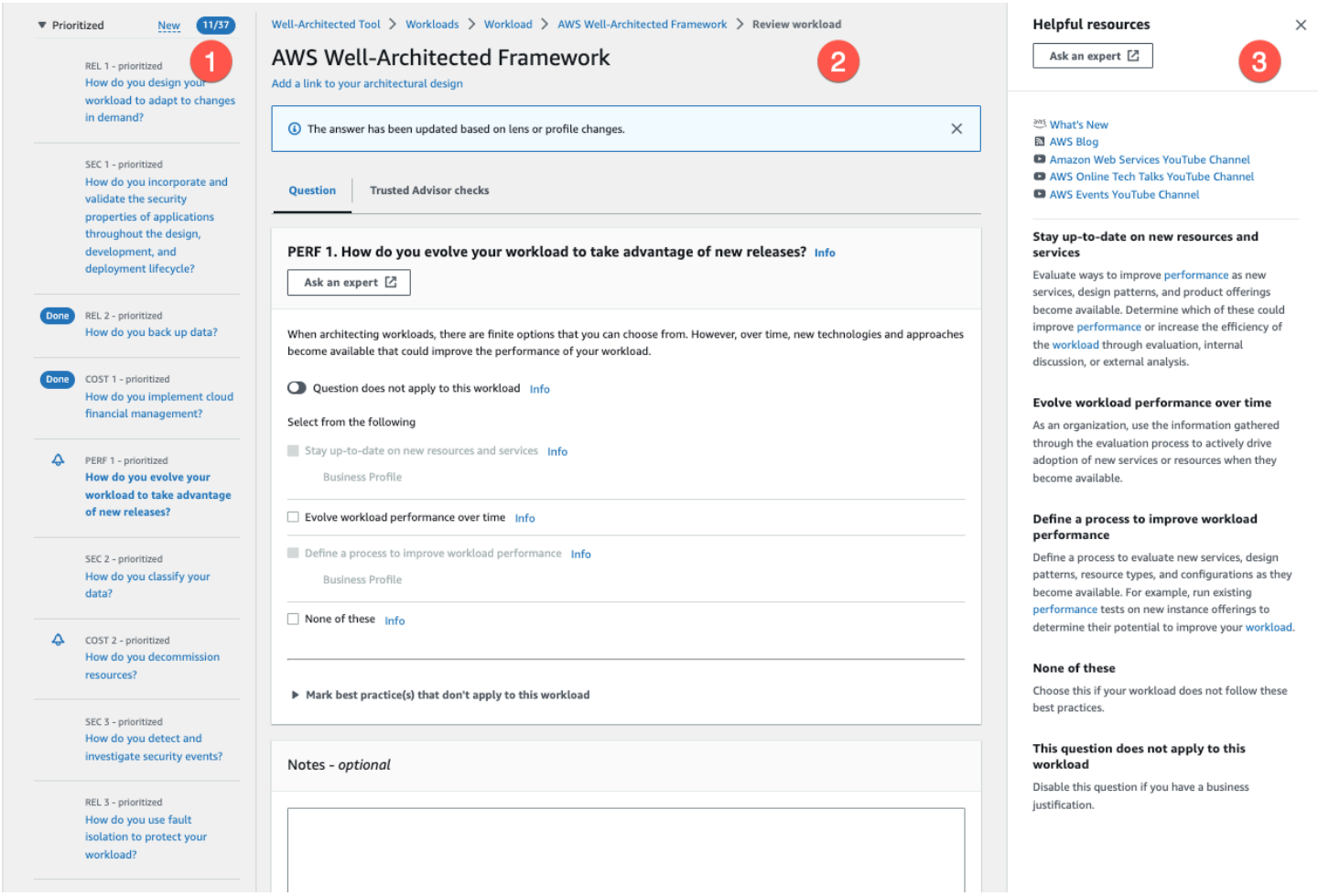
Répétez ces étapes pour chaque question de chaque pilier.

3. Choisissez Save and exit (Enregistrer et quitter) à tout moment pour enregistrer vos modifications et suspendre la documentation de votre charge de travail.

Après avoir documenté votre charge de travail, vous pouvez revenir aux questions ou reprendre l'examen à tout moment. Pour plus d'informations, consultez Examen d'une charge de travail à l'aide du cadre AWS Well-Architected.

Examen d'une charge de travail à l'aide du cadre AWS Well-Architected.

Vous pouvez passer en revue votre charge de travail dans la console sur la page Examiner la charge de travail. Cette page fournit les bonnes pratiques et des ressources utiles pour optimiser les performances de votre charge de travail.



1. Pour ouvrir la page Examiner la charge de travail, sur la page des détails de la charge de travail, choisissez Continuer l'examen. Le volet de navigation de gauche affiche les questions relatives à chaque pilier. Les questions auxquelles vous avez répondu sont marquées Terminé. Le nombre de réponses dans chaque pilier est affiché en regard du nom du pilier.

   Vous pouvez accéder à des questions dans d'autres piliers en choisissant le nom du pilier, puis en choisissant la question à laquelle vous souhaitez répondre.

   (Facultatif) Si un profil est associé à votre charge de travail, l'AWS WA Tool utilise les informations présentes dans le profil pour déterminer quelles questions de l'examen de la charge de travail sont hiérarchisées et quelles questions ne s'appliquent pas à votre entreprise. Dans le volet de navigation de gauche, vous pouvez utiliser les questions hiérarchisées pour accélérer le processus d'examen de la charge de travail. Une icône de notification apparaît à côté des questions nouvellement ajoutées à la liste des questions hiérarchisées.
2. Le volet central affiche la question en cours. Sélectionnez les bonnes pratiques que vous suivez. Choisissez Infos pour obtenir des informations supplémentaires sur la question ou une bonne pratique. Choisissez Demandez à un expert pour accéder à la communauté AWS re:Post dédiée à AWS Well-Architected. AWS re:Post est une communauté de questions-réponses basée sur les sujets qui remplace les forums AWS. Avec re:Post, vous pouvez trouver des réponses, répondre à des questions, rejoindre un groupe, suivre des sujets populaires et voter pour vos questions et réponses préférées.

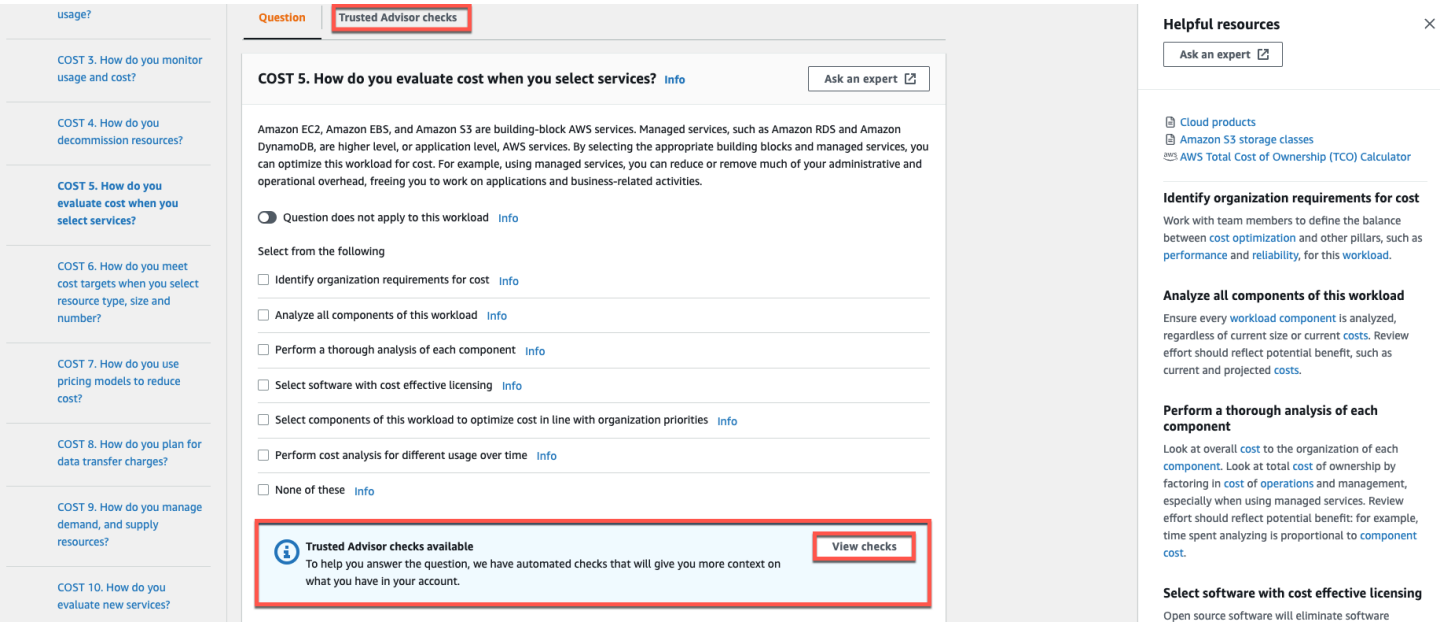
   (Facultatif) Pour marquer une ou plusieurs bonnes pratiques comme non applicables, choisissez Marquer les bonnes pratiques qui ne s'appliquent pas à cette charge de travail et sélectionnez-les.

   Utilisez les boutons en bas de ce volet pour accéder à la question suivante, revenir à la question précédente, ou enregistrer vos modifications et quitter la session.
3. Le volet d'aide de droite affiche des informations supplémentaires et des ressources utiles. Choisissez Demandez à un expert pour accéder à la communauté AWS re:Post dédiée à AWS Well-Architected. Dans cette communauté, vous pouvez poser des questions relatives à la conception, à la création, au déploiement et à l'exploitation des charges de travail sur AWS.

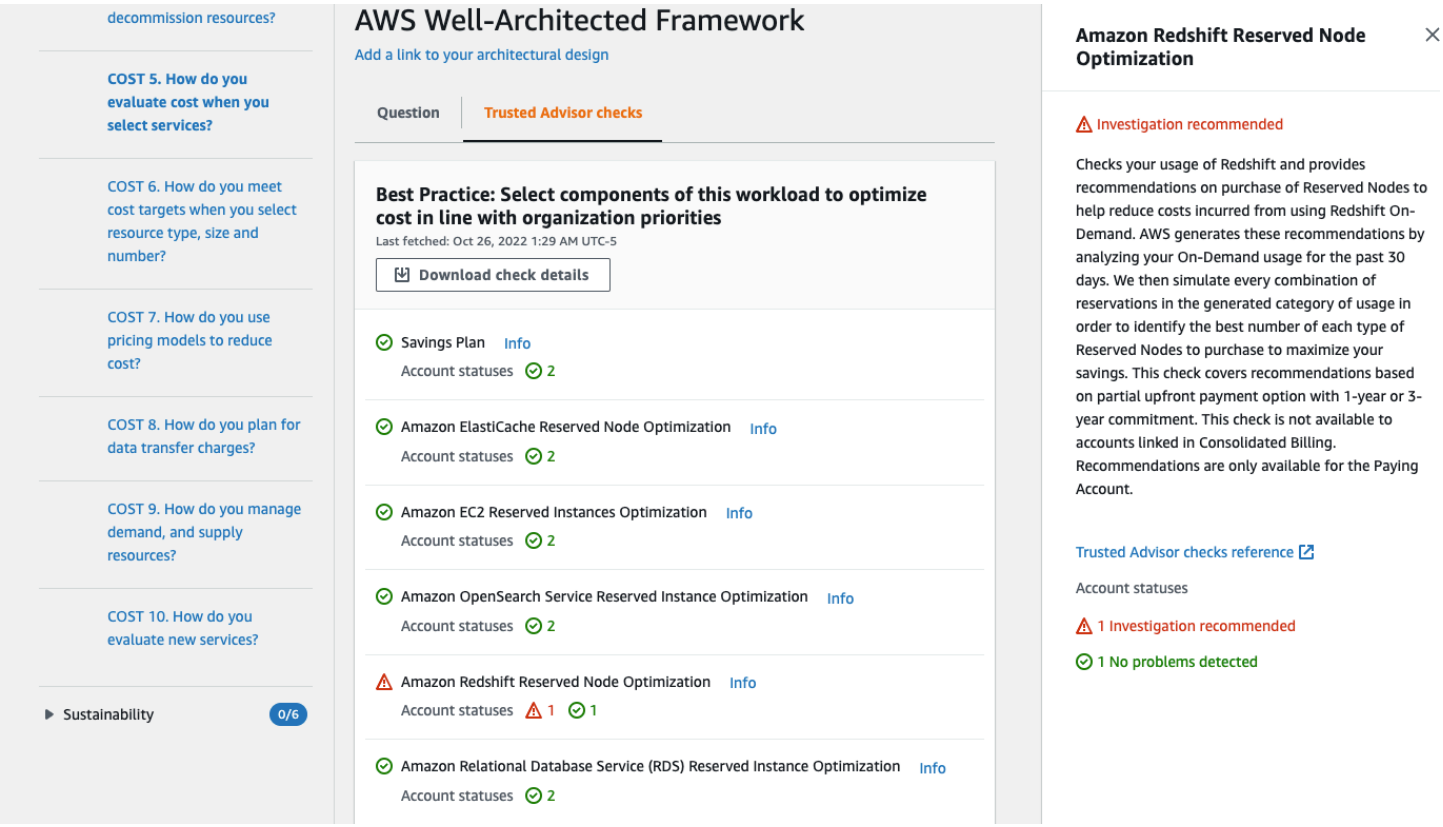
Affichage des vérifications Trusted Advisor relatives à votre charge de travail

Si Trusted Advisor est activé pour votre charge de travail, un onglet Contrôles Trusted Advisor est affiché à côté de Question. Si des vérifications sont disponibles pour la bonne pratique, une

notification indiquant que des vérifications Trusted Advisor sont disponibles s'affiche après la sélection de la question. Si vous sélectionnez Afficher les vérifications, vous accédez à l'onglet Contrôles Trusted Advisor.



Dans l'onglet Contrôles Trusted Advisor, vous pouvez consulter des informations plus détaillées sur les vérifications des bonnes pratiques par Trusted Advisor, consulter les liens vers la documentation Trusted Advisor dans le volet Ressources d'aide ou Télécharger les détails de la vérification, qui fournit un rapport sur les vérifications Trusted Advisor et les statuts de chaque bonne pratique dans un fichier CSV.



Les catégories des vérifications Trusted Advisor sont affichées sous forme d'icônes colorées, et le nombre à côté de chaque icône indique le nombre de comptes ayant ce statut.

- Action recommandée (rouge) :Trusted Advisor recommande une action pour la vérification.
- Investigation recommandée (jaune) : Trusted Advisor détecte un problème possible pour la vérification.
- Aucun problème détecté (vert) : Trusted Advisor ne détecte pas de problème pour la vérification.
- Éléments exclus (gris) : nombre de vérifications qui ont exclu des éléments, tels que les ressources que vous souhaitez ignorer.

Pour plus d'informations sur les vérifications proposées par Trusted Advisor, consultez Affichage des catégories de vérifications dans le Guide de l'utilisateur Support.

La sélection du lien Informations situé à côté de chaque vérification Trusted Advisor permet d'afficher des informations sur la vérification dans le volet Ressources d'aide. Pour plus d'informations, consultez Référence de la vérification AWS Trusted Advisor dans le Guide de l'utilisateur Support.

Enregistrement d'un jalon pour une charge de travail dans l'AWS WA Tool

Vous pouvez enregistrer un jalon pour une charge de travail à tout moment. Un jalon enregistre l'état actuel de la charge de travail.

Pour enregistrer un jalon

1. A partir de la page des détails de la charge de travail, choisissez Save milestone (Enregistrer un jalon).
2. Dans la case Milestone name (Nom d'un jalon), saisissez un nom pour votre jalon.

   > **Note**
   >
   > Le nom doit avoir entre 3 et 100 caractères. Au moins trois caractères ne doivent pas être des espaces. Les noms de jalons associés à une charge de travail doivent être uniques. Les espaces et les majuscules sont ignorés lors du contrôle de l'unicité.

3. Choisissez Enregistrer.

Une fois qu'un jalon a été enregistré, vous ne pouvez pas modifier les données de charge de travail qui ont été capturées dans ce jalon.

Pour de plus amples informations, consultez Jalons.

Tutoriel : Documenter une AWS Well-Architected Tool charge de travail

Ce didacticiel décrit comment AWS Well-Architected Tool documenter et mesurer une charge de travail. Cet exemple illustre, étape par étape, comment définir et documenter une charge de travail pour un site web de commerce électronique au détail.

Rubriques

Étape 1 : définir une charge de travail

Vous commencez par définir une charge de travail. Il existe deux manières de définir une charge de travail. Dans ce didacticiel, nous ne définissons pas une charge de travail à partir d'un modèle de révision. Pour plus de détails sur la définition d'une charge de travail à partir d'un modèle de révision, consultezthe section called “Définition d’une charge de travail”.

Pour définir une charge de travail

1. Connectez-vous à la AWS Well-Architected Tool console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wellarchitected/.

   > **Note**
   >
   > L'utilisateur qui documente l'état de la charge de travail doit disposer d'autorisations d'accès complètes pour AWS WA Tool.

2. Dans la section Define a workload (Définir une charge de travail), choisissez Define a workload (Définir une charge de travail).
3. Dans la zone Name (Nom), entrez **`Retail Website - North America`** comme nom de la charge de travail.
4. Dans la zone Description, entrez une description de la charge de travail.

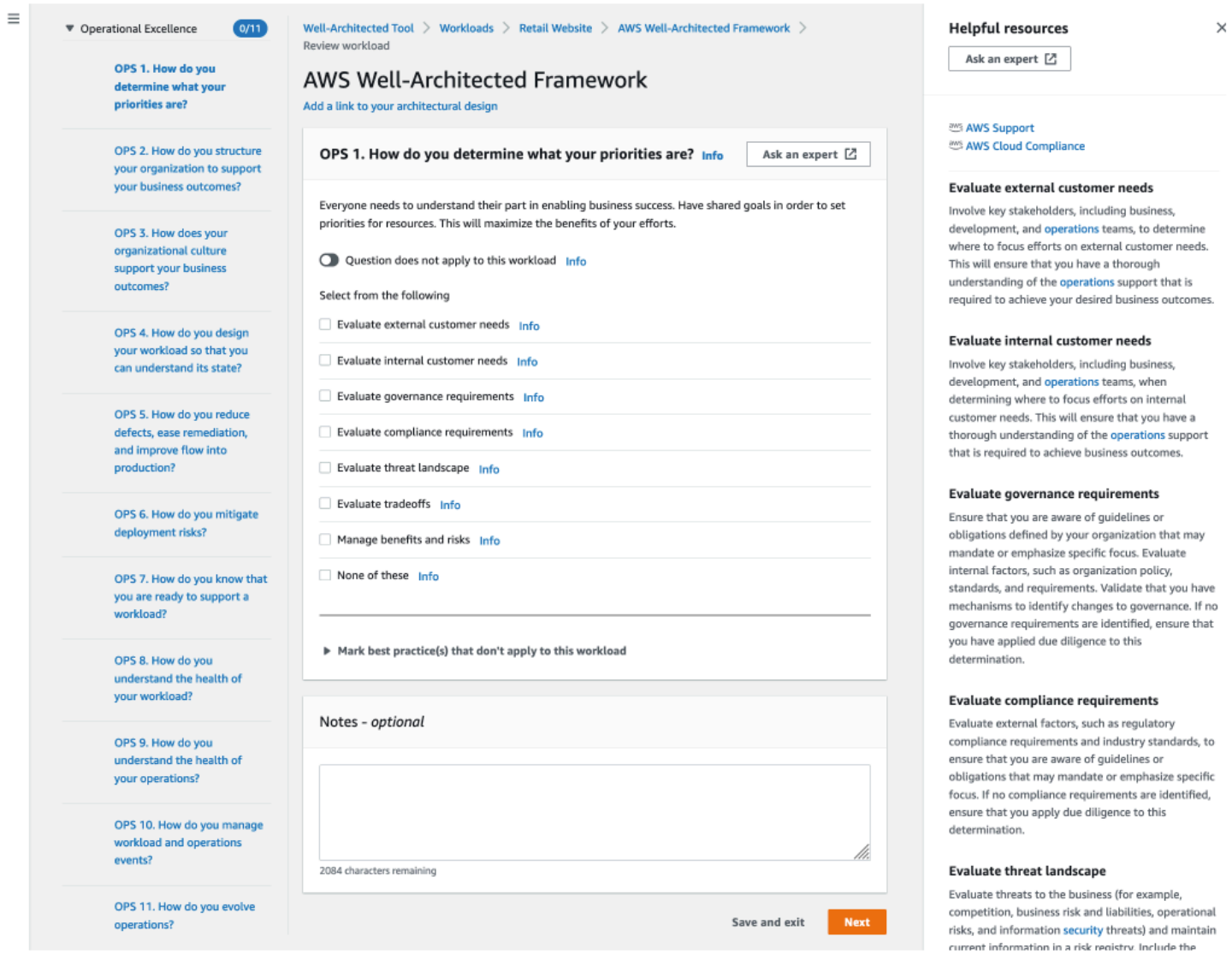
5. Dans le champ Propriétaire de la révision, entrez le nom de la personne responsable du processus de révision de la charge de travail.
6. Dans le champ Environnement, indiquez que la charge de travail se trouve dans un environnement de production.
7. Notre charge de travail s'étend à la fois à notre centre de données local AWS et à notre centre de données local :
    a. Sélectionnez Régions AWSet choisissez les deux régions d'Amérique du Nord où la charge de travail est exécutée.
    b. Sélectionnez également Non AWS régions et entrez le nom du centre de données local.
8. La IDs case Compte est facultative. N'en associez aucune Comptes AWS à cette charge de travail.
9. La case Application est facultative. Ne saisissez pas d'application ARN pour cette charge de travail.
10. La case Schéma architectural est facultative. N'associez pas de schéma architectural à cette charge de travail.
11. Les zones Industry type (Type de secteur) et Industry (Secteur) sont facultatives et ne sont pas spécifiées pour cette charge de travail.
12. La section Trusted Advisor est facultative. N'activez pas le Trusted Advisor Support pour cette charge de travail.
13. La section Jira est facultative. Ne remplacez pas les paramètres au niveau du compte dans la section Jira pour cette charge de travail.
14. Dans cet exemple, n'appliquez aucune balise à la charge de travail. Choisissez Suivant.
15. L'étape Appliquer le profil est facultative. N'appliquez pas de profil pour cette charge de travail. Choisissez Suivant.
16. Pour cet exemple, appliquez l'objectif AWS Well-Architected Framework, qui est automatiquement sélectionné. Choisissez Define workload (Définir une charge de travail) pour enregistrer ces valeurs et définir la charge de travail.
17. Une fois la charge de travail définie, choisissez Start reviewing (Démarrer la vérification) pour commencer à documenter l'état de la charge de travail.

Étape 2 : Documenter l'état de la charge de travail

Pour documenter l'état de la charge de travail, vous êtes confronté à des questions correspondant à l'objectif sélectionné qui couvrent les piliers du AWS Well-Architected Framework : excellence opérationnelle, sécurité, fiabilité, efficacité des performances, optimisation des coûts et durabilité.

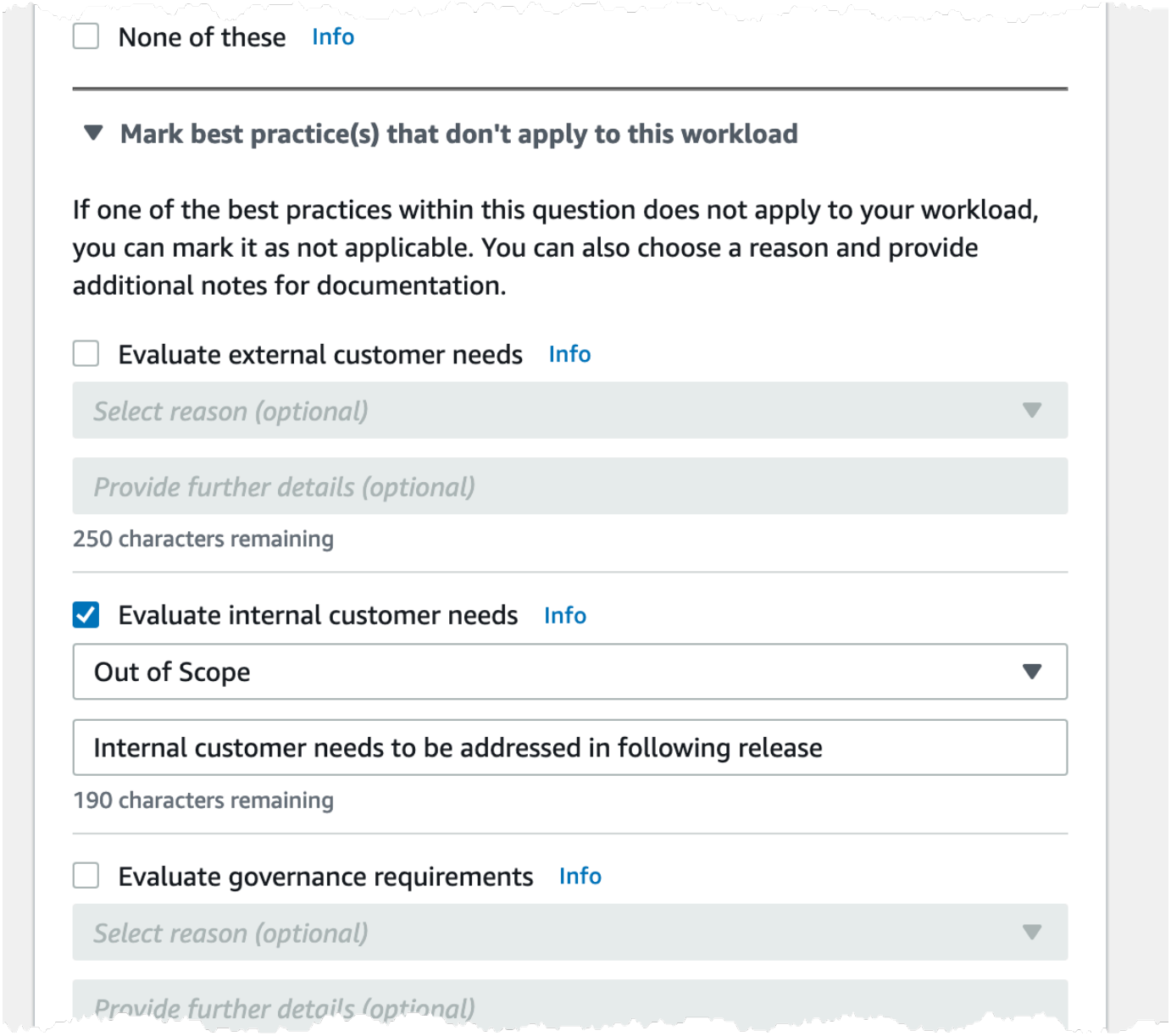
Pour chaque question, choisissez les bonnes pratiques que vous suivez dans la liste fournie. Si vous avez besoin d'informations détaillées sur une bonne pratique, choisissez Infos et affichez les informations supplémentaires et les ressources dans le volet droit.

Choisissez Ask an expert pour accéder à la communauté AWS Re:post dédiée à Well-Architected AWS . Dans cette communauté, vous pouvez poser des questions relatives à la conception, à la création, au déploiement et à l'exploitation des charges de travail sur AWS.



1. Choisissez Next (Suivant) pour passer à la question suivante. Vous pouvez utiliser le volet gauche pour accéder à une autre question dans le même pilier ou à une question dans l'un des autres piliers.
2. Si vous choisissez La question ne s'applique pas à cette charge de travail ou Aucune de ces questions, il est AWS recommandé d'en indiquer la raison dans le champ Remarques. Ces notes sont incluses dans le cadre du rapport de la charge de travail et peuvent être utiles à l'avenir lorsque des modifications sont apportées à la charge de travail.

> **Note**
>
> Vous pouvez éventuellement marquer une ou plusieurs bonnes pratiques individuelles comme non applicables. Choisissez Marquer les meilleures pratiques qui ne s'appliquent pas à cette charge de travail et sélectionnez les meilleures pratiques qui ne s'appliquent pas. Vous pouvez éventuellement sélectionner un motif et fournir des informations supplémentaires. Répétez l'opération pour chaque bonne pratique qui ne s'applique pas.



> **Note**
>
> Vous pouvez suspendre ce processus à tout moment en choisissant Enregistrer et quitter. Pour le reprendre ultérieurement, ouvrez la AWS WA Tool console et choisissez Workloads dans le volet de navigation de gauche.

3. Sélectionnez le nom de la charge de travail pour ouvrir la page des détails de la charge de travail.

4. Choisissez Continue reviewing (Continuer la vérification), puis accédez à l'endroit où vous vous étiez arrêté.
5. Une fois que vous avez terminé toutes les questions, une page de présentation de la charge de travail s'affiche. Vous pouvez examiner ces détails maintenant ou y accédez ultérieurement en choisissant Workloads (Charges de travail) dans le panneau de navigation de gauche et en sélectionnant le nom de la charge de travail.

Après avoir documenté l'état de votre charge de travail pour la première fois, vous devez enregistrer un jalon et générer un rapport sur la charge de travail.

Un jalon enregistre l'état actuel de la charge de travail et vous permet de mesurer les progrès lorsque vous apportez des modifications en fonction de votre plan d'amélioration.

Sur la page des détails de la charge de travail :

1. Dans la section Vue d'ensemble de la charge de travail, cliquez sur le bouton Enregistrer le jalon.
2. Entrez **`Version 1.0 - initial review`** comme nom du jalon.
3. Choisissez Save (Enregistrer).
4. Pour générer un rapport de charge de travail, sélectionnez l'objectif souhaité et choisissez Générer un rapport. Un PDF fichier est créé. Ce fichier contient l'état de la charge de travail, le nombre de risques identifiés et une liste des améliorations suggérées.

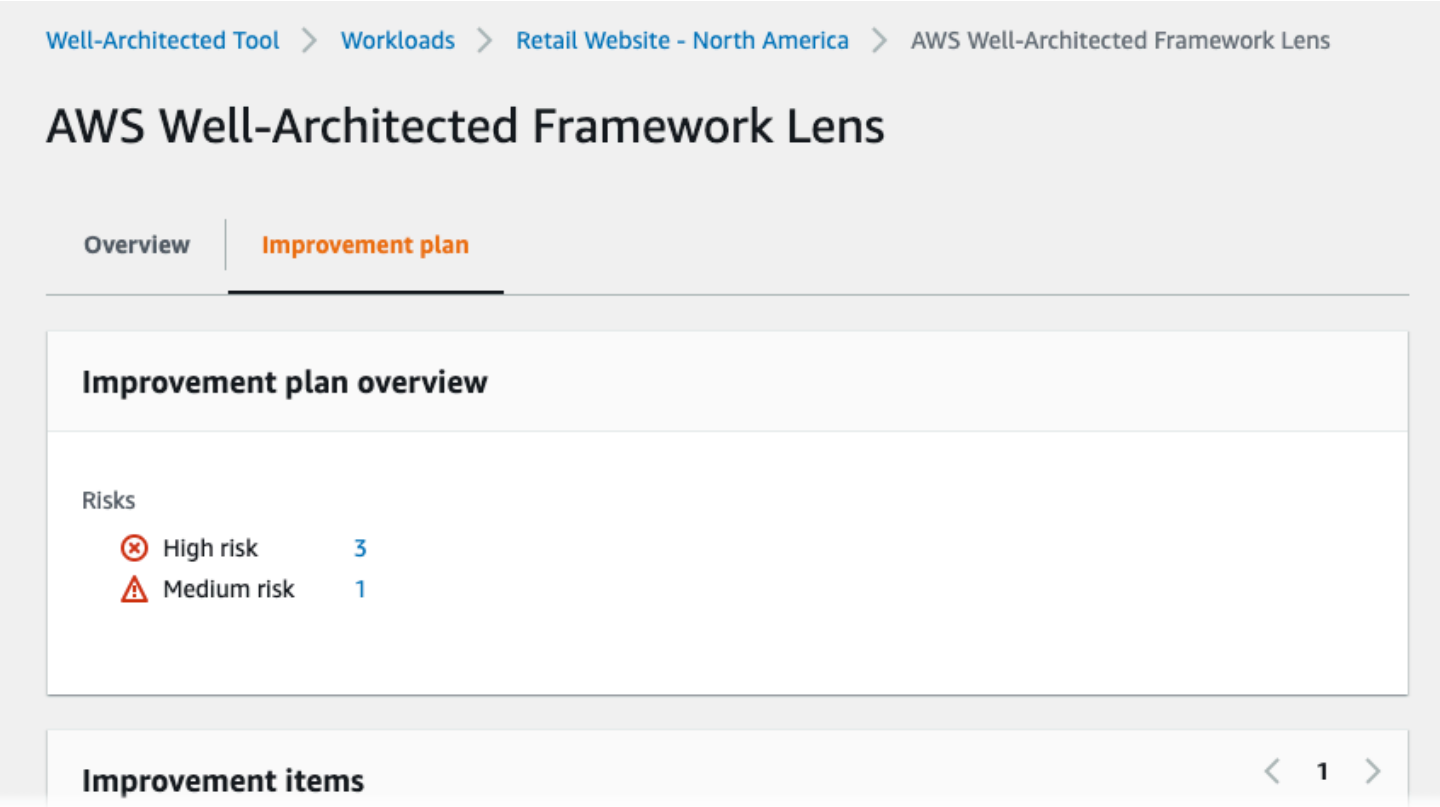
Étape 3 : Réviser le plan d'amélioration

Sur la base des meilleures pratiques sélectionnées, AWS WA Tool identifie les domaines présentant un risque élevé ou moyen, tels que mesurés par rapport au AWS Well-Architected Framework Lens.

Pour consulter le plan d'amélioration :

1. Choisissez AWS Well-Architected Framework dans la section Lenses de la page d'aperçu.
2. Choisissez ensuite Improvement plan (Plan d'amélioration).

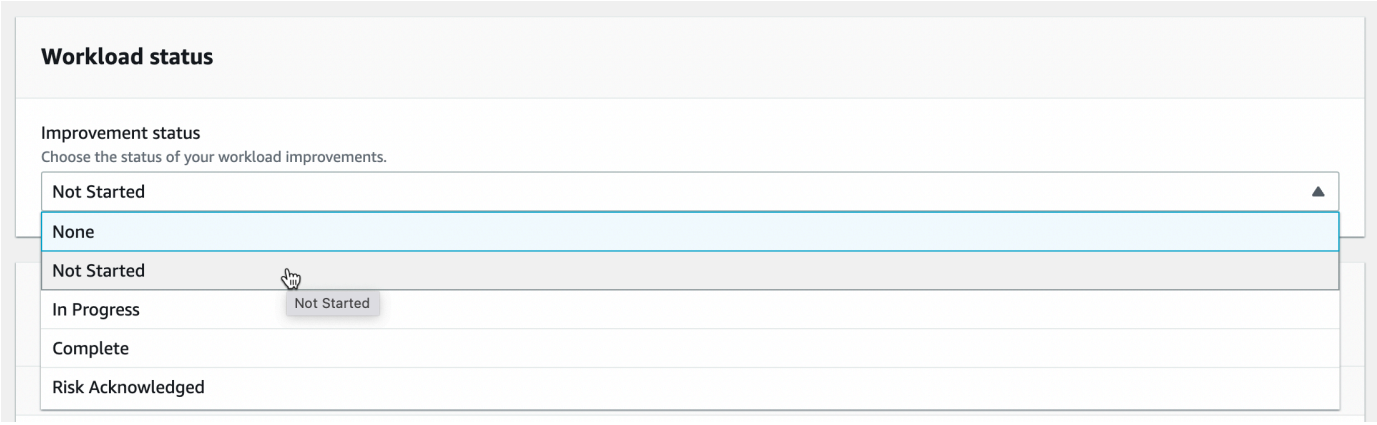
Pour cet exemple particulier de charge de travail, trois problèmes à haut risque et un problème à risque moyen ont été identifiés par le AWS Well-Architected Framework Lens.



Mettez à jour l'état d'amélioration de la charge de travail pour indiquer que les améliorations apportées à la charge de travail n'ont pas encore commencé.

Pour modifier le statut d'amélioration :

1. Dans le plan d'amélioration, cliquez sur le nom de la charge de travail (**`Retail Website - North America`**) dans le fil de navigation en haut de la page.
2. Cliquez sur l'onglet Propriétés.
3. Accédez à la section État de la charge de travail et sélectionnez Non démarré dans la liste déroulante.



4. Revenez au plan d'amélioration depuis l'onglet Propriétés en cliquant sur l'onglet Overview, puis sur le lien AWS Well-Architected Framework dans la section Lenses. Cliquez ensuite sur l'onglet Plan d'amélioration en haut de la page.

La section Improvement items (Éléments d'amélioration) affiche les éléments d'amélioration recommandés identifiés dans la charge de travail. Les questions sont classées en fonction de la priorité par pilier qui a été définie, les problèmes à risque élevé étant répertoriés en premier, suivis des problèmes à risque moyen.

Développez des Recommended improvement items (Éléments d'amélioration recommandés) pour afficher les bonnes pratiques suggérées pour une question. Chaque action d'amélioration recommandée est liée à un conseil d'expert détaillé pour vous aider à supprimer, ou du moins atténuer, les risques identifiés.

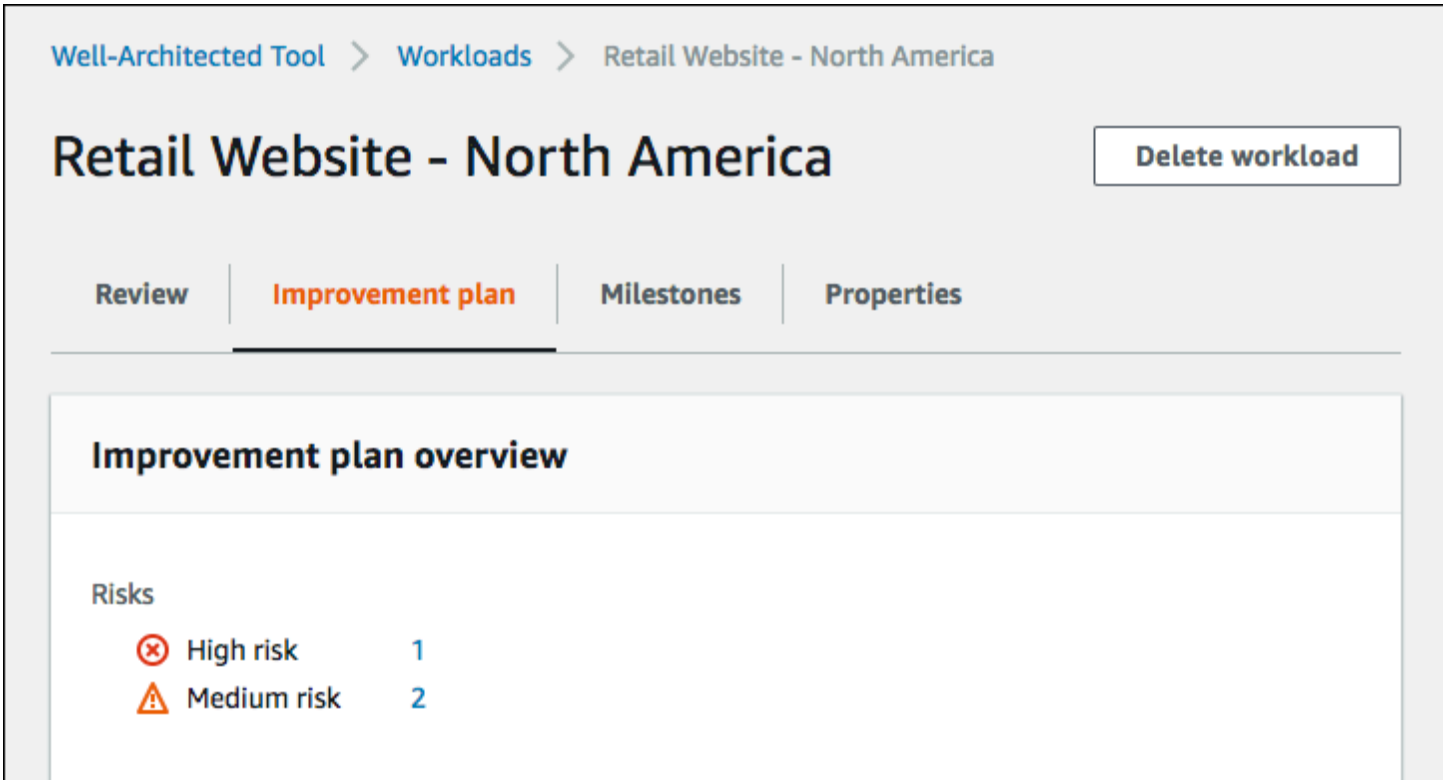
Si un profil est associé à la charge de travail, le nombre de risques hiérarchisés est affiché dans la section Vue d'ensemble du plan d'amélioration, et vous pouvez filtrer la liste des éléments d'amélioration en sélectionnant Priorisé par profil. La liste des éléments d'amélioration affiche une étiquette Priorisée.

Étape 4 : Apporter des améliorations et mesurer les progrès

Dans le cadre de ce plan d'amélioration, l'un des problèmes les plus risqués a été résolu par l'ajout d'Amazon CloudWatch et du AWS Auto Scaling support à la charge de travail.

Dans la section Éléments d'amélioration :

1. Choisissez la question pertinente et mettez à jour les meilleures pratiques sélectionnées pour refléter les modifications. Des notes sont ajoutées pour enregistrer les améliorations.
2. Choisissez ensuite Enregistrer et quitter pour mettre à jour l'état de la charge de travail.
3. Après avoir apporté des modifications, vous pouvez revenir au plan d'amélioration et voir l'effet de ces modifications sur la charge de travail. Dans cet exemple, ces actions ont amélioré le profil de risque en réduisant le nombre de problèmes à haut risque de trois à un seul.



Vous pouvez enregistrer un jalon à ce stade, puis aller à la section Milestones (Jalons) pour voir comment la charge de travail s'est améliorée.

Révision du cadre Well-Architected (WAFR)

Le cadre Well-Architected décrit les concepts clés, les principes de conception et les bonnes pratiques architecturales pour la conception et l'exécution de charges de travail dans le cloud. Il vous permet de comprendre les avantages et les inconvénients des décisions que vous prenez lors du développement de systèmes sur AWS. En utilisant ce framework, vous apprenez les bonnes pratiques architecturales en matière de conception et d'exploitation d'applications fiables, sécurisées, efficaces, économiques et durables.

Au cours de la révision du cadre Well-Architected (WAFR), vous répondrez à une série de questions fondamentales pour savoir dans quelle mesure votre architecture s'aligne sur les bonnes pratiques du cloud et vous recevrez des conseils pour mettre en œuvre des améliorations.

Phases WAFR

Le processus WAFR comprend trois phases principales :

- Préparation : préparez-vous à réussir grâce à une planification appropriée et à un alignement des parties prenantes
- Révision : réalisez l'évaluation proprement dite en vous appuyant sur les bonnes pratiques AWS
- Amélioration : transformez les résultats en améliorations concrètes pour votre charge de travail

Ce document vous guide à travers les trois phases, en vérifiant que vous êtes suffisamment préparé pour tirer le meilleur parti de la phase de révision. Nous vous aidons également à transformer les résultats de votre WAFR en améliorations concrètes pour votre charge de travail.

Préparation au WAFR

Il est important de ne pas se précipiter dans la réalisation d'une révision du cadre Well-Architected (WAFR) sans une préparation suffisante. La précipitation peut allonger le processus, ce qui entraîne un résultat moins favorable et complique les actions.

La révision d'une architecture a un coût humain associé. Si un membre du groupe ou de l'équipe peut se préparer dès le départ, cela permet de gagner du temps lors des étapes ultérieures, lorsque davantage de personnes sont nécessaires pour assister aux sessions. Cela peut également éliminer le besoin de discussions en groupe plus important grâce à une meilleure planification des sessions et à des techniques de communication asynchrones.

Une définition claire de la personne responsable de la charge de travail, de son architecture, de son objectif et de son alignement sur les résultats commerciaux de votre organisation peut vous aider à obtenir de meilleurs résultats lors des phases de révision et d'amélioration.

La phase de préparation comprend trois éléments clés :

1. Charge de travail et portée
2. Personnes et culture
3. Documentation et infrastructure

Charge de travail et portée

Selon le cadre AWS Well-Architected :

> Une charge de travail est un ensemble de ressources et de code qui fournit une valeur business, par exemple une application destinée au client ou un processus dorsal. Une charge de travail peut se composer d'un sous-ensemble de ressources dans un même Compte AWS ou être un ensemble de plusieurs ressources couvrant plusieurs Comptes AWS. Une petite entreprise peut avoir seulement quelques charges de travail alors qu'une grande entreprise peut en avoir plusieurs milliers.

Une charge de travail ne se limite pas à des services ou à des ressources cloud. Elle inclut également les personnes, les équipes, les processus et les dossiers d'exploitation, ainsi que la technologie et l'infrastructure qui apportent de la valeur métier. Avant d'exécuter un WAFR, prenez le temps de comprendre et de documenter les composants de votre charge de travail. Cela peut vous permettre de gagner du temps lors de la phase de révision.

Choix d'une charge de travail pour un WAFR

Pour préparer une charge de travail pour un WAFR, discutez des questions suivantes avec l'équipe :

- À qui appartient la charge de travail ? Qui est responsable si une interruption de la charge de travail a un impact sur l'entreprise ?
- Quel est l'objectif de la charge de travail ? Existe-t-il des outils d'analytique pour l'entreprise ? Dispose-t-elle d'un environnement de test (sandbox), d'une formation et d'une journalisation ?
- Cette charge de travail doit-elle exister ? Que se passe-t-il si vous l'arrêtez ?
- La charge de travail est-elle orientée vers le client ou est-elle interne ?
- La charge de travail est-elle productive ou non ?

- À quelle phase se situe la charge de travail dans son cycle de vie ?
- Quel est l'impact d'une interruption de l'activité ?
- Quelles sont les limites de la charge de travail ?
- Quelles sont les dépendances de cette charge de travail ?

Vous devriez être en mesure de répondre clairement à la plupart de ces questions lors de l'évaluation de votre charge de travail avant de poursuivre avec le WAFR.

Quelle est la portée de l'examen ?

Bien qu'en fin de compte, un WAFR couvre tous les piliers du cadre, nous pouvons identifier les compromis et comprendre le contexte avant de prendre des décisions. Une bonne façon de commencer est de se concentrer sur les piliers prioritaires ou sur un domaine particulier de la charge de travail.

La définition d'un processus de révision global, la production de résultats exploitables et l'itération vous permettent de mieux rentabiliser la charge de travail et l'entreprise.

Envisagez une approche progressive :

1. Identifiez les deux ou trois principaux piliers les plus pertinents dans le contexte métier et technique actuel.
2. Démontrez la valeur de votre charge de travail au sein de ces piliers.
3. Après avoir obtenu des résultats satisfaisants, répétez avec plus de piliers.

Pour réduire davantage la portée, utilisez des objectifs spécialement conçus pour vos charges de travail.

Personnes et culture

Chaque charge de travail a besoin d'un propriétaire, et de nombreuses personnes et équipes peuvent être impliquées dans le cycle de vie d'une charge de travail. Toutefois, avant d'exécuter un WAFR, définissez un propriétaire monothread (STO) pour la charge de travail.

Cette personne doit être capable de prendre des décisions et de contrôler le budget, les effectifs et la feuille de route. Des exemples de ce rôle sont un propriétaire de produit, un chef de produit, un architecte en chef ou un responsable de l'ingénierie.

En fin de compte, ce rôle est responsable si la charge de travail ne fonctionne plus comme prévu.

Il est important de gérer un WAFR avec un STO pour améliorer vos résultats. Par exemple, vous pouvez trouver des éléments d'amélioration pour la charge de travail, mais vous ne parvenez pas à les hiérarchiser dans la feuille de route du produit. Il se peut également que vous ayez du mal à obtenir le financement ou les ressources nécessaires à l'exécution du travail.

Cela se traduit souvent par la collecte d'une liste irréalisable d'articles en attente. Le STO vous aide à éviter ce résultat, car il est propriétaire du WAFR et il est investi dans le processus.

Parties prenantes requises

Le STO ne peut pas répondre à toutes les questions. De nombreuses personnes et équipes participent à l'architecture, au développement, à la sécurisation ou à l'exploitation d'une charge de travail. En fonction de l'organisation et de l'ampleur de la charge de travail, le nombre de parties prenantes et d'équipes impliquées varie.

Réfléchissez aux questions suivantes concernant les parties prenantes :

1. Qui doit être présent pour répondre à chaque catégorie de questions ?
2. Quelles parties prenantes sont tenues d'être présentes pendant quelles parties du WAFR ?
3. Comment pouvez-vous informer les différentes parties prenantes des questions à l'avance ?

Sponsors du pilier

Le cadre Well-Architected Framework repose sur six piliers. Bien que la définition d'un STO soit cruciale, il est tout aussi important de recueillir le soutien de sponsors ou de champions spécifiques aux piliers afin d'accélérer et d'accroître la valeur du processus WAFR.

Définissez les sponsors ou champions piliers qui peuvent :

- Assister à des parties spécifiques du WAFR pour fournir des informations ou des conseils
- Maîtriser les résultats dans leur domaine
- Définir, influencer et communiquer les changements stratégiques interorganisationnels

Votre organisation dispose-t-elle d'un centre d'excellence ou d'une communauté de pratique sur le cloud ? Commencez modestement et formez un groupe de personnes partageant les mêmes idées

qui peuvent se soutenir mutuellement dans le cadre de discussions et d'améliorations sur la santé architecturale.

Création d'un espace sécurisé

Le développement d'une culture organisationnelle saine est essentiel pour des discussions saines et productives sur les choix technologiques. Le groupe de personnes impliquées dans le WAFR peut être nouveau ou ancien, avoir un mandat et une ancienneté différents, ou être impliqué en tant que partenaires ou tiers. Il est essentiel d'entretenir une conversation saine et respectueuse au sujet d'une charge de travail afin d'améliorer les chances d'une amélioration durable et utile.

Définissez une intention positive dès le début et insistez à nouveau pendant la totalité du processus pour maintenir l'alignement et concentrez-vous sur la découverte d'opportunités d'amélioration. La technologie et les bonnes pratiques évoluent, c'est pourquoi un WAFR doit être conçu comme une opportunité de découvrir des améliorations.

Un WAFR n'est pas un audit. Bien que les résultats puissent vous aider à respecter différentes normes de conformité, il n'existe pas de processus permettant de « noter » une charge de travail. Concentrez-vous sur l'amélioration de la santé architecturale.

Un WAFR est l'occasion de se demander « où en sommes-nous ? » et d'obtenir une vue ponctuelle de la charge de travail. Ensuite, vous pouvez utiliser les résultats pour prendre une décision éclairée et répondre à la question « où devons-nous aller ? »

L'amélioration architecturale est un parcours guidé par AWS Well-Architected. Lorsque vous commencez votre processus WAFR, posez-vous les questions suivantes :

1. Pourquoi exécutez-vous le WAFR ?
2. Qu'espérez-vous en retirer ?
3. Quels seront les avantages de cette expérience pour tout le monde ?
4. Où êtes-vous actuellement et où souhaitez-vous vous rendre ?

Ressources

- Article de blog sur la responsabilisation
- Équipe de deux pizzas Amazon

Documentation et infrastructure

Lorsque vous exécuterez une WAFR, vous constaterez peut-être que pour la plupart des bonnes pratiques que vous suivez, vous disposez d'un processus documenté, d'une procédure opérationnelle standard (SOP), d'un dossier d'exploitation ou d'un playbook. Pendant la WAFR, enregistrez les informations et le contexte dans le champ de notes de l'outil Well-Architected (WA Tool). Vous pouvez gagner du temps lors de la révision en rassemblant à l'avance tous les artefacts de documentation pertinents relatifs à la charge de travail.

Lorsque vous étudiez votre documentation, posez-vous les questions suivantes :

- Quelle documentation existe sur la charge de travail ?
- Quels sont les documents manquants ?
- Quels outils seraient utilisés pour créer et stocker ces artefacts ?
- Qui participerait à la création et à la maintenance de ces artefacts ?

Voici quelques exemples de documentation concernant votre charge de travail :

- Pages wiki sur la charge de travail
- Schéma de l'architecture
- Dossier de décisions architecturales
- Procédures opérationnelles standard
- Référentiels d'infrastructure en tant que code (IaC)
- Topologie du réseau
- Playbooks et dossiers d'exploitation
- Structure organisationnelle
- Documentation de la stratégie multicompte
- Configuration du fournisseur d'identité central
- Configuration de la solution de surveillance centralisée
- Documentation pour les charges de travail dépendantes
- Guide de référence des API
- Versions de la bibliothèque logicielle
- Processus et historique de correction des erreurs (COE)
- Stratégie d'ingénierie du chaos
- Informations sur l'équipe de test de charge
- Modèle de la menace

- Rétrospectives de l'équipe
- Documents de la journée de jeu

Antimodèles

Si aucune de ces ressources n'existe, vous pouvez toujours exécuter la WAFR en tant que mécanisme de découverte. Toutefois, le processus peut prendre plus de temps sans ces artefacts. La création de ressources documentaires peut être la première étape vers l'amélioration de la santé architecturale.

Découverte des charges de travail

Il est difficile de passer en revue efficacement une architecture sans connaître ses composants et ses ressources. Les charges de travail existantes évoluent souvent au fil du temps ou changent de propriétaire, et elles n'ont peut-être pas été définies à l'aide d'outils d'infrastructure en tant que code (IaC) tels que AWS CloudFormation, AWS CDK ou Terraform.

Avant de discuter des améliorations, comprenez les différents composants architecturaux de la charge de travail et ses dépendances, et créez une représentation visuelle afin de fournir une compréhension partagée.

De nombreux outils tiers de découverte et de création de diagrammes automatiques sont disponibles directement auprès des fournisseurs de logiciels, de AWS Marketplace ou sous forme de solutions open source.

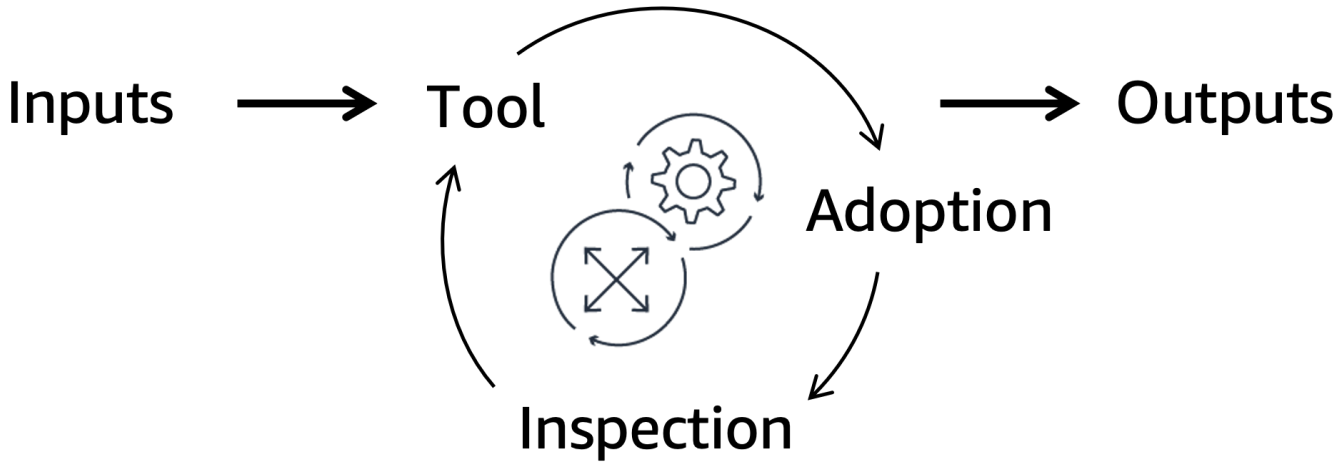
Ressources

- Schémas d'architecture de référence AWS
- Processus des dossiers de décisions architecturales
- Page d'accueil GitHub ADR
- Pourquoi mettre en place la correction des erreurs (COE)
- Découverte de la charge de travail sur la solution AWS

Mécanismes

Les mécanismes remplacent les meilleurs efforts humains par des processus et des outils reproductibles et évolutifs, souvent automatisés, pour obtenir le résultat souhaité. Un mécanisme est

un cycle complet dans lequel vous créez un outil ou un processus, pilotez son adoption et inspectez les résultats pour apporter des corrections de cap. Ce cycle prend des intrants contrôlables et les transforme en résultats permanents pour relever un défi commercial récurrent.



La nature cyclique d'un mécanisme le rend plus adapté pour résoudre des problèmes ou des opportunités récurrents. Le WAFR est un mécanisme doté d'un outil, d'un processus d'adoption et d'un processus d'inspection qui fonctionnent tous selon un cycle complet.

Lorsque vous effectuez des WAFR sur vos charges de travail, vous identifiez les opportunités d'amélioration pour développer d'autres mécanismes au sein de votre organisation. Les résultats d'un WAFR ne devraient pas être des solutions ponctuelles pour une seule équipe, mais devraient plutôt être partagés entre plusieurs équipes afin d'apporter le maximum de valeur.

Résultats métier

Avant de commencer à apporter des modifications technologiques, déterminez les priorités de votre entreprise. Il est moins efficace de revoir votre architecture sans une compréhension claire des priorités de votre organisation. Ces priorités peuvent servir de lignes directrices pour vous aider à maintenir l'alignement et à obtenir de meilleurs résultats.

Les résultats commerciaux sont des objectifs commerciaux clés à forte valeur ajoutée qui sont liés à la stratégie organisationnelle et déterminés par les commentaires des clients. Ils sont délibérément de haut niveau afin que les différentes équipes puissent définir des objectifs plus spécifiques pour atteindre ces résultats.

Voici des exemples de résultats commerciaux courants :

- Réduction des coûts

- Augmentation de la capacité
- Amélioration de la satisfaction de vos clients
- Amélioration de la rétention des clients
- Amélioration de la rétention du personnel
- Amélioration de la durabilité environnementale
- Niveau de sécurité amélioré

Le fait de connaître les résultats commerciaux de votre organisation et de travailler en rétrospective vous permet de gagner du temps en vous concentrant sur les changements technologiques susceptibles d'avoir le plus d'impact sur les objectifs de votre organisation. Cela renforce à son tour la confiance avec vos dirigeants.

Découvrez et discutez des priorités commerciales actuelles de votre organisation, de votre unité commerciale ou de votre équipe.

Ressources

- Comment effectuer une révision du cadre Well-Architected – Partie 1

Exécution d'un WAFR

Après toute la préparation requise, il est temps pour vous de lancer une révision du cadre Well-Architected (WAFR). Dans cette section, nous allons explorer des conseils et astuces pour devenir plus efficace lors de la conduite de votre WAFR.

Avant le WAFR

Avant de commencer à discuter de la charge de travail en groupe, passez en revue la section suivante et discutez des règles d'engagement pour la session. Vous devriez avoir un consensus au sein de votre groupe sur la façon de procéder.

Définition des rôles et des responsabilités

- Qui dirige le WAFR ?
- Qui partagera son écran et qu'est-ce qu'il y partagera ?
- Qui prendra des notes dans l'outil WA ou dans un autre format ?
- Quels piliers allez-vous examiner et dans quel ordre ?

- Avez-vous les bonnes personnes dans la salle pour répondre aux questions ?
- Comment allez-vous saisir les éléments hors de portée et comment créerez-vous votre carnet de commandes pour ces articles ?
- Combien de temps souhaitez-vous consacrer à chaque section ou pilier ?
- Que souhaitez-vous accomplir dans le temps qui vous est imparti ?

Conseils sur les performances

Planifiez les réunions autour de la capture de points de données relatifs aux choix architecturaux de la charge de travail. Vous pouvez faire un certain nombre de choses pour rendre cette section du WAFR aussi fluide que possible.

1. Communiquez une intention positive : revoyez l'intention positive du WAFR avec les participants. Les conversations critiques sur le travail peuvent être difficiles, alors réaffirmez que le WAFR est mis en œuvre pour trouver des opportunités d'amélioration. Renforcez la culture du non-blâme. Il n'y a ni attaque ni défense, mais plutôt une discussion collaborative sur l'amélioration de l'architecture.
2. Faites appel à un supporter : gérer une architecture de charge de travail complexe, poser des questions, modérer les réponses et prendre des notes peut s'avérer difficile pour une seule personne. Un WAFR réussi est une activité d'équipe. Désignez des rôles alternatifs, ce qui permet à une personne de mener la révision tandis qu'une autre prend des notes, vérifie la documentation et surveille la discussion.
3. Restez concentré sur le sujet : lors de conversations de groupe sur des décisions architecturales, les gens se laissent souvent distraire. Si vous voulez gagner du temps, assurez-vous que les participants au WAFR veillent à ce que chacun reste sur le sujet. Capturez les concepts secondaires et les idées dans un endroit centralisé qui pourra être repris lors de futures sessions de discussion.
4. Prenez de bonnes notes : le simple fait de cocher des cases dans l'outil WA ne fournit pas suffisamment de contexte pour revoir le WAFR ultérieurement. Utilisez la zone de notes de l'outil WA ou créez un document externe lié à partir de la zone de notes WAFR si vous dépassez la limite de caractères. Le contexte aide les autres parties, en particulier les personnes dont la charge de travail est nouvelle, à comprendre le travail en cours et à déterminer les priorités.
5. Ne vous concentrez pas sur les solutions : concentrez-vous sur la capture de points de données relatifs à la charge de travail plutôt que sur les solutions. Trop vous concentrer sur les solutions peut vous faire perdre du temps pendant votre session WAFR et vous empêcher de capturer des points de données importants. Ce n'est pas la meilleure façon d'utiliser le temps des autres participants si vous réfléchissez à quelque chose qui est hors de portée.

6. Concentrez-vous sur la charge de travail, pas sur l'outil : il est courant que les utilisateurs partagent leur écran montrant l'outil Well-Architected (WA Tool) dans la AWS Management Console. Bien que la capture de données dans l'outil WA soit cruciale, ne vous concentrez pas uniquement sur l'outil. Concentrez plutôt votre discussion sur l'architecture. Faites en sorte que l'évaluation reste conversationnelle et paraphrasez les questions en fonction du contexte.
7. Divisez la discussion en plusieurs parties : il peut être difficile de passer en revue les six piliers en une seule réunion. Répartissez l'évaluation en sessions plus petites, ce qui permet une approche plus ciblée sur le sujet et peut être plus facile à planifier avec vos participants.
8. N'oubliez pas de faire des pauses : une révision approfondie de l'architecture peut être fatigante pour les participants, et leur concentration peut s'amenuiser au fil du temps. Prévoyez des pauses fréquentes pendant le WAFR. Réduisez le temps des participants et permettez aux participants de se déplacer lorsqu'ils ne sont plus nécessaires.
9. Réfléchissez bien aux possibilités : si vous trouvez que la réponse à une question est « peut-être », « en quelque sorte » ou « nous avons quelque chose en attente pour y remédier », demandez-vous si cela signifie réellement « non ». Un WAFR consiste à capturer l'état honnête et actuel de la charge de travail, et non l'état prévu.
10. Envisagez des compromis : Well-Architected consiste à faire des compromis entre les piliers. Rendre une charge de travail plus résiliente peut se faire au détriment de l'optimisation des coûts, ou une optimisation plus poussée des coûts peut avoir un impact sur l'impact environnemental de votre charge de travail. Les piliers sont là pour structurer vos conversations et pour vous aider à faire des choix architecturaux éclairés.
11. Reconnaissez qu'aucune charge de travail ne peut être parfaite : les charges de travail sont rarement parfaites et n'ont souvent pas besoin de l'être. Évitez de transformer votre WAFR en un exercice visant à tout perfectionner, et concentrez-vous sur le fait que la charge de travail fonctionne de manière sûre et efficace pour l'objectif commercial auquel elle est destinée.

Exécution du WAFR

Exécutez le WAFR Compte AWS parallèlement à la charge de travail. Vous pouvez ensuite partager l'examen de la charge de travail avec d'autres Comptes AWS.

Partagez l'avis avec un compte central à l'aide de AWS Organizations. Vous pouvez ensuite utiliser le tableau de bord pour visualiser les charges de travail de votre organisation de manière centralisée.

Cela peut vous aider à identifier les types de risques et les améliorations à apporter à toutes vos charges de travail. Vous pouvez ensuite relever le défi de manière centralisée grâce à une approche

basée sur des modèles qui peut être partagée et utilisée sur de nombreux comptes et charges de travail.

Accès à IAM

L'accès au AWS WA Tool dans AWS Management Console nécessite des autorisations IAM. Déterminez à l'avance qui a besoin d'un accès pour gagner du temps au début de la session WAFR.

Pour plus d'informations, consultez Octroi aux utilisateurs, groupes ou rôles de l'accès à AWS Well-Architected Tool.

Vous pouvez configurer un rôle IAM entre comptes pour permettre aux parties prenantes externes d'accéder à l'outil WA et de modifier ou de consulter les avis.

Ressources

- Comment effectuer une révision du cadre Well-Architected – Partie 2

Amélioration de votre charge de travail

À ce stade, vous avez préparé le WAFR, effectué un examen et évalué votre charge de travail par rapport aux bonnes pratiques AWS.

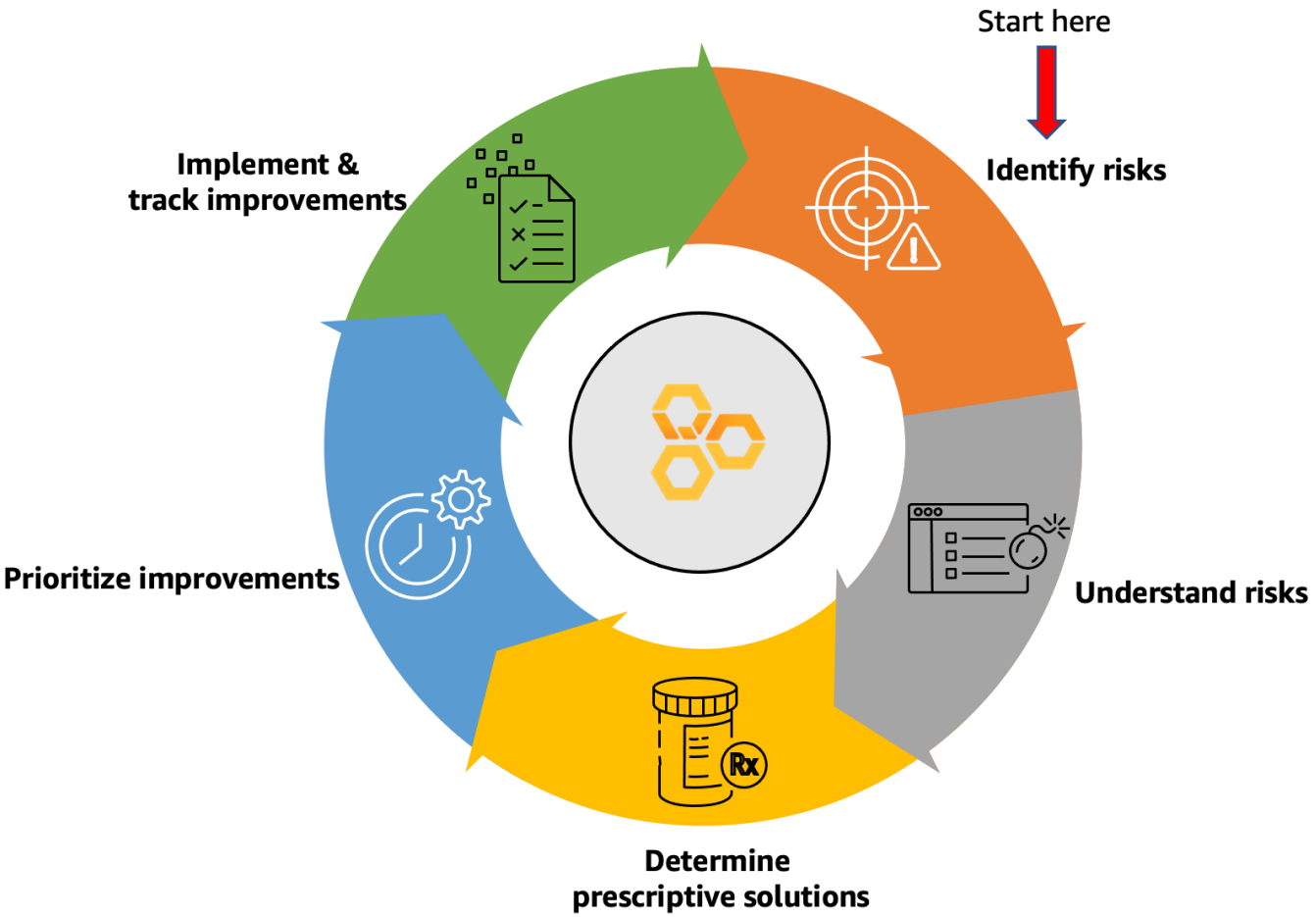
Les résultats du WAFR auront identifié les risques architecturaux sur la base des réponses recueillies lors de l'examen. Ces risques sont classés en deux catégories : problèmes à risque élevé (HRI) et problèmes à risque moyen (MRI).

Au cours de la dernière phase, vous créerez un plan d'amélioration qui consiste à créer une liste des risques, à comprendre leur impact sur votre entreprise, à identifier des solutions et à mettre en œuvre ces solutions conformément aux priorités de votre organisation.

Les sections suivantes fournissent des instructions détaillées pour le processus d'amélioration de la charge de travail :

- Identification et compréhension des risques
- Définition des solutions prescriptives
- Priorisation des améliorations
- Mise en œuvre et suivi des améliorations

Le cycle suivant montre les principales étapes incluses dans la phase d'amélioration du WAFR.



Identification et compréhension des risques

Considérez les risques identifiés comme des opportunités d'amélioration.

Il existe deux catégories de risques dans le contexte d'un WAFR : les problèmes à risque élevé (HRI) et à risque moyen (MRI).

- Les problèmes à risque élevé sont des choix architecturaux et opérationnels qu'AWS a détectés comme pouvant avoir un impact négatif important sur une entreprise. Une bonne pratique en matière de risque élevé est considérée comme une pratique fondamentale et incontournable au sein d'un pilier. Elle peut avoir un impact sur les opérations, les actifs et les individus de l'organisation. Par exemple, un HRI associé au pilier de sécurité est la non sécurisation de votre Compte AWS.
- Les problèmes à risque moyen (MRI) sont des choix qui peuvent également avoir un impact négatif sur votre entreprise, mais dans une moindre mesure que les HRI. Une bonne pratique en matière

de risque moyen est une pratique susceptible d'améliorer considérablement la charge de travail. Un exemple de MRI sur le pilier de sécurité consiste à ne pas auditer et à alterner régulièrement les informations d'identification.

Génération d'un rapport

La première étape pour identifier visuellement les HRI et les MRI consiste à générer un rapport indiquant les risques liés à chaque charge de travail que vous avez examinée.

Le tableau de bord AWS Well-Architected Tool (AWS WA Tool) permet d'accéder à vos charges de travail et aux HRI et MRI associés. Vous pouvez également inclure les charges de travail qui ont été partagées avec vous. À l'aide du tableau de bord, vous pouvez filtrer les problèmes par charge de travail, pilier ou gravité (élevée ou moyenne).

Sur la page du tableau de bord, vous pouvez voir la liste des HRI et des MRI filtrés par pilier ou par gravité. Une fois qu'un élément d'amélioration est sélectionné, il vous amène directement aux meilleures pratiques qui lui sont associées à partir du cadre Well-Architected. À partir de là, vous pouvez en savoir plus sur les mesures à prendre pour résoudre le problème, ainsi que sur les ressources nécessaires.

Vous pouvez combiner tous ces résultats dans un seul rapport en choisissant Générer un rapport dans le tableau de bord de WA Tool.

Nous vous recommandons d'envoyer un e-mail récapitulatif aux participants au WAFR avec le rapport, et de résumer les principaux résultats et le plan d'amélioration suggéré pour les préparer à l'étape suivante.

Gestion des risques

Pour gérer efficacement un risque, il est essentiel de définir le risque et son niveau acceptable. Grâce à l'analyse des risques, découvrez quels sont les problèmes potentiels et comment savoir s'il s'agit de véritables problèmes.

Il existe deux méthodes principales pour effectuer une évaluation des risques :

- Quantitative : utilise des données objectives pondérées pour évaluer l'impact d'un risque en termes de dépassement des coûts, de consommation de ressources et de retards dans le calendrier.
- Qualitative : utilise des données subjectives non liées aux valeurs réelles des coûts ou des avantages pour mesurer la probabilité et l'impact global.

Dans certains cas, vous pouvez finir par utiliser une approche hybride qui combine le meilleur des deux approches pour évaluer l'impact d'un risque.

Lorsque vous évaluez le niveau de risque sur la base des définitions HRI et MRI, pensez à vous poser les questions suivantes :

- Quelle est la probabilité que le risque ait un impact ?
- Quel serait l'impact sur le client ?
- Quel serait l'impact sur l'entreprise ?
- Le risque peut-il être totalement éliminé ou seulement atténué ?
- Qui est responsable du risque ?
- Qui est responsable des travaux d'amélioration à supprimer ou à atténuer ?
- Quelle est la probabilité que ce résultat se reproduise ? Cela risque-t-il d'avoir le même impact ?
- Pouvez-vous identifier une relation entre la probabilité d'un résultat et un schéma de récurrence ?

Le fait de demander aux principales parties prenantes ou aux propriétaires d'entreprise de répondre à ces questions vous aidera à créer une liste des risques les plus importants sur lesquels vous devez vous concentrer, ainsi que le temps prévu pour y faire face.

Ampleur du risque

Vous pouvez utiliser le tableau suivant pour déterminer l'ampleur du risque :

Probabilité x impact	Négligeable (1)	Mineur (2)	Modéré (3)	Majeur (4)	Critique (5)
Presque certain (5)	5	10	15	20	25
Probablement (4)	4	8	12	26	20
Possible (3)	3	6	9	12	15
Peu probable (2)	2	4	6	8	10
Rare (1)	1	2	3	4	5

Travaillez en groupe sur les HRI et les MRI et sur les risques qu'ils présentent pour les entreprises. Créez une liste des HRI qui doivent être traités. Classez les risques en fonction de leur importance pour l'entreprise afin d'établir un ordre de priorité.

Définition des solutions prescriptives

Une fois que les risques et les opportunités d'amélioration sont compris dans le contexte de votre organisation, travaillez avec les équipes sur les mesures d'atténuation. À ce stade, chaque équipe doit travailler sur les HRI présents dans leur région et définir une solution prescriptive pour y remédier.

Cette étape peut nécessiter des recherches supplémentaires, des discussions ou l'élaboration de preuves de concepts. Il est important de ne pas perdre trop de temps à aborder les détails de mise en œuvre d'une solution au cours de cette phase. Cela se produira plus tard si vous décidez que le HRI en question est une priorité.

Le but de cette étape est de comprendre la complexité de la solution et les ressources nécessaires afin que vous puissiez en tenir compte lors de la priorisation des tâches en fonction du temps, de la complexité et de l'impact.

Travaillez en groupe afin de dresser une liste de solutions possibles pour les HRI. Gardez les choses à un niveau élevé et n'entrez pas dans les détails de mise en œuvre.

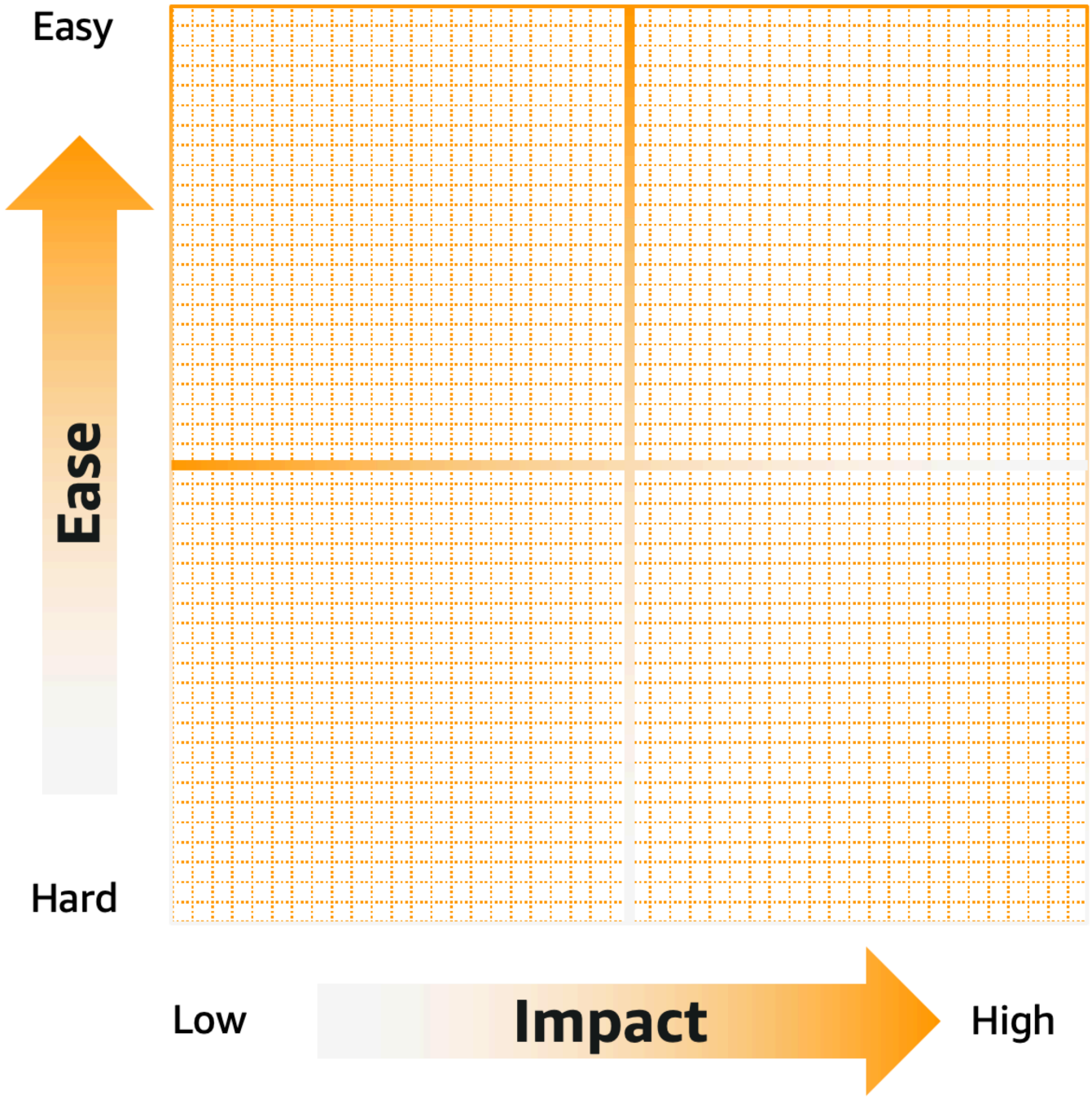
Priorisation des améliorations

Aucune organisation ne dispose d'un temps et de ressources illimités. Le fait d'aborder tous les HRI et les MRI identifiés en même temps n'est peut-être pas la bonne façon de tirer le meilleur parti d'un WAFR.

Commencez par un certain nombre de problèmes qui peuvent avoir le plus d'impact sur l'entreprise et qui sont plus faciles à mettre en œuvre. Travaillez sur la solution. Suivez l'amélioration, puis répétez cette approche.

Priorisation de la mise en œuvre

L'une des approches qui peut vous aider à visualiser la priorité des solutions est la matrice Eisenhower. Il existe différentes façons d'utiliser cet outil. Lors de l'évaluation, tenez compte à la fois de l'importance de l'amélioration (valeur qu'elle apporte à votre entreprise) et des efforts déployés pour la mettre en œuvre (temps requis, complexité de la mise en œuvre ou effectifs).



Le résultat de cette analyse fournit un ensemble de risques qui ont le plus d'impact sur votre entreprise, mais qui ne sont pas trop complexes à mettre en œuvre. Ce sont de bons candidats à mettre en œuvre dès la première itération.

Caractéristiques des solutions

Lorsque vous sélectionnez une solution pour un risque identifié, tenez compte des points suivants :

- Objectifs SMART : pensez à des objectifs spécifiques, mesurables, réalisables, pertinents et limités dans le temps (SMART).
- Propriétaires : pour chaque solution, identifiez un propriétaire.
- Plus simple que complexe : les solutions complexes peuvent fonctionner, mais elles rendent l'amélioration plus difficile à mettre en œuvre et leur création peut prendre plus de temps. Privilégiez la simplicité à la complexité, sauf si la solution complexe est une exigence non négociable.
- Prenez des décisions bidirectionnelles : les solutions doivent être extensibles et conçues pour s'améliorer et évoluer au fil du temps. Dans la mesure du possible, évitez les solutions statiques qui ne peuvent pas s'adapter au fur et à mesure du développement de votre architecture.
- Cibler des solutions basées sur des modèles : envisagez des solutions qui peuvent être codifiées, réutilisées et repartagées. Ne réinventez pas la roue. Accédez au Centre d'architecture AWS pour obtenir des exemples.
- Travaillez continuellement en équipe : travaillez en groupe pour créer une liste de solutions pour les HRI. Classez-les par ordre de priorité dans une matrice d'Eisenhower.

Mise en œuvre et suivi des améliorations

Le résultat idéal d'une mise en œuvre réussie est une réduction du nombre de HRI et de MRI, ce qui se traduit par une amélioration de la santé architecturale de votre charge de travail.

La mise en œuvre des mesures correctives doit être effectuée de manière itérative, en utilisant des jalons dans l'outil WA qui enregistrent l'état d'une charge de travail à un moment donné. Chaque fois que vous organisez une session de révision ou que vous terminez des améliorations, enregistrez un jalon pour mesurer les progrès au fur et à mesure.

WAFR en mode agile

Les résultats d'un exercice de priorisation du WAFR peuvent être utilisés pour hiérarchiser les tickets pour les sprints et les backlogs des équipes de développement. Les développeurs doivent être en mesure de comprendre l'impact des mises en œuvre et de s'approprier la contribution à l'amélioration de la santé architecturale. L'amélioration et le suivi du WAFR peuvent être intégrés dans une rétrospective agile.

Les rétrospectives sont des réunions organisées à la fin d'une itération ou des sprints. Au cours de la rétrospective, l'équipe réfléchit à ce qui s'est passé au cours de l'itération et identifie les mesures à prendre pour l'avenir. Il s'agit d'un mécanisme idéal pour inclure les évaluations du WAFR à des fins de discussion et donner aux membres les moyens de renforcer la santé architecturale.

Chronologie

Le calendrier de ces étapes varie d'une organisation à l'autre, chaque organisation étant différente et confrontée à des défis uniques. Cependant, suite à des WAFRs réussis réalisés auprès de nombreux clients chez AWS, nous recommandons que cette phase dure entre 90 et 180 jours.

Si votre liste de HRI et de MRI prend plus de temps, redéfinissez les priorités et établissez une liste plus courte afin de pouvoir commencer à pratiquer le processus pour obtenir des améliorations. Répétez ensuite avec les éléments restants.

Chronologie après le WAFR

Un jour après le WAFR :

1. Créez un e-mail récapitulatif avec le plan d'amélioration et résumez :
   - Qui a participé à l'évaluation
   - Principaux résultats
   - Planifier les prochaines étapes
2. Joindre le plan d'amélioration
3. Orienter les équipes vers la planification

Deux à trois jours après le WAFR :

1. Créez une réunion de priorisation des HRI et hiérarchisez les HRI :
   - Par effort
   - Par impact
   - Avec les équipes responsables des charges de travail
2. Collaborez sur ce qui compte vraiment le plus pour l'entreprise

Une semaine après le WAFR :

1. Commencez le plan d'amélioration
2. Tenez compte des recommandations suivantes :
   - Durée : 90 ou 180 jours
   - Identifier les HRI prioritaires

- Élaborer des mesures d’atténuation pour chacun
- Essayer de maximiser les initiatives pour résoudre plusieurs HRI

Tâches de routine :

1. Établir une cadence pour les réunions de suivi concernant le plan d’amélioration
2. Passer en revue les mesures à prendre pour améliorer la charge de travail
3. Tenez compte des recommandations suivantes :
   - Définir les attentes des participants
   - Leur envoyer les liens vers les questions WA
   - Procéder à des examens de suivi

Charges de travail

Une charge de travail est un ensemble de ressources et de code qui fournit une valeur business, par exemple une application destinée au client ou un processus dorsal.

Une charge de travail peut se composer d’un sous-ensemble de ressources dans un même Compte AWS ou être un ensemble de plusieurs ressources couvrant plusieurs Comptes AWS. Une petite entreprise peut avoir seulement quelques charges de travail alors qu’une grande entreprise peut en avoir plusieurs milliers.

La page Workloads (Charges de travail), disponible dans le volet de navigation de gauche, fournit des informations sur vos charges de travail et toutes les charges de travail partagées avec vous.

Les informations suivantes sont affichées pour chaque charge de travail :

Nom

Le nom de la charge de travail.

Owner

L’ID de Compte AWS propriétaire de la charge de travail.

Réponses aux questions

Le nombre de questions auxquelles nous avons répondu.

Risques élevés

Le nombre de problèmes à risque élevé identifiés.

Risques moyens

Le nombre de problèmes à risque moyen identifiés.

Statut d'amélioration

Le statut d'amélioration que vous avez défini pour la charge de travail :

- Aucune
- Non démarré
- En cours
- Complet
- Risque accepté

Date de la dernière mise à jour

Date et heure de la dernière mise à jour de la charge de travail.

Une fois que vous avez choisi une charge de travail dans la liste :

- Pour examiner les détails de la charge de travail, charge, choisissez View details (Afficher les détails).
- Pour modifier les propriétés de la charge de travail, choisissez Modifier.
- Pour gérer le partage de la charge de travail avec d'autres Comptes AWS, utilisateurs, AWS Organizations ou unités organisationnelles (UO), choisissez Afficher les détails, puis Partages.
- Pour supprimer la charge de travail et tous ses jalons, choisissez Supprimer. Seul le propriétaire de la charge de travail peut la supprimer.

> **Warning**
>
> La suppression d'une charge de travail ne peut pas être annulée. Toutes les données associées à la charge de travail sont supprimées.

Problèmes à risque élevé et problèmes à risque moyen

Les problèmes à risque élevé identifiés dans AWS Well-Architected Tool sont des choix architecturaux et opérationnels qu'AWS a détectés comme pouvant avoir un impact négatif important sur une entreprise. Ces problèmes peuvent avoir une incidence sur les opérations, les biens et les personnes de l'organisation. Les problèmes à risque moyen peuvent également avoir un impact négatif sur les entreprises, mais dans une moindre mesure. Ces problèmes sont basés sur vos réponses dans le AWS Well-Architected Tool. Les bonnes pratiques correspondantes sont largement appliquées par AWS et les clients AWS. Ces bonnes pratiques sont composées des orientations définies par le cadre AWS Well-Architected Framework et ses objectifs.

> **Note**
>
> Il s'agit seulement de lignes directrices ; il est de la responsabilité des clients d'évaluer et de mesurer l'impact du non respect des bonnes pratiques sur leur entreprise. Si des raisons techniques ou commerciales spécifiques empêchent l'application d'une bonne pratique à

la charge de travail, le risque peut être inférieur à celui indiqué. AWS suggère aux clients de documenter ces raisons et leur incidence sur la bonne pratique dans les notes relatives à la charge de travail. Pour tous les problèmes à risque élevé ou moyen, AWS suggère aux clients de mettre en œuvre les bonnes pratiques telles que définies dans AWS Well-Architected Tool. Si la bonne pratique est mise en œuvre, indiquez que le problème a été résolu en marquant la bonne pratique telle que présentée dans le AWS Well-Architected Tool. Si les clients choisissent de ne pas mettre en œuvre la bonne pratique, AWS leur suggère de documenter l'approbation applicable au niveau de l'entreprise et les raisons pour lesquelles ils ne la mettent pas en œuvre.

Définir une charge de travail dans AWS Well-Architected Tool

Il existe deux façons de définir une charge de travail. Sur la page Charges de travail, dans AWS WA Tool, vous pouvez définir une charge de travail sans modèle. Sur la page Modèles d'examen, vous pouvez également utiliser un modèle d'examen existant ou créer un nouveau modèle pour définir une charge de travail.

Pour définir une charge de travail à partir de la page Charges de travail

1. Dans le volet de navigation de gauche, sélectionnez Charges de travail.
2. Sélectionnez le menu déroulant Définir la charge de travail.
3. Choisissez Define workload (Définir une charge de travail). Ou, si vous avez créé un modèle d'examen et que vous souhaitez définir une charge de travail à partir de celui-ci, choisissez Définir à partir d'un modèle d'examen.
4. Suivez les instructions dans the section called "Définition d'une charge de travail" pour spécifier les propriétés de la charge de travail ou (éventuellement) appliquez des profils et des objectifs.

Pour définir une charge de travail à partir de la page Modèles d'examen

1. Dans le volet de navigation de gauche, sélectionnez Modèles d'examen.
2. Sélectionnez le nom d'un modèle d'examen existant ou suivez les instructions dans the section called "Création d'un modèle d'avis" pour créer un nouveau modèle d'examen.
3. Choisissez Définir la charge de travail à partir du modèle.
4. Suivez les instructions fournies dans the section called "Définition d'une charge de travail à partir d'un modèle" pour créer la charge de travail à partir de votre modèle d'examen.

Affichage d'une charge de travail dans AWS Well-Architected Tool

Vous pouvez afficher les détails des charges de travail que vous possédez et des charges de travail partagées avec vous.

Pour afficher une charge de travail

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.
2. Dans le panneau de navigation de gauche, choisissez Workloads (Charges de travail).
3. Sélectionnez la charge de travail à afficher de l'une des manières suivantes :
   - Choisissez le nom de la charge de travail.
   - Sélectionnez la charge de travail et choisissez View details (Afficher les détails).

La page de détails de la charge de travail s'affiche.

> **Note**
>
> Un champ obligatoire, Review owner (Responsable de la vérification), a été ajouté pour vous permettre d'identifier facilement la personne ou le groupe principal responsable du processus de vérification.
> La première fois que vous affichez une charge de travail définie avant l'ajout de ce champ, vous êtes informé de cette modification. Choisissez Edit (Modifier) pour définir le champ Review owner (Responsable de la vérification). Aucune autre action n'est requise.
> Choisissez Acknowledge (Accepter) pour différer la définition du champ Review owner (Responsable de la vérification). Pendant les 60 prochains jours, une bannière s'affiche pour vous rappeler que le champ est vide. Pour supprimer cette bannière, modifiez votre charge de travail et spécifiez un responsable de vérification.
> Si vous ne définissez pas le champ avant la date spécifiée, votre accès à la charge de travail est limité. Vous pouvez continuer à afficher la charge de travail et la supprimer, mais vous ne pouvez pas la modifier, sauf pour définir le champ Review owner (Responsable de la vérification). L'accès partagé à la charge de travail n'est pas affecté tant que votre accès est limité.

Modification d'une charge de travail dans AWS Well-Architected Tool

Vous pouvez modifier les détails d'une charge de travail que vous possédez.

Pour modifier une charge de travail

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.
2. Dans le panneau de navigation de gauche, choisissez Workloads (Charges de travail).
3. Sélectionnez la charge de travail à modifier, puis choisissez Modifier.
4. Apportez vos modifications à la charge de travail.

   Pour obtenir une description de chacun des champs, veuillez consulter Définition d'une charge de travail dans l'AWS WA Tool.

   > **Note**
   >
   > Lorsque vous mettez à jour une charge de travail existante, vous pouvez activer Trusted Advisor, ce qui crée automatiquement le rôle IAM pour le propriétaire de la charge de travail. Les propriétaires des comptes associés aux charges de travail qui ont activé Trusted Advisor doivent créer un rôle dans IAM. Pour en savoir plus, consultez the section called "Activation de Trusted Advisor dans IAM".

5. Choisissez Enregistrer pour enregistrer vos modifications de la charge de travail.

   Si un champ obligatoire est vide ou si une valeur spécifiée n'est pas valide, vous devez corriger le problème avant que vos mises à jour de la charge de travail soient enregistrées.

Partage d'une charge de travail dans AWS Well-Architected Tool

Vous pouvez partager une charge de travail dont vous êtes propriétaire avec d'autres Comptes AWS, des utilisateurs, une organisation et des unités organisationnelles (UO) dans la même Région AWS.

> **Note**
>
> Vous pouvez uniquement partager des charges de travail au sein de la même Région AWS.

Lorsque vous partagez une charge de travail avec un autre Compte AWS, si le destinataire n'a pas l'autorisation `wellarchitected:UpdateShareInvitation`, il ne peut pas accepter l'invitation de partage. Consultez the section called "Octroi de l'accès à l'AWS WA Tool" pour voir des exemples de politiques d'autorisation.

Pour partager une charge de travail avec d'autres Comptes AWS et utilisateurs

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.
2. Dans le panneau de navigation de gauche, choisissez Workloads (Charges de travail).
3. Sélectionnez une charge de travail que vous possédez de l'une des manières suivantes :
   - Choisissez le nom de la charge de travail.
   - Sélectionnez la charge de travail et choisissez View details (Afficher les détails).
4. Choisissez Shares (Partages). Choisissez ensuite Créer et Créer des partages avec des comptes ou des utilisateurs pour créer une invitation à la charge de travail.
5. Saisissez l'ID de Compte AWS à 12 chiffres ou l'ARN de l'utilisateur avec lequel vous souhaitez partager la charge de travail.
6. Choisissez l'autorisation que vous souhaitez accorder.

   Read-Only

   Fournit un accès en lecture seule à la charge de travail.

   Participant

   Fournit un accès mis à jour aux réponses et à leurs notes, et un accès en lecture seule au reste de la charge de travail.
7. Choisissez Créer pour envoyer une invitation à la charge de travail au Compte AWS ou à l'utilisateur spécifié.

Si l'invitation de charge de travail n'est pas acceptée dans les sept jours, elle expire automatiquement.

Si un utilisateur et son Compte AWS ont tous deux des invitations à la charge de travail, l'invitation à la charge de travail avec le niveau d'autorisation le plus élevé est appliquée à l'utilisateur.

> **Important**
>
> Avant de partager une charge de travail avec une organisation ou des unités organisationnelles (UO), vous devez activer l'accès à AWS Organizations.

Pour partager une charge de travail avec votre organisation ou vos unités organisationnelles

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.
2. Dans le panneau de navigation de gauche, choisissez Workloads (Charges de travail).
3. Sélectionnez une charge de travail que vous possédez de l'une des manières suivantes :
   - Choisissez le nom de la charge de travail.
   - Sélectionnez la charge de travail et choisissez View details (Afficher les détails).
4. Choisissez Shares (Partages). Choisissez ensuite Créer and Créer des partages avec des organisations.
5. Sur la page Créer un partage de charge de travail, choisissez d'accorder des autorisations à l'ensemble de l'organisation ou à une ou plusieurs unités organisationnelles.
6. Choisissez l'autorisation que vous souhaitez accorder.

   Read-Only

   Fournit un accès en lecture seule à la charge de travail.

   Participant

   Fournit un accès mis à jour aux réponses et à leurs notes, et un accès en lecture seule au reste de la charge de travail.
7. Choisissez Créer pour partager la charge de travail.

Pour savoir qui a un accès partagé à une charge de travail, choisissez Shares (Partages) dans la page Affichage des détails de la charge de travail dans AWS Well-Architected Tool.

Pour empêcher une entité de partager des charges de travail, attachez une stratégie qui refuse les actions `wellarchitected:CreateWorkloadShare`.

Vous pouvez également partager les objectifs personnalisés que vous possédez avec d'autres Comptes AWS, des utilisateurs, votre organisation et les unités organisationnelles dans la même

Région AWS. Pour plus d'informations, consultez Partage d'un cadre personnalisé dans AWS WA Tool.

Considérations relatives au partage des charges de travail AWS Well-Architected Tool

Une charge de travail peut être partagée avec un maximum de 20 Comptes AWS et utilisateurs différents. Une charge de travail ne peut être partagée qu'avec des comptes et des utilisateurs qui se trouvent dans la même Région AWS que la charge de travail.

Pour partager une charge de travail dans une région introduite après le 20 mars 2019, vous et le Compte AWS partagé devez activer la région dans la AWS Management Console. Pour plus d'informations, consultez Infrastructure mondiale AWS.

Vous pouvez partager une charge de travail avec un Compte AWS, des utilisateurs IAM individuels dans un compte, ou les deux. Lorsque vous partagez une charge de travail avec un Compte AWS, tous les utilisateurs de ce compte ont accès à la charge de travail. Si seuls des utilisateurs spécifiques d'un compte ont besoin d'un accès, suivez la bonne pratique consistant à accorder le moindre privilège et à partager la charge de travail individuellement avec ces utilisateurs.

Si un Compte AWS et un utilisateur du compte ont des invitations à la charge de travail, l'invitation à la charge de travail avec les autorisations de niveau le plus élevé détermine l'utilisateur autorisé à accéder à la charge de travail. Si vous supprimez l'invitation à la charge de travail pour l'utilisateur, l'accès de l'utilisateur est déterminé par l'invitation à la charge de travail pour le Compte AWS. Supprimez les deux invitations de charge de travail pour supprimer l'accès de l'utilisateur à la charge de travail.

Avant de partager une charge de travail avec une organisation ou une ou plusieurs unités organisationnelles (UO), vous devez activer l'accès à AWS Organizations.

Si vous partagez une charge de travail à la fois avec une organisation et une ou plusieurs unités organisationnelles, l'invitation à la charge de travail avec les autorisations les plus élevées détermine le compte autorisé à accéder à la charge de travail.

Pour activer le partage AWS Organizations

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.
2. Dans le panneau de navigation de gauche, choisissez Paramètres.

3. Choisissez Activer la prise en charge d'AWS Organizations.
4. Choisissez Save settings (Enregistrer les paramètres).

Suppression de l'accès partagé dans AWS Well-Architected Tool

Vous pouvez supprimer une invitation de charge de travail. La suppression d'une invitation de charge de travail supprime l'accès partagé à la charge de travail.

Pour supprimer l'accès partagé à une charge de travail

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.
2. Dans le panneau de navigation de gauche, choisissez Workloads (Charges de travail).
3. Sélectionnez la charge de travail à afficher de l'une des manières suivantes :
   - Choisissez le nom de la charge de travail.
   - Sélectionnez la charge de travail et choisissez View details (Afficher les détails).
4. Choisissez Shares (Partages).
5. Sélectionnez l'invitation de charge de travail à supprimer et choisissez Delete (Supprimer).
6. Choisissez Supprimer pour confirmer.

Si un utilisateur et le Compte AWS de l'utilisateur ont des invitations à une charge de travail, vous devez supprimer les deux invitations pour supprimer l'autorisation de l'utilisateur à accéder à la charge de travail.

Modification de l'accès partagé dans AWS Well-Architected Tool

Vous pouvez modifier une invitation de charge de travail en attente ou acceptée.

Pour modifier l'accès partagé à une charge de travail

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.
2. Dans le panneau de navigation de gauche, choisissez Workloads (Charges de travail).
3. Sélectionnez une charge de travail que vous possédez de l'une des manières suivantes :
   - Choisissez le nom de la charge de travail.

- Sélectionnez la charge de travail et choisissez View details (Afficher les détails).

4. Choisissez Shares (Partages).
5. Sélectionnez l'invitation de charge de travail à modifier et choisissez Edit (Modifier).
6. Choisissez la nouvelle autorisation que vous souhaitez accorder au Compte AWS ou à l'utilisateur.

   Read-Only

   Fournit un accès en lecture seule à la charge de travail.

   Participant

   Fournit un accès mis à jour aux réponses et à leurs notes, et un accès en lecture seule au reste de la charge de travail.
7. Choisissez Enregistrer.

Si l'invitation de charge de travail modifiée n'est pas acceptée dans les sept jours, elle expire automatiquement.

Acceptation et refus d'invitations à une charge de travail dans AWS Well-Architected Tool

Une invitation à une charge de travail est une demande de partage d'une charge de travail appartenant à un autre Compte AWS. Si vous acceptez l'invitation de charge travail, cette dernière est ajoutée à vos pages Workloads (Charges de travail) et Dashboard (Tableau de bord). Si vous refusez l'invitation de charge de travail, elle est supprimée de la liste des invitations de charge de travail.

Vous disposez de sept jours pour accepter une invitation de charge de travail. Si vous n'acceptez pas l'invitation dans les sept jours, elle expire automatiquement.

> **Note**
>
> Les charges de travail peuvent uniquement être partagées au sein de la même Région AWS.

Pour accepter ou rejeter une invitation de charge de travail

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.
2. Dans le volet de navigation de gauche, choisissez Workload invitations (Invitations de charge de travail).
3. Sélectionnez l'invitation de charge de travail à accepter ou à rejeter.
   - Pour accepter l'invitation de charge de travail, choisissez Accept (Accepter).

     La charge de travail est ajoutée aux pages Workloads (Charges de travail) et Dashboard (Tableau de bord).
   - Pour refuser l'invitation de charge globale, choisissez Reject (Refuser).

     L'invitation de charge de travail est supprimée de la liste.

Pour refuser l'accès partagé après l'acceptation d'une invitation de charge de travail, choisissez Reject share (Refuser le partage) dans la page Affichage des détails de la charge de travail dans AWS Well-Architected Tool correspondant à la charge de travail.

Suppression d'une charge de travail dans AWS Well-Architected Tool

Lorsque vous n'avez plus besoin d'une charge de travail, vous pouvez la supprimer. La suppression d'une charge de travail supprime toutes les données associées à cette dernière, y compris les jalons et les invitations de partage de charge de travail. Seul le propriétaire d'une charge de travail peut la supprimer.

> **Warning**
>
> La suppression d'une charge de travail ne peut pas être annulée. Toutes les données associées à la charge de travail sont définitivement supprimées.

Pour supprimer une charge de travail

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.

2. Dans le panneau de navigation de gauche, choisissez Workloads (Charges de travail).
3. Sélectionnez la charge de travail que vous voulez supprimer et choisissez Supprimer.
4. Dans la fenêtre Supprimer, choisissez Supprimer pour confirmer la suppression de la charge de travail et de ses jalons.

Pour éviter qu'une entité supprime des charges de travail, attachez une stratégie qui refuse les actions `wellarchitected:DeleteWorkload`.

Génération d'un rapport de charge de travail dans AWS Well-Architected Tool

Vous pouvez générer un rapport de charge de travail pour un cadre. Le rapport contient les réponses aux questions de l'examen de la charge de travail, vos notes, et le nombre actuel de risques élevés et moyens identifiés dans la charge de travail. Si une question comporte un ou plusieurs risques identifiés, le plan d'amélioration associé à cette question répertorie les mesures que vous pouvez prendre pour atténuer ces risques.

Si un profil est associé à votre charge de travail, les informations générales du profil et les risques prioritaires figurent dans le rapport sur la charge de travail.

Un rapport vous permet de partager des détails sur la charge de travail avec d'autres utilisateurs qui n'ont pas accès à AWS Well-Architected Tool.

Pour générer un rapport de charge de travail

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.
2. Dans le panneau de navigation de gauche, choisissez Workloads (Charges de travail).
3. Sélectionnez la charge de travail et choisissez View details (Afficher les détails).
4. Sélectionnez le cadre pour lequel vous souhaitez générer un rapport et choisissez Generate report (Générer un rapport).

   Le rapport est généré et vous pouvez le télécharger ou l'afficher.

Affichage des détails de la charge de travail dans AWS Well-Architected Tool

La page Détails de la charge de travail fournit des informations sur votre charge de travail, y compris ses jalons, son plan d'amélioration et ses partages de charge de travail. Utilisez les onglets en haut de la page pour accéder aux différentes sections des détails.

Pour supprimer la charge de travail, choisissez Delete workload (Supprimer la charge de travail). Seul le propriétaire d'une charge de travail peut la supprimer.

Pour supprimer votre accès à une charge de travail partagée, choisissez Reject share (Refuser le partage).

Rubriques

Onglet Présentation d'AWS Well-Architected Tool

Lorsque vous avez initialement affiché une charge de travail, l'onglet Overview (Présentation) affiche les premières informations. Cet onglet fournit l'état global de votre charge de travail suivi de l'état de chaque cadre.

Si vous n'avez pas répondu à toutes les questions, une bannière s'affiche pour vous rappeler de commencer ou de continuer à documenter votre charge de travail.

La section Workload overview (Présentation de la charge de travail) affiche l'état global actuel de la charge de travail et toutes les Workload notes (Notes de charge de travail) que vous avez entrées. Choisissez Modifier pour mettre à jour l'état ou les notes.

Pour capturer l'état actuel de la charge de travail, choisissez Save milestone (Enregistrer le jalon). Les jalons sont immuables et ne peuvent pas être modifiés une fois qu'ils sont enregistrés.

Pour continuer à documenter l'état de la charge de travail, choisissez Start reviewing (Démarrer la vérification) et sélectionnez le cadre souhaité.

Onglet Jalons d'AWS Well-Architected Tool

Pour afficher les jalons de votre charge de travail, choisissez l'onglet Jalons.

Une fois que vous avez sélectionné un jalon, choisissez Générer un rapport pour créer le rapport de charge de travail associé au jalon. Le rapport contient les réponses aux questions relatives à la charge de travail, à vos notes et au nombre de risques élevés et moyens dans la charge de travail au moment où le jalon a été enregistré.

Vous pouvez afficher les détails sur l'état de votre charge de travail au moment d'un jalon spécifique soit en :

- Choisissant le nom du jalon.
- Sélectionnant le jalon et en choisissant View milestone (Afficher le jalon).

Onglet Propriétés d'AWS Well-Architected Tool

Pour afficher les propriétés de votre charge de travail, choisissez l'onglet Propriétés. Initialement, ces propriétés sont les valeurs qui ont été spécifiées lors de la définition de la charge de travail. Vous pouvez choisir Edit (Modifier) pour effectuer des changements. Seul le propriétaire de la charge de travail peut apporter des modifications.

Pour voir des descriptions des propriétés, consultez Définition d'une charge de travail dans l'AWS WA Tool.

Onglet Partages d'AWS Well-Architected Tool

Pour afficher ou modifier vos invitations de charge de travail, choisissez l'onglet Shares (Partages). Cet onglet s'affiche uniquement pour le propriétaire d'une charge de travail.

Les informations suivantes s'affichent pour chaque Compte AWS et utilisateur ayant un accès partagé à la charge de travail :

Principal

L'ID de Compte AWS ou l'ARN de l'utilisateur avec un accès partagé à la charge de travail.

Statut

Statut de l'invitation de charge de travail.

- En attente

  L'invitation est en attente d'être acceptée ou refusée. Si une invitation de charge de travail n'est pas acceptée dans les sept jours, elle expire automatiquement.

- Acceptée

  L'invitation a été acceptée.

- Refusée

  L'invitation a été refusée.

- Expiré

  L'invitation n'a pas été acceptée ou refusée dans un délai de sept jours.

Autorisations

Autorisation accordée au Compte AWS ou à l’utilisateur.

- Read-Only

  Le mandataire dispose d'un accès en lecture seule à la charge de travail.

- Participant

  Le mandataire peut mettre à jour les réponses et leurs notes, et dispose d'un accès en lecture seule au reste de la charge de travail.

Détails de l’autorisation

Description détaillée de l'autorisation.

Pour partager la charge de travail avec un autre Compte AWS ou utilisateur dans la même Région AWS, choisissez Créer. Une charge de travail peut être partagée avec un maximum de 20 Comptes AWS et utilisateurs différents.

Pour supprimer une invitation de charge de travail, sélectionnez l'invitation et choisissez Delete (Supprimer).

Pour modifier une invitation de charge de travail, sélectionnez l'invitation et choisissez Edit (Modifier).

Utilisation des cadres dans AWS WA Tool

Dans l'AWS Well-Architected Tool, les cadres vous permettent d'évaluer continuellement vos architectures par rapport aux bonnes pratiques et d'identifier les points à améliorer. La Cadre AWS Well-Architected est automatiquement appliqué lorsqu'une charge de travail est définie.

Un ou plusieurs cadres peuvent être appliqués à une charge de travail. Chaque cadre a son propre ensemble de questions, de bonnes pratiques, de notes et de plan d'amélioration.

Deux types de cadres peuvent être appliqués à vos charges de travail : les cadres du catalogue Lens et les cadres personnalisés.

- Catalogue Lens : cadres officiels créés et maintenus par AWS. Le catalogue Lens est accessible à tous les utilisateurs et ne nécessite aucune installation supplémentaire.
- Cadres personnalisés : cadres définis par l'utilisateur qui ne sont pas du contenu AWS officiel. Vous pouvez créer des cadres personnalisés avec vos propres piliers, questions, bonnes pratiques et plans d'amélioration, ainsi que partager des cadres personnalisés avec d'autres Comptes AWS.

Cinq cadres peuvent être ajoutés à la fois à une charge de travail, avec un maximum de 20 cadres appliqués à une charge de travail.

Si un cadre est supprimé d'une charge de travail, les données associées au cadre sont conservées. Les données sont restaurées si vous ajoutez à nouveau le cadre à la charge de travail.

Ajout d'un cadre à une charge de travail dans AWS WA Tool

L'ajout d'un cadre à une charge de travail vous permet de mieux comprendre les forces et les faiblesses de votre architecture, d'identifier les améliorations et de vous assurer que vos charges de travail respectent les bonnes pratiques.

Pour ajouter un cadre à une charge de travail

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.
2. Dans le panneau de navigation de gauche, choisissez Workloads (Charges de travail).
3. Sélectionnez la charge de travail et choisissez View details (Afficher les détails).

4. Sélectionnez le cadre à ajouter et choisissez Enregistrer.

   Les cadres peuvent être sélectionnés dans Lentilles personnalisées, le catalogue Lens ou les deux.

Jusqu'à 20 objectifs peuvent être ajoutés à une charge de travail.

Pour plus d'informations sur le catalogue Lens AWS, rendez-vous sur Lentilles AWS Well-Architected. Notez que le livre blanc de chaque cadre n'est pas fourni sous forme de cadre dans le catalogue Lens.

> **Exclusion de responsabilité**
>
> En accédant et/ou en appliquant des objectifs personnalisés créés par un autre utilisateur ou compte AWS, vous reconnaissez que les objectifs personnalisés créés par d'autres utilisateurs et partagés avec vous constituent un contenu tiers tel que défini dans le contrat client AWS.

Suppression d'un cadre d'une charge de travail dans AWS WA Tool

Si un cadre n'est plus adapté à votre charge de travail, vous pouvez le supprimer.

Pour supprimer un cadre d'une charge de travail

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.
2. Dans le panneau de navigation de gauche, choisissez Workloads (Charges de travail).
3. Sélectionnez la charge de travail et choisissez View details (Afficher les détails).
4. Désélectionnez le cadre à supprimer et choisissez Enregistrer.

   Le Cadre AWS Well-Architected ne peut pas être supprimé d'une charge de travail.

Les données associées au cadre sont conservées. Si le cadre est à nouveau ajouté à la charge de travail, les données sont restaurées.

Affichage des détails des cadres pour une charge de travail dans AWS WA Tool

Vous pouvez afficher les détails de vos cadres dans la console AWS Well-Architected Tool. Pour afficher les détails relatif à un cadre, sélectionnez celui-ci.

Onglet Overview (Présentation)

L'onglet Overview (Vue d'ensemble) fournit des informations générales sur le cadre, telles que le nombre de questions auxquelles une réponse a été donnée. À partir de cet onglet, vous pouvez continuer à examiner une charge de travail, générer un rapport ou modifier les notes du cadre.

Onglet Plan d’amélioration

L'onglet Improvement Plan (Plan d'amélioration) fournit une liste des actions recommandées pour améliorer votre charge de travail. Vous pouvez filtrer les recommandations en fonction du risque et du pilier.

Onglet Partages

Pour un cadre personnalisé, l’onglet Partages fournit la liste des principaux IAM avec lesquels le cadre a été partagé.

Cadres personnalisés pour les charges de travail dans AWS WA Tool

Vous pouvez créer des cadres personnalisés avec vos propres piliers, questions, bonnes pratiques et plan d’amélioration. Vous appliquez des cadres personnalisés à une charge de travail de la même manière que vous appliquez les cadres fournis par AWS. Vous pouvez également partager les cadres personnalisés que vous créez avec d’autres Comptes AWS, et les cadres personnalisés appartenant à d’autres personnes peuvent être partagés avec vous.

Vous pouvez adapter les questions dans un cadre personnalisé pour qu’elles soient spécifiques à une technologie particulière, vous aident à répondre aux besoins de gouvernance au sein de votre organisation ou étendent les conseils fournis par le cadre Well-Architected et les cadres AWS. À l’instar des cadres existants, vous pouvez suivre les progrès au fil du temps en créant des jalons et fournir un statut périodique en générant des rapports.

Rubriques

Affichage des cadres personnalisés dans AWS WA Tool

Vous pouvez afficher les détails des cadres personnalisés que vous possédez et des cadres personnalisés qui ont été partagés avec vous.

Pour afficher un cadre

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.
2. Dans le volet de navigation de gauche, choisissez Lentilles personnalisées.

   > **Note**
   >
   > La section Lentilles personnalisées est vide si vous n'avez pas créé de cadre personnalisé ou si aucun cadre personnalisé n'a été partagé avec vous.

3. Choisissez les cadres personnalisés que vous souhaitez afficher :
   - En ma possession : affiche les cadres personnalisés que vous avez créés.
   - En partage : affiche les cadres personnalisés qui ont été partagés avec vous.
4. Sélectionnez le cadre personnalisé à afficher de l'une des manières suivantes :
   - Choisissez le nom du cadre.
   - Sélectionnez le cadre et choisissez Afficher les détails.

La page Affichage des détails des cadres pour une charge de travail dans AWS WA Tool s'affiche.

La page Cadres personnalisés contient les champs suivants :

Nom

Nom du cadre.

Propriétaire

Identifiant du Compte AWS propriétaire du cadre personnalisé.

Statut

Le statut PUBLIÉ signifie que le cadre personnalisé a été publié et peut être appliqué aux charges de travail ou partagé avec d'autres Comptes AWS.

Le statut BROUILLON signifie que le cadre personnalisé a été créé mais n'a pas encore été publié. Un cadre personnalisé doit être publié avant de pouvoir être appliqué aux charges de travail ou partagé.

Version

Nom de la version du cadre personnalisé.

Dernière mise à jour

Date et heure de la dernière mise à jour des cadres personnalisés.

Création d'un cadre personnalisé pour une charge de travail dans AWS WA Tool

Pour créer un cadre personnalisé

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.
2. Dans le volet de navigation de gauche, choisissez Lentilles personnalisées.
3. Choisissez Créer un cadre personnalisé.
4. Choisissez Télécharger le fichier pour télécharger le fichier de modèle JSON.
5. Ouvrez le fichier de modèle JSON avec votre éditeur de texte préféré et ajoutez les données pour votre cadre personnalisé. Ces données incluent vos piliers, vos questions, vos bonnes pratiques et les liens vers les plans d'amélioration.

Pour plus d'informations, consultez Spécification du format des cadres dans AWS WA Tool. La taille d'un cadre personnalisé ne peut pas dépasser 500 Ko.

6. Choisissez Choisir un fichier pour sélectionner votre fichier JSON.
7. (Facultatif) Dans la section Balises, ajoutez les balises que vous souhaitez associer au cadre personnalisé.
8. Choisissez Soumettre et prévisualiser pour prévisualiser le cadre personnalisé, ou Soumettre pour soumettre le cadre personnalisé sans prévisualisation.

   Si vous choisissez de soumettre et prévisualiser votre cadre personnalisé, vous pouvez sélectionner Suivant pour naviguer dans l'aperçu du cadre, ou sélectionner Quitter l'aperçu pour revenir à la page Lentilles personnalisées.

Si la validation échoue, modifiez votre fichier JSON et réessayez de créer le cadre personnalisé.

Une fois qu'AWS WA Tool a validé votre fichier JSON, votre cadre personnalisé est affiché dans Lentilles personnalisées.

Une fois qu'un cadre personnalisé a été créé, il passe au statut BROUILLON. Vous devez publier le cadre avant de l'appliquer à des charges de travail ou de le partager avec d'autres Comptes AWS.

Vous pouvez créer jusqu'à 15 cadres personnalisés dans un Compte AWS.

> **Exclusion de responsabilité**
>
> N'incluez et ne collectez pas de données d'identification personnelle (PII) d'utilisateurs finaux ou d'autres personnes identifiables dans ou via vos cadres personnalisés. Si votre cadre personnalisé ou ceux partagés avec vous et utilisés dans votre compte incluent ou collectent des données d'identification personnelle, vous devez : vous assurer que les données d'identification personnelle incluses sont traitées conformément à la loi applicable, fournir des avis de confidentialité adéquats et obtenir les consentements nécessaires pour traiter ces données.

Prévisualisation d'un cadre personnalisé pour une charge de travail dans AWS WA Tool

Pour prévisualiser un cadre personnalisé

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.
2. Dans le volet de navigation de gauche, choisissez Lentilles personnalisées.
3. Seuls les cadres dotés du statut BROUILLON peuvent être prévisualisés. Sélectionnez le cadre personnalisé BROUILLON souhaité et choisissez Prévisualiser l'expérience.
4. Choisissez Suivant pour parcourir l'aperçu du cadre.
5. (Facultatif) Vous pouvez examiner votre plan d'amélioration en sélectionnant les bonnes pratiques pour chaque question de l'aperçu et en choisissant Mettre à jour selon les réponses pour tester votre logique de risque. Si des modifications sont nécessaires, vous pouvez mettre à jour les règles de risque dans votre modèle JSON avant de le publier.
6. Choisissez Quitter l'aperçu pour revenir au cadre personnalisé.

> **Note**
>
> Vous pouvez également prévisualiser un cadre personnalisé en sélectionnant Soumettre et prévisualiser lors de la création d'un cadre personnalisé.

Publication d'un cadre personnalisé dans AWS WA Tool pour la première fois

Pour publier un cadre personnalisé

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.
2. Dans le volet de navigation de gauche, choisissez Lentilles personnalisées.
3. Sélectionnez le cadre personnalisé souhaité, puis choisissez Publier la lentille.
4. Dans le champ Nom de la version, entrez un identifiant unique pour le changement de version. Cette valeur peut comporter jusqu'à 32 caractères et ne doit contenir que des caractères alphanumériques et des points (« . »).

5. Choisissez Publier une lentille personnalisée.

   Une fois qu'un cadre personnalisé a été publié, il prend le statut PUBLIÉ.

Le cadre personnalisé peut désormais être appliqué aux charges de travail ou partagé avec d'autres utilisateurs ou Comptes AWS.

Publication d'une mise à jour d'un cadre personnalisé dans AWS WA Tool

Pour publier une mise à jour d'un cadre personnalisé existant

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.
2. Dans le volet de navigation de gauche, choisissez Lentilles personnalisées.
3. Sélectionnez le cadre personnalisé souhaité et choisissez Modifier.
4. Si aucun fichier JSON mis à jour n'est prêt, choisissez Télécharger le fichier pour télécharger une copie du cadre personnalisé actuel. Modifiez le fichier JSON téléchargé à l'aide de votre éditeur de texte préféré et apportez les modifications souhaitées.
5. Choisissez Choisir un fichier pour sélectionner votre fichier JSON mis à jour et choisissez Soumettre et prévisualiser pour prévisualiser le cadre personnalisé, ou Soumettre pour soumettre le cadre personnalisé sans prévisualisation.

   La taille d'un cadre personnalisé ne peut pas dépasser 500 Ko.

   Une fois qu'AWS WA Tool a validé votre fichier JSON, votre cadre personnalisé est affiché dans Lentilles personnalisées avec le statut BROUILLON.
6. Sélectionnez à nouveau le cadre personnalisé et choisissez Publier la lentille.
7. Choisissez Vérifier les modifications avant de les publier pour vérifier que les modifications apportées à votre cadre personnalisé sont correctes. Cela inclut la validation des éléments suivants :

   - Nom du cadre personnalisé
   - Noms des piliers
   - Questions nouvelles, mises à jour et supprimées

   Choisissez Suivant.

8. Spécifiez le type de changement de version.

   Version majeure

   Indique que des changements substantiels ont été apportés au cadre. À utiliser pour les changements qui ont un impact sur la signification du cadre personnalisé.

   Toutes les charges de travail auxquelles le cadre a été appliqué seront informées qu'une nouvelle version du cadre personnalisé est disponible.

   Les changements de version majeurs ne sont pas automatiquement appliqués aux charges de travail utilisant le cadre.

   Version mineure

   Indique que des changements mineurs ont été apportés au cadre. À utiliser pour de petites modifications, telles que des modifications de texte ou des mises à jour des liens URL.

   Les changements de version mineurs sont automatiquement appliqués aux charges de travail utilisant le cadre personnalisé.

   Choisissez Suivant.

9. Dans le champ Nom de la version, entrez un identifiant unique pour le changement de version. Cette valeur peut comporter jusqu'à 32 caractères et ne doit contenir que des caractères alphanumériques et des points (« . »).
10. Choisissez Publier une lentille personnalisée.

    Une fois qu'un cadre personnalisé a été publié, il prend le statut PUBLIÉ.

Le cadre personnalisé mis à jour peut désormais être appliqué aux charges de travail ou partagé avec d'autres utilisateurs ou Comptes AWS.

Si la mise à jour est un changement de version majeur, toutes les charges de travail associées à la version précédente du cadre seront informées qu'une nouvelle version est disponible et auront la possibilité de procéder à une mise à niveau.

Les mises à jour de version mineure sont automatiquement appliquées sans notification.

Vous pouvez créer jusqu'à 100 versions d'un cadre personnalisé.

Partage d'un cadre personnalisé dans AWS WA Tool

Vous pouvez partager un cadre personnalisé avec d'autres Comptes AWS, utilisateurs et unités d'organisation (UO).

Pour partager un cadre personnalisé avec d'autres Comptes AWS et utilisateurs

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.
2. Dans le volet de navigation de gauche, choisissez Lentilles personnalisées.
3. Sélectionnez le cadre personnalisé à partager et choisissez Afficher les détails.
4. Sur la page Affichage des détails des cadres pour une charge de travail dans AWS WA Tool, choisissez Partagers. Choisissez ensuite Créer et Créer des partages avec des comptes ou des utilisateurs pour créer une invitation de partage de cadre.
5. Saisissez l'ID de Compte AWS à 12 chiffres ou l'ARN de l'utilisateur avec lequel vous souhaitez partager le cadre personnalisé.
6. Choisissez Créer pour envoyer une invitation de partage de cadre au Compte AWS ou à l'utilisateur spécifié.

Vous pouvez partager un cadre personnalisé avec un maximum de 300 Comptes AWS ou utilisateurs.

Si l'invitation de partage de cadre n'est pas acceptée dans les sept jours, elle expire automatiquement.

> **Important**
>
> Avant de partager un cadre personnalisé avec une organisation ou des unités d'organisation (UO), vous devez activer l'accès AWS Organizations.

Pour partager un cadre personnalisé avec votre organisation ou vos unités d'organisation

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.
2. Dans le volet de navigation de gauche, choisissez Lentilles personnalisées.

3. Sélectionnez le cadre personnalisé à partager.
4. Sur la page Affichage des détails des cadres pour une charge de travail dans AWS WA Tool, choisissez Partagers. Choisissez ensuite Créer and Créer des partages avec des organisations.
5. Sur la page Créer un partage de lentille personnalisée, choisissez d'accorder des autorisations à l'ensemble de l'organisation ou à une ou plusieurs unités d'organisation.
6. Choisissez Créer pour partager le cadre personnalisé.

Pour savoir qui a un accès partagé à un cadre personnalisé, choisissez Partages dans la page Affichage des détails des cadres pour une charge de travail dans AWS WA Tool.

> **Exclusion de responsabilité**
>
> En partageant vos cadres personnalisés avec d'autres Comptes AWS, vous reconnaissez qu'AWS mettra vos cadres personnalisés à la disposition de ces autres comptes. Ces autres comptes pourront continuer à accéder à vos cadres personnalisés partagés et à les utiliser même si vous supprimez les cadres personnalisés de votre propre Compte AWS ou si vous résiliez votre Compte AWS.

Ajout de balises à un cadre personnalisé dans AWS WA Tool

Pour ajouter des balises à un cadre personnalisé

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.
2. Dans le volet de navigation de gauche, choisissez Lentilles personnalisées.
3. Sélectionnez le cadre personnalisé que vous souhaitez mettre à jour.
4. Dans la section Balises, choisissez Gérer les balises.
5. Sélectionnez Ajouter une nouvelle balise et entrez la clé et la valeur de chaque balise à ajouter.
6. Sélectionnez Save.

Pour supprimer une balise, choisissez Supprimer en regard de la balise que vous souhaitez supprimer.

Suppression d'un cadre personnalisé dans AWS WA Tool

Pour supprimer un cadre personnalisé

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.
2. Dans le volet de navigation de gauche, choisissez Lentilles personnalisées.
3. Sélectionnez le cadre personnalisé à supprimer, puis choisissez Supprimer.
4. Sélectionnez Delete (Supprimer).

   Les charges de travail existantes auxquelles le cadre est appliqué sont informées que le cadre personnalisé a été supprimé, mais peuvent continuer à l'utiliser. Le cadre personnalisé ne peut plus être appliqué aux nouvelles charges de travail.

> **Exclusion de responsabilité**
>
> En partageant vos cadres personnalisés avec d'autres Comptes AWS, vous reconnaissez qu'AWS mettra vos cadres personnalisés à la disposition de ces autres comptes. Ces autres comptes pourront continuer à accéder à vos cadres personnalisés partagés et à les utiliser même si vous supprimez les cadres personnalisés de votre propre Compte AWS ou si vous résiliez votre Compte AWS.

Spécification du format des cadres dans AWS WA Tool

Les cadres sont définis à l'aide d'un format JSON spécifique. Lorsque vous commencez à créer un cadre personnalisé, vous avez la possibilité de télécharger un fichier de modèle JSON. Vous pouvez utiliser ce fichier comme base pour vos cadres personnalisés car il définit la structure de base des piliers, des questions, des bonnes pratiques et du plan d'amélioration.

Section du cadre

Cette section définit les attributs du cadre personnalisé lui-même. Il s'agit de son nom et de sa description.

- `schemaVersion` : version du schéma du cadre personnalisé à utiliser. Défini par le modèle, à ne pas modifier.

- `name` : nom du cadre. La longueur maximale du nom est de 128 caractères.
- `description` : description textuelle du cadre. Ce texte s'affiche lorsque vous sélectionnez des cadres à ajouter lors de la création de la charge de travail ou lorsque vous sélectionnez un cadre à appliquer ultérieurement à une charge de travail existante. La description peut comporter jusqu'à 2 048 caractères.

```
   "schemaVersion": "2021-11-01",
   "name": "Company Policy ABC",
   "description": "This lens provides a set of specific questions to assess compliance
with company policy ABC-2021 as revised on 2021/09/01.",
```

Section « pillars »

Cette section définit les piliers associés au cadre personnalisé. Vous pouvez mapper vos questions aux piliers du cadre AWS Well-Architected, définir vos propres piliers, ou les deux.

Vous pouvez définir jusqu'à 10 piliers dans un cadre personnalisé.

- `id` : ID du pilier. L'identifiant peut comporter entre 3 et 128 caractères et ne peut contenir que des caractères alphanumériques et des traits de soulignement (« _ »). Les identifiants utilisés dans un pilier doivent être uniques.

  Lorsque vous mappez vos questions aux piliers du cadre, utilisez les identifiants suivants :

  - `operationalExcellence`
  - `security`
  - `reliability`
  - `performance`
  - `costOptimization`
  - `sustainability`
- `name` : nom du pilier. La longueur maximale du nom est de 128 caractères.

```
    "pillars": [
       {
           "id": "company_Privacy",
           "name": "Privacy Excellence",
```

```
            .
            .
            .
        },
        {
            "id": "company_Security",
            "name": "Security",
            .
            .
            .
        }
    ]
```

Section « questions »

Cette section définit les questions associées à un pilier.

Vous pouvez définir jusqu'à 20 questions dans un pilier d'un cadre personnalisé.

- `id` : identifiant de la question. L'identifiant peut comporter entre 3 et 128 caractères et ne peut contenir que des caractères alphanumériques et des traits de soulignement (« _ »). Les identifiants utilisés dans une question doivent être uniques.
- `title` : intitulé de la question. La longueur maximale de l'intitulé est de 128 caractères.
- `description` : décrit la question de manière plus détaillée. La description peut comporter jusqu'à 2 048 caractères.
- `helpfulResource displayText` : facultatif. Texte fournissant des informations utiles sur la question. La longueur maximale du texte est de 2 048 caractères. Il doit être spécifié, si `helpfulResource url` est spécifié.
- `helpfulResource url` : facultatif. Une ressource URL qui explique la question plus en détail. L'URL doit commencer par `http://` ou `https://`.

> **Note**
>
> Lorsque vous synchronisez la charge de travail d'un cadre personnalisé avec Jira, la section « questions » affiche à la fois les éléments « id » et « title » de la question.
> Le format utilisé dans les tickets Jira est `[ QuestionID ] QuestionTitle`.

```
"questions": [
    {
        "id": "privacy01",
        "title": "How do you ensure HR conversations are private?",
        "description": "Career and benefits discussions should occur on secure channels
 only and be audited regularly for compliance.",
        "helpfulResource": {
            "displayText": "This is helpful text for the first question",
            "url": "https://example.com/poptquest01_help.html"
        },
        .
        .
        .
    },
    {
        "id": "privacy02",
        "title": "Is your team following the company privacy policy?",
        "description": "Our company requires customers to opt-in to data use and does
 not disclose customer data to third parties either individually or in aggregate.",
        "helpfulResource": {
            "displayText": "This is helpful text for the second question",
            "url": "https://example.com/poptquest02_help.html"
        },
        .
        .
        .
    }
]
```

Section « choices »

Cette section définit les choix associées à une question.

Vous pouvez définir jusqu'à 15 choix pour une question dans un cadre personnalisé.

- `id` : identifiant du choix. L'identifiant peut comporter entre 3 et 128 caractères et ne peut contenir que des caractères alphanumériques et des traits de soulignement (« _ »). Un identifiant unique doit être spécifié pour chaque choix d'une question. L'ajout d'un choix avec le suffixe _no fera office de choix `None of these` pour la question.
- `title` : intitulé du choix. La longueur maximale de l'intitulé est de 128 caractères.

- `helpfulResource displayText` : facultatif. Texte fournissant des informations utiles sur un choix. La longueur maximale du texte est de 2 048 caractères. Doit être inclus si `helpfulResource url` est spécifié.
- `helpfulResource url` : facultatif. Une ressource URL qui explique le choix plus en détail. L'URL doit commencer par `http://` ou `https://`.
- `improvementPlan displayText` : texte qui décrit comment un choix peut être amélioré. La longueur maximale du texte est de 2 048 caractères. Un élément `improvementPlan` est requis pour chaque choix, sauf pour un choix `None of these`.
- `improvementPlan url` : facultatif. Une ressource URL qui peut contribuer à l'amélioration. L'URL doit commencer par `http://` ou `https://`.
- `additionalResources type` : facultatif. Type de ressources supplémentaires. La valeur peut être `HELPFUL_RESOURCE` ou `IMPROVEMENT_PLAN`.
- `additionalResources content` : facultatif. Spécifie les valeurs `displayText` et `url` pour la ressource supplémentaire. Jusqu'à cinq ressources utiles supplémentaires et jusqu'à cinq éléments supplémentaires du plan d'amélioration peuvent être spécifiés pour un choix.
  - `displayText` : facultatif. Texte décrivant la ressource utile ou le plan d'amélioration. La longueur maximale du texte est de 2 048 caractères. Doit être inclus si `url` est spécifié.
  - `url` : facultatif. Une ressource URL pour la ressource utile ou le plan d'amélioration. L'URL doit commencer par `http://` ou `https://`.

> **Note**
>
> Lorsque vous synchronisez une charge de travail de cadre personnalisé avec Jira, les choix affichent l'élément « id » de la question et du choix, ainsi que l'élément « title » du choix. Le format utilisé est `[ QuestionID | ChoiceID ] ChoiceTitle`.

```
"choices": [
     {
         "id": "choice_1",
         "title": "Option 1",
         "helpfulResource": {
             "displayText": "This is helpful text for the first choice",
             "url": "https://example.com/popt01_help.html"
         },
         "improvementPlan": {
```

```
                "displayText": "This is text that will be shown for improvement of
this choice.",
                "url": "https://example.com/popt01_iplan.html"
            }
        },
        {
            "id": "choice_2",
            "title": "Option 2",
            "helpfulResource": {
                "displayText": "This is helpful text for the second choice",
                "url": "https://example.com/hr_manual_CORP_1.pdf"
            },
            "improvementPlan": {
                "displayText": "This is text that will be shown for improvement of
this choice.",
                "url": "https://example.com/popt02_iplan_01.html"
            },
            "additionalResources":[
               {
                 "type": "HELPFUL_RESOURCE",
                 "content": [
                   {
                     "displayText": "This is the second set of helpful text for this
choice.",
                     "url": "https://example.com/hr_manual_country.html"
                   },
                   {
                     "displayText": "This is the third set of helpful text for this
choice.",
                     "url": "https://example.com/hr_manual_city.html"
                   }
                 ]
               },
               {
                 "type": "IMPROVEMENT_PLAN",
                 "content": [
                   {
                     "displayText": "This is additional text that will be shown for
improvement of this choice.",
                     "url": "https://example.com/popt02_iplan_02.html"
                   },
                   {
                     "displayText": "This is the third piece of improvement plan
text.",
```

```
                    "url": "https://example.com/popt02_iplan_03.html"
                  }
                  {
                    "displayText": "This is the fourth piece of improvement plan
text.",
                    "url": "https://example.com/popt02_iplan_04.html"
                  }
                ]
              }
            ]
        },
        {
             "id": "option_no",
             "title": "None of these",
             "helpfulResource": {
               "displayText": "Choose this if your workload does not follow these best
practices.",
               "url": "https://example.com/popt02_iplan_none.html"
             }

           }
```

Section des règles de risque

Cette section définit comment les choix sélectionnés déterminent le niveau de risque.

Vous pouvez définir un maximum de trois règles de risque par question, une pour chaque niveau de risque.

- `condition` : expression booléenne des choix correspondant au niveau de risque de la question, ou `default`.

  Il doit exister une règle de risque `default` pour chaque question.
- `risk` : indique le risque associé à la condition. Les valeurs valides sont `HIGH_RISK`, `MEDIUM_RISK` et `NO_RISK`.

L'ordre de vos règles de risque est important. La première `condition` qui a pour valeur `true` définit le risque associé à la question. Un modèle courant de mise en œuvre des règles de risque consiste à commencer par les règles les moins risquées (et généralement les plus précises) et à poursuivre jusqu'aux règles les plus risquées (et les moins spécifiques).

Par exemple :

```
"riskRules": [
      {
        "condition": "choice_1 && choice_2 && choice_3",
        "risk": "NO_RISK"
      },
      {
        "condition": "((choice_1 || choice_2) && choice_3) || (!choice_1 &&
choice_3)",
        "risk": "MEDIUM_RISK"
      },
      {
        "condition": "default",
        "risk": "HIGH_RISK"
      }
]
```

Si la question comporte trois choix (`choice_1`, `choice_2` et `choice_3`), ces règles de risque entraînent le comportement suivant :

- Si les trois choix sont sélectionnés, il n'y a aucun risque.
- Si `choice_1` ou `choice_2` est sélectionné et si `choice_3` est sélectionné, le risque est moyen.
- Si `choice_1` n'est pas sélectionné mais que `choice_3` est sélectionné, le risque est moyen également.
- Si aucune de ces conditions préalables n'est vraie, le risque est élevé.

Mises à niveau des cadres dans AWS WA Tool

Le cadre AWS Well-Architected et d'autres cadres fournis par AWS sont mis à jour lorsque de nouveaux services sont introduits, que les bonnes pratiques existantes pour les systèmes basés sur le cloud sont affinées, et que de nouvelles bonnes pratiques sont ajoutées. Quand la nouvelle version d'un cadre est disponible, AWS WA Tool est mis à jour pour refléter le dernier ensemble de bonnes pratiques. Toute nouvelle charge de travail définie utilise la nouvelle version du cadre.

Une mise à niveau du cadre se produit également lors de la publication d'une nouvelle version majeure d'un cadre personnalisé que vous avez appliqué à une charge de travail ou à un modèle de révision.

La mise à niveau d'un cadre peut consister en une combinaison quelconque des éléments suivants :

- Ajout de nouvelles questions ou bonnes pratiques
- Suppression d'anciennes questions ou pratiques qui ne sont plus recommandées
- Mise à jour des questions existantes ou des bonnes pratiques
- Ajout ou suppression de piliers

Vos réponses aux questions existantes sont conservées.

> **Note**
>
> Vous ne pouvez pas annuler une mise à niveau du cadre. Une fois qu'une charge de travail a été mise à niveau vers la dernière version du cadre, vous ne pouvez pas revenir à la version précédente du cadre.

Détermination du cadre à mettre à niveau dans AWS WA Tool

Vous pouvez trouver les charges de travail qui n'utilisent pas la version la plus récente du cadre en consultant la page Notifications.

Les informations suivantes sont affichées sur la page Notifications pour chaque charge de travail :

Ressource

Nom de la charge de travail ou du modèle de révision.

Type de ressource

Type de ressource. Il peut s'agir de Charge de travail ou de Modèle de révision.

Ressource associée

Nom du cadre.

Type de notification

Type de notification de mise à niveau.

- Not current (Non actuelle) – La charge de travail utilise une version du cadre qui n'est plus à jour. Effectuez une mise à niveau vers la version actuelle du cadre pour de meilleurs conseils.

- Obsolète : la charge de travail utilise une version du cadre qui ne reflète plus les bonnes pratiques. Procédez à la mise à niveau vers la version actuelle du cadre.
- Supprimé : la charge de travail utilise un cadre qui a été supprimé par son propriétaire.

Version utilisée

Version du cadre actuellement utilisée pour la charge de travail.

Version actuelle disponible

Version du cadre disponible pour la mise à niveau, ou Aucune si le cadre a été supprimé.

Pour mettre à niveau le cadre associé à une charge de travail, sélectionnez la charge de travail et choisissez Upgrade lens version (Mettre à niveau la version du cadre).

Mise à niveau d'un cadre dans AWS WA Tool

Les cadres peuvent être mis à niveau pour les charges de travail et les modèles de révision.

> **Note**
>
> Vous ne pouvez pas annuler la mise à niveau d'un cadre. Une fois qu'une charge de travail ou un modèle de révision a été mis à niveau vers la dernière version du cadre, vous ne pouvez pas revenir à la version précédente du cadre.

Mise à niveau d'un cadre pour une charge de travail

1. Sur la page Notifications, sélectionnez une charge de travail à mettre à niveau, puis choisissez Mise à niveau de la version de la lentille. Des informations sur ce qui a changé dans chaque pilier sont affichées.

   > **Note**
   >
   > Vous pouvez également choisir Afficher les mises à niveau disponibles dans l'onglet Vue d'ensemble de la charge de travail.

2. Avant la mise à niveau d'un cadre pour une charge de travail, un jalon est créé afin d'enregistrer l'état de votre charge de travail existante pour référence ultérieure. Entrez un nom unique pour ce jalon dans le champ Nom du jalon.

3. Cochez la case Confirmation à côté de Je comprends et j'accepte ces modifications., puis choisissez Enregistrer.

Une fois le cadre mis à niveau, vous pouvez consulter la version précédente du cadre dans l'onglet Jalons.

Mise à niveau d'un cadre pour un modèle de révision

1. Pour mettre à niveau le cadre pour un modèle de révision, choisissez
2. Sur la page Notifications, sélectionnez un modèle d'évaluation à mettre à niveau, puis choisissez Mise à niveau de la version de la lentille. Des informations sur ce qui a changé dans chaque pilier sont affichées.

   > **Note**
   >
   > Vous pouvez également choisir Afficher les mises à niveau disponibles dans l'onglet Vue d'ensemble du modèle de révision.

3. Cochez la case Confirmation à côté de Je comprends et j'accepte ces modifications., puis choisissez Mettre à jour et modifier le modèle de réponses pour ajuster les réponses aux questions des bonnes pratiques pour votre modèle d'évaluation, ou choisissez Mettre à niveau pour mettre à niveau le cadre sans ajuster les réponses de votre modèle.

Catalogue Lens pour AWS WA Tool

Le catalogue Lens est une collection de cadres AWS officiels créés pour AWS Well-Architected Tool, qui offrent une technologie de pointe et des bonnes pratiques axées sur le secteur. Ces cadres sont disponibles pour tous les utilisateurs et ne nécessitent aucune installation supplémentaire pour être utilisés.

Le tableau suivant décrit tous les cadres AWS officiels actuellement disponibles dans le catalogue Lens.

Nom du cadre	Description
AWS Well-Architected Framework	Appliqué par défaut à toutes les charges de travail. Collection de bonnes pratiques architect

Nom du cadre	Description
	urales pour concevoir et exploiter des systèmes fiables, sécurisés, efficaces, économiques et durables dans le cloud.
Mobilité connectée	Bonnes pratiques pour intégrer la technolog ie dans les systèmes de transport et améliorer l'expérience globale de mobilité.
Génération de conteneur	Fournit les bonnes pratiques relatives au processus de conception et de génération d'un conteneur.
Analytique des données	Contient des informations exploitables recueilli es par AWS à partir d'études de cas réels et vous aide à découvrir les principaux éléments de conception des charges de travail analytiqu es Well-Architected, ainsi que des recommand ations d'amélioration.
DevOps	Décrit une approche structurée que les organisations de toutes tailles peuvent suivre pour développer une culture à grande vitesse axée sur la sécurité, capable de générer une valeur commerciale substantielle en utilisant les technologies modernes et les bonnes pratiques DevOps.
Secteur des services financiers	Bonnes pratiques pour structurer vos charges de travail du secteur des services financiers sur AWS.
IA générative	Bonnes pratiques pour structurer vos charges de travail d'IA générative sur AWS.
Gouvernement	Bonnes pratiques de conception et de fournitur e de services gouvernementaux sur AWS.

Nom du cadre	Description
Secteur de la santé	Bonnes pratiques et conseils sur la manière de concevoir, de déployer et de gérer vos charges de travail dans le secteur de la santé dans le AWS Cloud.
IoT	Bonnes pratiques pour gérer les charges de travail de l'Internet des objets (IoT) dans AWS.
Fusions et acquisitions	Bonnes pratiques en matière d'intégration et de migration des charges de travail vers le cloud lors de fusions et d'acquisitions.
Machine Learning (apprentissage automatique)	Bonnes pratiques pour gérer vos ressources et charges de travail de machine learning dans AWS.
Migration	Bonnes pratiques pour migrer vers le AWS Cloud.
SaaS	Axé sur la conception, le déploiement et la structuration de vos charges de travail de logiciel en tant que service (SaaS) dans le AWS Cloud.
SAP	Principes et bonnes pratiques de conception pour les charges de travail SAP dans le AWS Cloud.
Applications sans serveur	Bonnes pratiques pour créer des charges de travail sans serveur sur AWS. Couvre des scénarios tels que les microservices RESTful, les backends d'application mobile, le traitement des flux et les applications Web.

Modèles de révision dans AWS WA Tool

Vous pouvez créer des modèles d'avis AWS WA Tool contenant des réponses préremplies à Well-Architected Framework et des questions sur les meilleures pratiques relatives à l'objectif personnalisé. Les modèles de révision Well-Architected réduisent la nécessité de saisir manuellement les mêmes réponses aux meilleures pratiques communes à plusieurs charges de travail lors de la réalisation d'une révision Well-Architected, et ils contribuent à la cohérence et à la standardisation des meilleures pratiques au sein des équipes et des charges de travail.

Vous pouvez créer un modèle de révision pour répondre aux questions courantes sur les meilleures pratiques ou créer des notes, qui peuvent être partagées avec un autre IAM utilisateur ou un autre compte, ou avec une organisation ou une unité organisationnelle du même Région AWS. Vous pouvez définir une charge de travail à partir d'un modèle de révision, ce qui permet d'appliquer les meilleures pratiques courantes et de réduire la redondance entre vos charges de travail.

Création d'un modèle d'avis dans AWS WA Tool

Pour créer un modèle d'avis

1. Sélectionnez Réviser les modèles dans le volet de navigation de gauche.
2. Sélectionnez Create template (Créer un modèle).
3. Sur la page Spécifier les détails du modèle, saisissez le nom et la description de votre modèle de révision.
4. (Facultatif) Dans les sections Notes et Balises du modèle, ajoutez les notes ou balises du modèle que vous souhaitez associer au modèle de révision. Toutes les notes ajoutées sont appliquées à toutes les charges de travail qui utilisent le modèle de révision, tandis que les balises sont spécifiques au modèle de révision.

   Pour plus d'informations sur les balises, consultezBalisage de vos ressources AWS WA Tool.
5. Choisissez Suivant.
6. Sur la page Appliquer des objectifs, sélectionnez les objectifs que vous souhaitez appliquer au modèle d'évaluation. Le nombre maximum de lentilles pouvant être appliquées est de 20.

   Les objectifs peuvent être sélectionnés dans les objectifs personnalisés, le catalogue d'objectifs ou les deux.

> **Note**
>
> Les objectifs partagés avec vous ne peuvent pas être appliqués au modèle d'évaluation.

7. Sélectionnez Create template (Créer un modèle).

Pour commencer à répondre aux questions relatives au modèle d'évaluation que vous venez de créer

1. Dans l'onglet Aperçu du modèle, dans l'alerte d'information Commencer à répondre aux questions, sélectionnez l'objectif dans le menu déroulant Répondre aux questions.

> **Note**
>
> Vous pouvez également accéder à la section Objectifs, sélectionner l'objectif et choisir Répondre aux questions.

2. Pour chaque objectif que vous avez appliqué à votre modèle d'évaluation, répondez aux questions applicables, choisissez Enregistrer et quittez lorsque vous avez terminé.

Une fois votre modèle de révision créé, vous pouvez définir une nouvelle charge de travail à partir de celui-ci.

L'onglet Aperçu du modèle d'évaluation doit refléter le nombre total de questions auxquelles il a été répondu dans la section Détails du modèle et les questions auxquelles il a été répondu pour chaque objectif dans la section Objectifs.

Modification d'un modèle d'avis dans AWS WA Tool

Pour modifier un modèle d'avis

1. Sélectionnez Réviser les modèles dans le volet de navigation de gauche.
2. Sélectionnez le nom du modèle d'avis que vous souhaitez modifier.
3. Pour mettre à jour le nom, la description ou le modèle de notes du modèle de révision, choisissez Modifier dans la section Détails du modèle de l'onglet Aperçu.
   a. Apportez vos modifications aux notes relatives au nom, à la description ou au modèle.

b. Choisissez Enregistrer le modèle pour mettre à jour le modèle de révision avec vos modifications.

4. Pour mettre à jour les verres appliqués au modèle d'évaluation, dans la section Objectifs de l'onglet Aperçu, choisissez Modifier les verres appliqués.
   a. Cochez ou désélectionnez les cases correspondant aux objectifs que vous souhaitez ajouter ou supprimer.

      Les objectifs peuvent être sélectionnés ou désélectionnés dans les objectifs personnalisés, le catalogue d'objectifs ou les deux.

   b. Choisissez Enregistrer le modèle pour enregistrer vos modifications.
5. Pour mettre à jour les réponses aux questions relatives aux meilleures pratiques concernant l'objectif, dans la section Objectifs de l'onglet Aperçu, sélectionnez le nom de l'objectif.
   a. Dans la section Vue d'ensemble de Lens, choisissez Répondre aux questions.

      > **Note**
      >
      > Vous pouvez éventuellement sélectionner le nom de l'objectif dans le menu déroulant Modèles de révision dans le volet de navigation de gauche pour accéder à la section de présentation de l'objectif.

   b. Cochez ou désélectionnez les cases à cocher situées à côté des réponses aux meilleures pratiques que vous souhaitez modifier.
   c. Choisissez Enregistrer et quitter pour enregistrer vos modifications.

Partage d'un modèle d'avis dans AWS WA Tool

Les modèles d'avis peuvent être partagés avec les utilisateurs ou les comptes, ou ils peuvent être partagés avec l'ensemble d'une organisation ou d'une unité organisationnelle.

Pour partager un modèle d'avis

1. Sélectionnez Réviser les modèles dans le volet de navigation de gauche.
2. Sélectionnez le nom du modèle d'avis que vous souhaitez partager.
3. Choisissez l'onglet Shares.

4. Pour partager avec un utilisateur ou un compte, choisissez Créer, puis sélectionnez Partager avec des IAM utilisateurs ou des comptes. Dans la zone Envoyer des invitations, spécifiez l'utilisateur ou le compteIDs, puis choisissez Créer.
5. Pour partager avec une organisation ou une unité organisationnelle, choisissez Create et sélectionnez Share with Organizations. Pour partager avec l'ensemble de l'organisation, sélectionnez Accorder des autorisations à l'ensemble de l'organisation. Pour partager avec une unité organisationnelle, sélectionnez Accorder des autorisations à des unités organisationnelles individuelles, spécifiez l'unité organisationnelle dans le champ, puis choisissez Créer.

> **Important**
>
> Avant de partager un profil avec une organisation ou une unité organisationnelle (UO), vous devez activer AWS Organizations l'accès.

Définition d'une charge de travail à partir d'un modèle dans AWS WA Tool

Vous pouvez définir une charge de travail à partir d'un modèle de révision que vous avez créé ou d'un modèle de révision qui a été partagé avec vous. Vous ne pouvez pas définir une nouvelle charge de travail à partir d'un modèle de révision qui a été supprimé, et si le modèle de révision contient une version obsolète d'un objectif, vous devez mettre à niveau le modèle de révision avant de pouvoir définir une nouvelle charge de travail à partir de celui-ci. Pour plus d'informations sur la mise à niveau d'un modèle de révision, consultezthe section called “Mise à niveau d'un cadre”.

> **Note**
>
> Pour définir une charge de travail à partir d'un modèle de révision, vous devez disposer des IAM autorisations permettant de créer une charge de travail activées :`wellarchitected:CreateWorkload`,, et des autorisations de modèle de révision suivantes : `wellarchitected:GetReviewTemplate` `wellarchitected:GetReviewTemplateAnswerwellarchitected:ListReviewTemplateAns etwellarchitected:GetReviewTemplateLensReview`. Pour plus d'informations sur IAM les autorisations, consultez le guide de Gestion des identités et des accès AWS l'utilisateur.

Pour définir une charge de travail à partir d'un modèle de révision

1. Sélectionnez Réviser les modèles dans le volet de navigation de gauche.
2. Sélectionnez le nom du modèle de révision à partir duquel vous souhaitez définir une charge de travail.
3. Choisissez Définir la charge de travail à partir du modèle.

   > **Note**
   >
   > Vous pouvez également choisir Définir à partir du modèle de révision dans le menu déroulant Définir la charge de travail de la page Charges de travail.

4. À l'étape Sélectionner un modèle de révision, sélectionnez la fiche du modèle de révision, puis cliquez sur Suivant.
5. À l'étape Spécifier les propriétés, renseignez les champs obligatoires pour les propriétés de la charge de travail, puis choisissez Next. Pour en savoir plus, veuillez consulter the section called "Définition d'une charge de travail".
6. (Facultatif) À l'étape Appliquer le profil, associez un profil à la charge de travail en sélectionnant un profil existant, en recherchant le nom du profil ou en choisissant Créer un profil pour créer un profil. Choisissez Suivant.

   Les profils Well-Architected et les modèles de révision peuvent être utilisés en tandem. Les questions préremplies dans votre modèle d'évaluation restent traitées dans la charge de travail, et les questions sont classées par ordre de priorité en fonction de votre profil.
7. (Facultatif) À l'étape Appliquer des objectifs, vous pouvez choisir d'appliquer des objectifs supplémentaires provenant des objectifs personnalisés ou du catalogue d'objectifs qui n'ont pas encore été appliqués au modèle d'évaluation.
8. Choisissez Define workload (Définir une charge de travail).

Supprimer un modèle d'avis dans AWS WA Tool

Pour supprimer un modèle d'avis

1. Sélectionnez Réviser les modèles dans le volet de navigation de gauche.
2. Dans la section Modèles de révision, choisissez le modèle de révision que vous souhaitez supprimer et dans le menu déroulant Actions, sélectionnez Supprimer.

> **Note**
>
> Vous pouvez également sélectionner le nom du modèle et choisir Supprimer dans l'onglet Aperçu du modèle de révision.

3. Dans la boîte de dialogue Supprimer le modèle de révision, entrez le nom du modèle de révision dans le champ pour confirmer la suppression.
4. Sélectionnez Delete (Supprimer).

Vous ne pouvez pas créer une nouvelle charge de travail à partir d'un modèle de révision qui a été supprimé. Si vous avez partagé un modèle d'avis que vous avez supprimé avec d'autres IAM utilisateurs, comptes ou organisations, ils ne pourront pas créer de charges de travail à partir de celui-ci.

Utilisation de profils dans AWS WA Tool

Vous pouvez créer des profils pour fournir le contexte de votre entreprise et identifier les objectifs que vous souhaitez atteindre lors de la réalisation d'une évaluation Well-Architected. AWS Well-Architected Tool utilise les informations recueillies à partir de votre profil pour vous aider à vous concentrer sur une liste hiérarchisée de questions pertinentes pour votre entreprise lors de l'examen de la charge de travail. L'association d'un profil à votre charge de travail vous permet également de déterminer les risques à traiter en priorité dans le cadre de votre plan d'amélioration.

Vous pouvez créer un profil à partir de la page Profils et l'associer à une nouvelle charge de travail, ou vous pouvez ajouter un profil à une charge de travail existante.

Création d'un profil

Pour créer un profil

1. Dans le panneau de navigation de gauche, sélectionnez Profils.
2. Choisissez Créer un profil.
3. Dans la section Propriétés du profil, fournissez un Nom et une Description pour votre profil.
4. Pour affiner les informations prioritaires pour votre entreprise dans le cadre de l'examen de la charge de travail et du plan d'amélioration, sélectionnez les réponses les plus pertinentes pour votre entreprise dans la section Questions sur le profil.
5. (Facultatif) Dans la section Balises, ajoutez les balises que vous souhaitez associer au profil.

   Pour plus d'informations sur les balises, consultez Balisage de vos ressources AWS WA Tool.
6. Choisissez Enregistrer. Un message de réussite s'affiche lorsque le profil est créé avec succès.

Lorsqu'un profil est créé, l'aperçu du profil s'affiche. L'aperçu présente les données associées au profil, y compris le nom, la description, l'ARN, les dates de création et de mise à jour, ainsi que les réponses aux questions sur le profil. Sur la page d'aperçu du profil, vous pouvez modifier, supprimer et partager votre profil.

Modification d'un profil dans AWS WA Tool

Pour modifier un profil

1. Sélectionnez Profils dans le volet de navigation de gauche ou choisissez Afficher le profil dans la section Profils de la charge de travail.
2. Sélectionnez le nom du profil que vous souhaitez mettre à jour.
3. Choisissez Modifier sur la page Présentation du profil.
4. Apportez les mises à jour nécessaires aux questions sur le profil.
5. Choisissez Enregistrer.

Partage d'un profil dans AWS WA Tool

Les profils peuvent être partagés avec des utilisateurs ou des comptes, ou ils peuvent être partagés avec une organisation tout entière ou une unité organisationnelle.

Pour partager un profil

1. Dans le panneau de navigation de gauche, sélectionnez Profils.
2. Sélectionnez le nom du profil que vous souhaitez partager.
3. Choisissez l'onglet Partages.
4. Pour partager avec un utilisateur ou un compte, choisissez Créer, puis sélectionnez Créer des partages avec des comptes ou des utilisateurs IAM. Dans la zone Envoyer des invitations, spécifiez les identifiants d'utilisateur ou de compte, puis choisissez Créer.
5. Pour partager avec une organisation ou une unité organisationnelle, choisissez Créer, puis Créer des partages avec des organisations. Pour partager avec une organisation tout entière, sélectionnez Accorder des autorisations à l'ensemble de l'organisation. Pour partager avec une unité organisationnelle, sélectionnez Accorder des autorisations à des unités organisationnelles individuelles, spécifiez l'unité organisationnelle dans la zone, puis choisissez Créer.

> **Important**
>
> Avant de partager un profil avec une organisation ou une unité organisationnelle (UO), vous devez activer l'accès à AWS Organizations.

Ajout d'un profil à une charge de travail dans AWS WA Tool

Vous pouvez ajouter un profil à une charge de travail existante, ou lors de la définition d'une charge de travail, pour accélérer le processus d'examen de la charge de travail. AWS WA Tool utilise les informations recueillies à partir de votre profil pour hiérarchiser les questions pertinentes pour votre entreprise dans le cadre de l'examen de la charge de travail.

Pour plus d'informations sur l'ajout d'un profil lors de la définition d'une charge de travail, consultez the section called "Définition d'une charge de travail".

Pour ajouter un profil à une charge de travail existante

1. Sélectionnez Charges de travail dans le volet de navigation gauche, puis sélectionnez le nom de la charge de travail que vous souhaitez associer à un profil.

   > **Note**
   >
   > Un seul profil peut être associé à une charge de travail.

2. Dans la section Profil, choisissez Ajouter un profil.
3. Sélectionnez le profil que vous souhaitez appliquer à la charge de travail dans la liste des profils disponibles, ou choisissez Créer un profil. Pour de plus amples informations, consultez the section called "Création d'un profil ".
4. Choisissez Enregistrer.

L'aperçu de la charge de travail affiche le nombre de questions prioritaires auxquelles il a été répondu et les risques classés par ordre de priorité en fonction des informations du profil associé. Choisissez Continuer l'examen pour répondre aux questions prioritaires de l'examen de la charge de travail. Pour de plus amples informations, consultez the section called "Documentation d'une charge de travail".

La section Profil affiche le nom, la description, l'ARN, la version et la date de dernière mise à jour du profil associé à la charge de travail.

Suppression d'un profil d'une charge de travail dans AWS WA Tool

La suppression d'un profil de la charge de travail rétablit la charge de travail à la version antérieure à laquelle le profil lui était associé, et les questions et les risques liés à l'examen de la charge de travail ne sont plus prioritaires.

Pour supprimer un profil d'une charge de travail

1. Dans la section Profils de la charge de travail, choisissez Supprimer.
2. Pour confirmer la suppression, saisissez le nom du profil dans la zone de saisie de texte.
3. Cliquez sur Supprimer.

Une notification indiquant que le profil a été correctement supprimé de la charge de travail s'affiche. La suppression d'un profil rétablit la charge de travail à la version antérieure à laquelle le profil lui était associé, et les questions et les risques liés à l'examen de la charge de travail ne sont plus prioritaires.

Suppression d'un profil d'AWS WA Tool

Si vous avez créé un profil, vous pouvez le supprimer de la liste des profils disponibles dans AWS WA Tool.

La suppression d'un profil de la page Profils ne supprime pas le profil des charges de travail associées. Vous pouvez continuer à utiliser les profils partagés et associés à une charge de travail avant la suppression, mais aucune nouvelle charge de travail ne peut être associée à un profil supprimé. Des the section called "Notifications de profil" sont envoyées aux propriétaires de la charge de travail à l'aide des profils supprimés.

> **Exclusion de responsabilité**
>
> En partageant vos profils avec d'autres Comptes AWS, vous reconnaissez qu'AWS mettra vos profils à la disposition de ces autres comptes. Ces autres comptes pourront continuer à accéder à vos profils partagés et à les utiliser même si vous supprimez les profils de votre propre Compte AWS ou si vous résiliez votre Compte AWS.

Pour supprimer un profil de votre liste de profils

1. Dans le panneau de navigation de gauche, sélectionnez Profils.
2. Sélectionnez le nom du profil que vous souhaitez supprimer.
3. Sélectionnez Delete (Supprimer).
4. Pour confirmer la suppression, saisissez le nom du profil dans la zone de saisie de texte.
5. Sélectionnez Delete (Supprimer).

Si vous souhaitez conserver un profil dans votre liste Profils, mais le supprimer d'une charge de travail, consultez the section called "Suppression d'un profil d'une charge de travail".

AWS Well-Architected Tool Connecteur pour Jira

Vous pouvez utiliser le AWS Well-Architected Tool Connector for Jira pour associer votre compte Jira AWS Well-Architected Tool et synchroniser les éléments d'amélioration de vos charges de travail avec les projets Jira afin de créer un mécanisme en boucle fermée pour mettre en œuvre les améliorations.

Le connecteur permet une synchronisation automatique et manuelle. Pour plus de détails, consultez la section Configuration du connecteur.

Le connecteur peut être configuré au niveau du compte et au niveau de la charge de travail, avec la possibilité de remplacer les paramètres de votre compte par charge de travail. Au niveau de la charge de travail, vous pouvez également choisir d'exclure complètement une charge de travail de la synchronisation.

Vous pouvez choisir de synchroniser les éléments d'amélioration avec le projet WA Jira par défaut ou de spécifier une clé de projet existante avec laquelle synchroniser. Au niveau de la charge de travail, vous pouvez synchroniser chaque charge de travail avec un projet Jira unique si nécessaire.

> **Note**
>
> Le connecteur prend uniquement en charge les projets Scrum et Kanban dans Jira.

Lorsque les éléments d'amélioration sont synchronisés avec Jira, ils sont organisés de la manière suivante :

- Projet : WA (ou projet existant que vous spécifiez)
- Epic : Charge de travail
- Tâche : Question
- Sous-tâche : Bonnes pratiques
- Étiquette : Pilier

Après avoir configuré la synchronisation des comptes Jira sur la page Paramètres, vous pouvez configurer le connecteur Jira et synchroniser les éléments d'amélioration avec votre compte Jira.

Configuration du connecteur

Pour installer le connecteur

> **Note**
>
> Toutes les étapes suivantes sont effectuées dans votre compte Jira, et non dans votre Compte AWS.

1. Connectez-vous à votre compte Jira.
2. Dans la barre de navigation supérieure, choisissez Applications, puis sélectionnez Découvrir d'autres applications.
3. Sur la page Découvrez les applications et les intégrations pour Jira, saisissez Well-Architected AWS . Choisissez ensuite le AWS Well-Architected Tool connecteur pour Jira.
4. Sur la page de l'application, sélectionnez Télécharger l'application.
5. Dans le volet Ajouter à Jira, choisissez Get it now.
6. Une fois l'application installée, pour terminer la configuration, choisissez Configurer.
7. Sur la page AWS Well-Architected Tool Configuration, choisissez Connect a new Compte AWS.
8. Entrez votre AccessKeyidentifiant et votre clé secrète. Facultatif : entrez votre jeton de session. Choisissez ensuite Connect.

   > **Note**
   >
   > Assurez-vous que votre compte dispose de cette autorisation`wellarchitected:ConfigureIntegration`. Cette autorisation est requise pour ajouter Comptes AWS à Jira.
   > Plusieurs Comptes AWS peuvent être connectés à AWS WA Tool.

   > **Note**
   >
   > Pour des raisons de sécurité, il est vivement recommandé d'utiliser des informations d'identification IAM à court terme. Pour plus de détails sur la création d'un AccessKeyidentifiant et d'une clé secrète pour votre Compte AWS compte, voir Gestion

des clés d'accès (console), et pour plus de détails sur l'utilisation d'informations d'identification à court terme, voir Demande d'informations d'identification temporaires.

9. Pour Régions, sélectionnez celle que Régions AWS vous souhaitez connecter. Choisissez ensuite Connect.

Configuration du projet Jira

Lorsque vous utilisez des projets personnalisés, assurez-vous que la configuration de votre projet comporte les types de problèmes suivants :

- Scrum : Epic, Story, Subtask
- Kanban : Epic, Task, Subtask

Pour en savoir plus sur la gestion des types de problèmes, consultez Atlassian Support | Ajouter, modifier et supprimer un type de problème.

Pour vérifier l'état du connecteur dans AWS Well-Architected Tool

1. Connectez-vous à votre Compte AWS et accédez à AWS Well-Architected Tool.
2. Sélectionnez Paramètres dans le volet de navigation de gauche.
3. Dans la section de synchronisation des comptes Jira, sous État de la connexion à l'application Jira, vérifiez l'état Configuré.

Le connecteur est maintenant configuré et prêt à être configuré. Pour configurer les paramètres de synchronisation Jira au niveau du compte et de la charge de travail, consultez Configuration du connecteur.

Configuration du connecteur

Avec le AWS Well-Architected Tool connecteur pour Jira, vous pouvez configurer la synchronisation Jira au niveau du compte, au niveau de la charge de travail, ou les deux. Vous pouvez configurer les paramètres Jira au niveau de la charge de travail indépendamment des paramètres au niveau du compte, ou remplacer les paramètres de votre compte sur une charge de travail spécifique pour spécifier le comportement de synchronisation de la charge de travail. Vous pouvez également configurer les paramètres Jira lors de la définition d'une charge de travail.

Le connecteur propose deux méthodes de synchronisation : synchronisation automatique et manuelle. Dans les deux méthodes de synchronisation, les modifications apportées AWS WA Tool sont reflétées dans votre projet Jira, et les modifications effectuées dans Jira sont resynchronisées avec. AWS WA Tool

> **Important**
>
> En utilisant la synchronisation automatique, vous acceptez de AWS WA Tool modifier votre charge de travail en réponse aux modifications apportées à Jira.
> Si vous avez des informations sensibles que vous ne souhaitez pas synchroniser avec Jira, ne les saisissez pas dans le champ Notes de vos charges de travail.

- Synchronisation automatique : le connecteur met automatiquement à jour votre projet Jira et votre charge de travail chaque fois qu'une question est mise à jour, notamment en sélectionnant ou désélectionnant une bonne pratique et en répondant à une question.
- Synchronisation manuelle : vous devez choisir Synchroniser avec Jira dans le tableau de bord de la charge de travail lorsque vous souhaitez synchroniser les éléments d'amélioration entre Jira et le. AWS WA Tool Vous pouvez également choisir les piliers et les questions spécifiques que vous souhaitez synchroniser. Pour plus de détails, consultez la section Synchronisation d'une charge de travail.

Pour configurer le connecteur au niveau du compte

1. Sélectionnez Paramètres dans le volet de navigation de gauche.
2. Dans le volet de synchronisation des comptes Jira, choisissez Modifier.
3. Pour le type de synchronisation, sélectionnez l'une des options suivantes :
    a. Pour synchroniser automatiquement les charges de travail lorsque des modifications sont apportées, sélectionnez Automatique.
    b. Pour choisir manuellement quand synchroniser les charges de travail, sélectionnez Manuel.
4. Par défaut, le connecteur crée un projet WA Jira. Pour spécifier votre propre clé de projet Jira, procédez comme suit :
    a. Sélectionnez Remplacer la clé de projet Jira par défaut.
    b. Entrez la clé de votre projet Jira.

> **Note**
>
> La clé de projet Jira spécifiée est utilisée pour toutes les charges de travail, sauf si vous modifiez le projet au niveau de la charge de travail.

5. Choisissez Save settings (Enregistrer les paramètres).

Pour configurer le connecteur au niveau de la charge de travail

1. Sélectionnez Workloads dans le volet de navigation de gauche, puis sélectionnez le nom de la charge de travail que vous souhaitez configurer.
2. Choisissez Propriétés.
3. Dans le volet Jira, choisissez Modifier.
4. Pour configurer les paramètres Jira du workload, sélectionnez Remplacer les paramètres au niveau du compte.

> **Note**
>
> Les paramètres de remplacement au niveau du compte doivent être sélectionnés afin d'appliquer les paramètres spécifiques à la charge de travail.

5. Pour annuler la synchronisation, sélectionnez l'une des options suivantes :

   a. Pour exclure la charge de travail de la synchronisation Jira, sélectionnez Ne pas synchroniser la charge de travail.

   b. Pour choisir manuellement quand synchroniser la charge de travail, sélectionnez Synchroniser la charge de travail - Manuel.

   c. Pour synchroniser automatiquement les modifications de charge de travail, sélectionnez Synchroniser la charge de travail - Automatique.

6. (Facultatif) Pour la clé de projet Jira, entrez la clé de projet avec laquelle synchroniser la charge de travail. Cette clé de projet peut être différente de la clé de projet au niveau de votre compte.

   Si vous ne spécifiez pas de clé de projet, le connecteur crée un projet WA Jira.

7. Choisissez Enregistrer.

Pour plus de détails sur l'exécution d'une synchronisation manuelle, voir Synchronisation d'une charge de travail.

Synchronisation d'une charge de travail

Pour la synchronisation automatique, le connecteur synchronise automatiquement les éléments d'amélioration lorsque vous mettez à jour une charge de travail (par exemple, lorsque vous répondez à une question ou que vous sélectionnez une nouvelle meilleure pratique).

Dans le cadre de la synchronisation manuelle et automatique, toutes les modifications apportées dans Jira (comme répondre à une question ou aux meilleures pratiques) sont resynchronisées avec. AWS Well-Architected Tool

Pour synchroniser manuellement une charge de travail

1. Lorsque vous êtes prêt à synchroniser votre charge de travail avec Jira, sélectionnez Charges de travail dans le volet de navigation de gauche. Sélectionnez ensuite la charge de travail que vous souhaitez synchroniser.
2. Dans l'aperçu de la charge de travail, choisissez Synchroniser avec Jira.
3. Sélectionnez l'objectif que vous souhaitez synchroniser.
4. Pour synchroniser les questions avec Jira, sélectionnez les questions ou les piliers complets que vous souhaitez synchroniser avec le projet Jira.
    - Pour toutes les questions que vous souhaitez supprimer, sélectionnez l'icône X à côté du titre de la question.
5. Choisissez Sync.

Désinstallation du connecteur

Pour désinstaller complètement le AWS Well-Architected Tool connecteur pour Jira, effectuez les tâches suivantes :

- Désactivez la synchronisation Jira dans toutes les charges de travail qui remplacent les paramètres de synchronisation au niveau du compte
- Désactiver la synchronisation Jira au niveau du compte
- Dissociez votre compte Compte AWS dans Jira

- Désinstallez le connecteur de votre compte Jira

Pour désactiver le connecteur au niveau du compte

> **Note**
>
> Les étapes suivantes sont effectuées dans votre Compte AWS.

1. Sélectionnez Paramètres dans le volet de navigation de gauche.
2. Dans la section de synchronisation des comptes Jira, choisissez Modifier.
3. Désactivez l'option Activer la synchronisation des comptes Jira.
4. Choisissez Save settings (Enregistrer les paramètres).

Pour dissocier un Compte AWS

> **Note**
>
> Toutes les étapes suivantes sont effectuées dans votre compte Jira, et non dans votre Compte AWS.

1. Connectez-vous à votre compte Jira.
2. Dans la barre de navigation supérieure, choisissez Applications, puis sélectionnez Gérer vos applications.
3. Cliquez sur la flèche déroulante à côté de AWS Well-Architected Tool Connector for Jira, puis sélectionnez Configurer.
4. Dans le volet AWS Well-Architected Tool Configuration, pour dissocier un Compte AWS, choisissez X sous Actions.

Pour désinstaller le connecteur

> **Note**
>
> Toutes les étapes suivantes sont effectuées dans votre compte Jira, et non dans votre Compte AWS.

Nous vous recommandons de vérifier que toutes les connexions Comptes AWS sont déconnectées dans la configuration du connecteur avant de le désinstaller.

1. Connectez-vous à votre compte Jira.
2. Dans la barre de navigation supérieure, choisissez Applications, puis sélectionnez Gérer vos applications.
3. Cliquez sur la flèche déroulante située à côté de AWS Well-Architected Tool Connector for Jira.
4. Choisissez Désinstaller, puis sélectionnez Désinstaller l'application.

Jalons

Un jalon important enregistre l'état d'une charge de travail à un moment donné.

Enregistrez un jalon important après avoir terminé toutes les questions associées à une charge de travail. Au fur et à mesure que vous modifiez votre charge de travail en fonction des éléments dans votre plan d'amélioration, vous pouvez enregistrer des jalons supplémentaires pour mesurer les progrès.

Une bonne pratique consiste à enregistrer un jalon important chaque fois que vous apportez des améliorations à une charge de travail.

Enregistrement d'un jalon

Un jalon enregistre l'état actuel d'une charge de travail. Le propriétaire d'une charge de travail peut enregistrer un jalon à tout moment.

Pour enregistrer un jalon

1. A partir de la page des détails de la charge de travail, choisissez Save milestone (Enregistrer un jalon).
2. Dans la case Milestone name (Nom d'un jalon), saisissez un nom pour votre jalon.

   > **Note**
   >
   > Le nom doit avoir entre 3 et 100 caractères. Au moins trois caractères ne doivent pas être des espaces. Les noms de jalons associés à une charge de travail doivent être uniques. Les espaces et les majuscules sont ignorés lors du contrôle de l'unicité.

3. Choisissez Enregistrer pour enregistrer le jalon.

Une fois un jalon enregistré, vous ne pouvez pas modifier les données de la charge de travail qui ont été enregistrées. Lorsque vous supprimez une charge de travail, les jalons qui y sont associés sont également supprimés.

Affichage des jalons

Vous pouvez afficher les jalons d'une charge de travail de plusieurs façons :

- Sur la page des détails de la charge de travail, choisissez Milestones (Jalons) et choisissez le jalon que vous souhaitez afficher.
- Sur la page Dashboard (Tableau de bord), choisissez la charge de travail et dans la section Milestones (Jalons), choisissez le jalon que vous souhaitez afficher.

Génération d'un rapport de jalon

Vous pouvez générer un rapport de jalon. Le rapport contient les réponses aux questions relatives à la charge de travail, vos notes et tous les risques élevés et moyens qui étaient présents lorsque le jalon a été enregistré.

Un rapport vous permet de partager des détails sur le jalon avec d'autres utilisateurs qui n'ont pas accès à l'AWS Well-Architected Tool.

Pour générer un rapport de jalon

1. Sélectionnez le jalon de l'une des manières suivantes.
   - Depuis la page des détails de la charge de travail, choisissez Milestones (Jalons) et choisissez le jalon.
   - Sur la page Dashboard (Tableau de bord), choisissez la charge de travail avec le jalon concerné. Dans la section Milestones (Jalons), choisissez le jalon.
2. Choisissez Generate report (Générer un rapport) pour générer un rapport.

   Le fichier PDF est généré et vous pouvez le télécharger ou l'afficher.

Partagez des invitations

Une invitation de partage est une demande de partage d'une charge de travail, d'un objectif personnalisé ou d'un modèle d'avis appartenant à un autre AWS compte. Une charge de travail ou un objectif peuvent être partagés avec tous les utilisateurs d'unCompte AWS, avec des utilisateurs individuels ou avec les deux.

- Si vous acceptez une invitation de charge de travail, la charge de travail est ajoutée à vos pages de charge de travail et de tableau de bord.
- Si vous acceptez une invitation pour un objectif personnalisé, l'objectif est ajouté à votre page d'objectifs personnalisés.
- Si vous acceptez une invitation de profil, le profil est ajouté à votre page Profils.
- Si vous acceptez une invitation de modèle d'évaluation, le modèle est ajouté à votre page de modèles de révision.

Si vous refusez l'invitation, elle est supprimée de la liste.

> **Note**
>
> Les charges de travail, les objectifs personnalisés, les profils et les modèles d'avis ne peuvent être partagés qu'au sein d'un même Région AWS outil.

Le propriétaire de la charge de travail ou de l'objectif personnalisé contrôle qui dispose d'un accès partagé.

La page Partager les invitations, disponible dans le menu de navigation de gauche, fournit des informations sur votre charge de travail en attente et sur les invitations Lens personnalisées.

Les informations suivantes sont affichées pour chaque charge de travail :

Nom

Le nom de la charge de travail, de l'objectif personnalisé ou du modèle de révision à partager.

Type de ressource

Type d'invitation, qu'il s'agisse de la charge de travail, de l'objectif personnalisé, des profils ou du modèle de révision.

Propriétaire

Compte AWSID propriétaire de la charge de travail.

Autorisation

Autorisation qui vous est accordée pour la charge de travail.

- Read-Only

  Fournit un accès en lecture seule à la charge de travail, à l'objectif personnalisé, aux profils ou au modèle de révision.

- Participant

  Fournit un accès mis à jour aux réponses et à leurs notes, et un accès en lecture seule au reste de la charge de travail. Cette autorisation n'est disponible que pour les charges de travail.

Détails de l’autorisation

Description détaillée de l'autorisation.

Accepter une invitation à partager

Pour accepter une invitation de partage

1. Sélectionnez l'invitation de partage à accepter.
2. Choisissez Accepter.

Pour les invitations à une charge de travail, la charge de travail est ajoutée aux pages Charges de travail et Tableau de bord. Pour les invitations personnalisées, l'objectif personnalisé est ajouté à la page des objectifs personnalisés. Pour les invitations de profil, le profil est ajouté à la page Profils. Pour les modèles d'invitations à réviser, le modèle est ajouté à la page des modèles de révision.

Vous avez sept jours pour accepter une invitation. Si vous n'acceptez pas l'invitation dans les sept jours, elle expire automatiquement.

Si un utilisateur et ses Compte AWS deux ont accepté des invitations à une charge de travail, l'invitation à une charge de travail destinée à l'utilisateur détermine l'autorisation de l'utilisateur.

Rejet d'une invitation à partager

Pour rejeter une invitation à partager

1. Sélectionnez la charge de travail ou l'invitation personnalisée à rejeter.
2. Choisissez Reject (Refuser).

L'invitation est supprimée de la liste.

Notifications

La page Notifications affiche les différences de version pour les charges de travail et les modèles de révision associés à des objectifs et à des profils. Vous pouvez passer à la version la plus récente d'un objectif ou d'un profil pour une charge de travail à partir de la page Notifications.

Notifications relatives à

Lorsqu'une nouvelle version d'un objectif est disponible, une bannière apparaît en haut de la page des charges de travail ou des modèles de révision pour vous en informer. Si vous consultez une charge de travail ou un modèle de révision spécifique à l'aide d'un objectif obsolète, vous verrez également une bannière indiquant qu'une nouvelle version de l'objectif est disponible.

Choisissez Afficher les mises à niveau disponibles pour obtenir une liste des charges de travail ou des modèles de révision pouvant être mis à niveau.

Consultez the section called "Mise à niveau d'un cadre" les instructions relatives à la mise à niveau d'un objectif pour une charge de travail ou un modèle de révision.

Lorsque le propriétaire d'un objectif partagé le supprime, si une charge de travail est associée à l'objectif supprimé, vous recevez une notification indiquant que vous pouvez toujours utiliser l'objectif dans votre charge de travail existante, mais que vous ne pouvez pas l'ajouter à de nouvelles charges de travail.

Notifications de profil

Il existe deux types de notifications de profil :

- Mise à niveau du profil
- Suppression du profil

Lorsqu'un profil associé à une charge de travail a été modifié (pour plus d'informations, voirthe section called "Modification d'un profil"), une notification indiquant qu'il existe une nouvelle version du profil est affichée dans les notifications du profil.

Lorsque le propriétaire d'un profil partagé le supprime, si une charge de travail est associée au profil supprimé, vous recevez une notification indiquant que vous pouvez toujours utiliser le profil dans

votre charge de travail existante, mais que vous ne pouvez pas l'ajouter à de nouvelles charges de travail.

Pour mettre à niveau une version de profil

1. Dans le volet de navigation de gauche, sélectionnez Notifications.
2. Sélectionnez le nom de la charge de travail dans la liste de l'onglet Notifications de profil ou utilisez la barre de recherche pour effectuer une recherche par nom de charge de travail.
3. Choisissez la version du profil de mise à niveau.
4. Dans la section Confirmation, cochez la case de confirmation pour « J'ai compris et j'accepte ces modifications ».
5. (Facultatif) Si vous choisissez d'enregistrer un jalon, cochez la case Enregistrer un jalon et saisissez le nom du jalon.
6. Sélectionnez Save.

Une fois le profil mis à niveau, le dernier numéro de version et la date de mise à jour sont affichés dans la section Profil de la charge de travail.

Pour plus d'informations, consultez Profils.

Tableau de bord

Le tableau de bord, disponible dans le menu de navigation de gauche, vous donne accès à vos charges de travail et aux problèmes à risque moyen et élevé associés. Vous pouvez également inclure les charges de travail qui ont été partagées avec vous. Le tableau de bord comprend quatre sections.

- Résumé : indique le nombre total de charges de travail, celles présentant des risques élevés et moyens et le nombre total de problèmes présentant un risque élevé et moyen pour toutes les charges de travail.
- Problèmes liés à un framework Well-Architected par pilier : affiche une représentation graphique des problèmes à risque élevé et moyen par pilier pour toutes vos charges de travail.
- Problèmes de structure Well-Architected par charge de travail : affiche les problèmes à risque élevé et moyen par pilier pour chacune de vos charges de travail.
- Problèmes liés à une structure Well-Architected par élément du plan d'amélioration : affiche les éléments du plan d'amélioration pour toutes vos charges de travail.

Récapitulatif

Cette section indique le nombre total de charges de travail et le nombre de charges de travail présentant des problèmes à risque élevé et moyen selon l'objectif Well-Architected Framework et tous les autres objectifs. Le nombre total de problèmes à risque élevé et moyen pour toutes les charges de travail, qu'ils vous appartiennent ou que vous partagiez avec vousCompte AWS, est indiqué.

Choisissez Inclure les charges de travail partagées avec moi pour que les statistiques récapitulatives, le rapport consolidé et les autres sections du tableau de bord reflètent à la fois vos charges de travail et celles qui ont été partagées avec vous.

Choisissez Générer un rapport pour qu'un rapport consolidé soit créé pour vous sous la forme d'un fichier PDF.

Le nom du rapport se présente sous la forme :`wellarchitected_consolidatedreport_`*`account-ID`*`.pdf`.

Problèmes liés à Well-Architected Framework par pilier

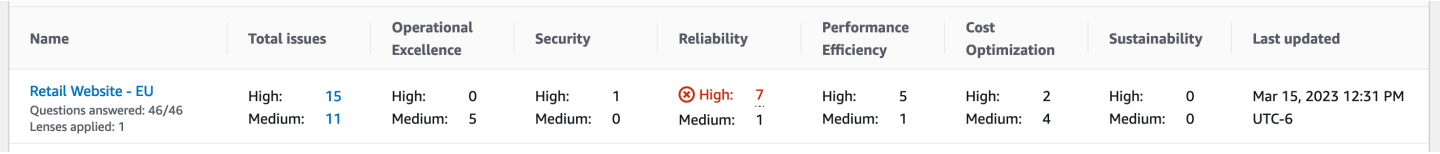
La section des problèmes du Well-Architected Framework par pilier présente une représentation graphique du nombre de problèmes à risque élevé et moyen par pilier pour toutes les charges de travail.

Utilisez les sections restantes du tableau de bord pour passer d'un niveau de détail à l'autre.

> **Note**
>
> Seuls les problèmes liés au Well-Architected Framework sont inclus dans cette section.

Problèmes de framework Well-Architected par charge de travail

La section Problèmes du framework Well-Architected par charge de travail affiche des informations pour chaque charge de travail.



Name	Total issues	Operational Excellence	Security	Reliability	Performance Efficiency	Cost Optimization	Sustainability	Last updated
Retail Website - EU Questions answered: 46/46 Lenses applied: 1	High: 15 Medium: 11	High: 0 Medium: 5	High: 1 Medium: 0	High: 7 Medium: 1	High: 5 Medium: 1	High: 2 Medium: 4	High: 0 Medium: 0	Mar 15, 2023 12:31 PM UTC-6

Les informations suivantes sont affichées pour chaque charge de travail :

Nom

Le nom de la charge de travail. Le nombre de questions auxquelles on a répondu et le nombre de lentilles appliquées à la charge de travail sont également indiqués.

Choisissez le nom de la charge de travail pour accéder à la page détaillée de la charge de travail et consulter les jalons, les plans d'amélioration et les partages.

Nombre total de problèmes

Nombre total de problèmes identifiés par l'optique du Well-Architected Framework en ce qui concerne la charge de travail.

Choisissez le nombre de problèmes présentant un risque élevé ou moyen pour consulter les plans d'amélioration recommandés pour ces problèmes.

Excellence opérationnelle

Nombre de problèmes à haut risque (HRI) et de problèmes à risque moyen (IRM) identifiés dans la charge de travail pour le pilier Excellence opérationnelle.

Sécurité

Nombre d'IRH et d'IRM identifiés pour le pilier Sécurité.

Fiabilité

Nombre d'IRH et d'IRM identifiés pour le pilier Fiabilité.

Efficacité des performances

Nombre d'IRH et d'IRM identifiés pour le pilier Efficacité des performances.

Optimisation des coûts

Nombre d'IRH et d'IRM identifiés pour le pilier Optimisation des coûts.

Durabilité

Le nombre d'IRH et d'IRM identifiés pour le pilier Durabilité.

Date de la dernière mise à jour

Date et heure de la dernière mise à jour de la charge de travail.

Pour chaque charge de travail, le pilier présentant le plus grand nombre de problèmes à haut risque (HRI) est mis en évidence.

> **Note**
>
> Seuls les problèmes liés au Well-Architected Framework sont inclus dans cette section.

Problèmes liés au framework Well-Architected par élément du plan d'amélioration

La section Problèmes du framework Well-Architected par élément du plan d'amélioration affiche les éléments du plan d'amélioration pour toutes vos charges de travail. Vous pouvez filtrer les éléments en fonction du pilier et de la gravité.

Les informations suivantes sont affichées pour chaque élément du plan d'amélioration :

Élément d'amélioration

Nom de l'élément du plan d'amélioration.

Choisissez le nom pour afficher la meilleure pratique associée à l'élément du plan d'amélioration.

Pilier

Le pilier associé à l'élément d'amélioration.

Risque

Indique si le problème associé présente un risque élevé ou moyen.

Charges de travail applicables

Nombre de charges de travail auxquelles ce plan d'amélioration s'applique.

Sélectionnez un élément du plan d'amélioration pour voir les charges de travail applicables.

> **Note**
>
> Seuls les éléments du plan d'amélioration sous l'angle du Well-Architected Framework sont inclus dans cette section.

Sécurité dans AWS Well-Architected Tool

Chez AWS, la sécurité dans le cloud est la priorité numéro 1. En tant que client AWS, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité.

La sécurité est une responsabilité partagée entre AWS et vous-même. Le modèle de responsabilité partagée décrit ceci comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est responsable de la protection de l'infrastructure qui exécute des services AWS dans le cloud AWS Cloud. AWS vous fournit également les services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de conformité AWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Well-Architected Tool, consultez Services AWS concernés par le programme de conformité.
- Sécurité dans le cloud : votre responsabilité est déterminée par le service AWS que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de AWS WA Tool. Les rubriques suivantes expliquent comment configurer AWS WA Tool pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres services AWS pour surveiller et sécuriser vos ressources AWS WA Tool.

Rubriques

Protection des données dans AWS Well-Architected Tool

Le modèle de responsabilité partagée AWS s'applique à la protection des données dans l'AWS Well-Architected Tool. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure globale sur laquelle l'ensemble du AWS Cloud s'exécute. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée d'AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécurité AWS.

À des fins de protection des données, nous vous recommandons de protéger les informations d'identification Compte AWS et de configurer les comptes utilisateur individuels avec AWS IAM Identity Center ou Gestion des identités et des accès AWS (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez les certificats SSL/TLS pour communiquer avec les ressources AWS. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez une API (Interface de programmation) et la journalisation des activités des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des sentiers CloudTrail pour capturer des activités AWS, consultez la section Utilisation des sentiers CloudTrail dans le Guide de l'utilisateur AWS CloudTrail.
- Utilisez des solutions de chiffrement AWS, ainsi que tous les contrôles de sécurité par défaut au sein des Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules de chiffrement validés FIPS (Federal Information Processing Standard) 140-3 lorsque vous accédez à AWS via une interface de ligne de commande ou une API (interface de programmation), utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela est également valable lorsque vous utilisez AWS WA Tool ou d'autres Services AWS à l'aide de la console, de l'API, d'AWS CLI ou des kits SDK AWS. Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Chiffrement au repos

Toutes les données stockées par AWS WA Tool sont chiffrées au repos.

Chiffrement en transit

Toutes les données envoyées vers et depuis AWS WA Tool sont chiffrées en transit.

Comment AWS utilise vos données

L'équipe AWS Well-Architected recueille des données agrégées à partir de l'AWS Well-Architected Tool afin de fournir et d'améliorer le service AWS WA Tool aux clients. Les données individuelles des clients peuvent être partagées avec les équipes de Compte AWS afin de soutenir les efforts de nos clients pour améliorer leurs charges de travail et leur architecture. L'équipe AWS Well-Architected peut accéder uniquement aux propriétés de charge de travail et aux choix sélectionnés pour chaque question. AWS ne partage aucune donnée provenant d'AWS WA Tool à l'extérieur d'AWS.

Les propriétés de charge de travail auxquelles l'équipe AWS Well-Architected a accès sont les suivantes :

- Nom de la charge de travail
- Propriétaire de la vérification
- Environnement
- Régions
- ID de compte
- Type d'activité

L'équipe AWS Well-Architected n'a pas accès aux éléments suivants :

- Description de la charge de travail
- Conception de l'architecture
- Toutes les notes que vous avez saisies

Gestion des identités et des accès pour AWS Well-Architected Tool

Gestion des identités et des accès AWS (IAM) est un Service AWS qui aide un administrateur à contrôler en toute sécurité l'accès aux ressources AWS. Des administrateurs IAM contrôlent les personnes qui s'authentifient (sont connectées) et sont autorisées (disposent d'autorisations) à utiliser des ressources AWS WA Tool. IAM est un Service AWS que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction de votre rôle :

- Utilisateur du service : demandez des autorisations à votre administrateur si vous ne pouvez pas accéder aux fonctionnalités (voir Résolution des problèmes d'identité et d'accès avec AWS Well-Architected Tool)
- Administrateur du service : déterminez l'accès des utilisateurs et soumettez les demandes d'autorisation (voir Fonctionnement de AWS Well-Architected Tool avec IAM)
- Administrateur IAM : rédigez des politiques pour gérer l'accès (voir AWS Well-Architected ToolExemples de politiques basées sur l'identité)

Authentification par des identités

L'authentification correspond au processus par lequel vous vous connectez à AWS avec vos informations d'identification. Vous devez vous authentifier en tant qu'Utilisateur racine d'un compte AWS, en tant qu'utilisateur IAM ou en endossant un rôle IAM.

Vous pouvez vous connecter en tant qu'identité fédérée en utilisant les informations d'identification provenant d'une source d'identité telle que AWS IAM Identity Center (IAM Identity Center), l'authentification unique ou les informations d'identification Google/Facebook. Pour plus d'informations sur la connexion, consultez Connexion à votre Compte AWS dans le Guide de l'utilisateur Connexion à AWS.

Pour l'accès par programmation, AWS fournit un kit SDK et une CLI pour signer les demandes de manière cryptographique. Pour plus d'informations, consultez Signature AWS Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Utilisateur racine Compte AWS

Lorsque vous créez un Compte AWS, vous commencez avec une seule identité de connexion nommée utilisateur racine du Compte AWS, qui bénéficie d'un accès complet à tous les Services AWS et toutes les ressources du compte. Il est vivement déconseillé d'utiliser l'utilisateur racine pour vos tâches quotidiennes. Pour les tâches qui requièrent des informations d'identification de l'utilisateur racine, consultez Tâches qui requièrent les informations d'identification de l'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

Nous vous recommandons vivement d'exiger de vos utilisateurs humains qu'ils utilisent une fédération liée à un fournisseur d'identité pour accéder à Services AWS avec des informations d'identification temporaires.

Une identité fédérée est un utilisateur provenant de l'annuaire de votre entreprise, de votre fournisseur d'identité Web ou Directory Service qui y accède à Services AWS l'aide d'informations d'identification provenant d'une source d'identité. Les identités fédérées assument des rôles qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Pour plus d'informations, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center.

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité qui dispose d'autorisations spécifiques pour une seule personne ou application. Nous vous recommandons d'utiliser ces informations d'identification temporaires au lieu des utilisateurs IAM avec des informations d'identification à long terme. Pour plus d'informations, consultez Exiger des utilisateurs humains qu'ils utilisent une fédération avec un fournisseur d'identité pour accéder à AWS en utilisant des informations d'identification temporaires dans le Guide de l'utilisateur IAM.

Les groupes IAM spécifient une collection d'utilisateurs IAM et permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Pour plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité dotée d'autorisations spécifiques qui fournit des informations d'identification temporaires. Pour endosser un rôle, passez d'un utilisateur à un rôle IAM (console) ou appelez une AWS CLI ou une opération d'API AWS. Pour plus d'informations, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM sont utiles pour l'accès des utilisateurs fédérés, les autorisations temporaires des utilisateurs IAM, les accès intercompte, les accès entre services et les applications exécutées sur Amazon EC2. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez les accès dans AWS en créant des politiques et en les attachant à des identités AWS ou à des ressources. Une politique définit les autorisations lorsqu'elles sont associées à une identité ou une ressource. AWS évalue ces politiques lorsqu'un principal effectue une demande. La plupart des politiques sont stockées dans AWS en tant que documents JSON. Pour plus d'informations les documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

À l'aide de politiques, les administrateurs précisent qui a accès à quoi en définissant quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Un administrateur IAM crée des politiques IAM et les ajoute aux rôles, que les utilisateurs peuvent ensuite assumer. Les

politiques IAM définissent les autorisations quelle que soit la méthode que vous utilisez pour exécuter l'opération.

Politiques basées sur l'identité

Les stratégies basées sur l'identité sont des documents de stratégie d'autorisations JSON que vous attachez à une identité (utilisateur, groupe ou rôle). Ces politiques contrôlent les actions que peuvent exécuter ces identités, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être des politiques intégrées (intégrées directement dans une seule identité) ou des politiques gérées (politiques autonomes associées à plusieurs identités). Pour découvrir comment choisir entre des politiques gérées et en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Les exemples incluent les politiques de confiance de rôle IAM et les stratégies de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Vous devez spécifier un principal dans une politique basée sur les ressources.

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques gérées AWS depuis IAM dans une politique basée sur une ressource.

Autres types de politique

AWS prend en charge des types de politiques supplémentaires qui peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants :

- Limites d'autorisations : une limite des autorisations définit le nombre maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM. Pour plus d'informations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) : spécifient les autorisations maximales pour une organisation ou une unité organisationnelle dans AWS Organizations. Pour plus d'informations, consultez Politiques de contrôle de service dans le Guide de l'utilisateur AWS Organizations.

- Politiques de contrôle des ressources (RCP) : définissent les autorisations maximales disponibles pour les ressources de votre organisation. Pour plus d'informations, consultez Politiques de contrôle des ressources (RCP) dans le Guide de l'utilisateur AWS Organizations.
- Politiques de session : politiques avancées que vous passez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Pour plus d'informations, consultez Politiques de session dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour découvrir la façon dont AWS détermine s'il convient d'autoriser une demande en présence de plusieurs types de politiques, consultez Logique d'évaluation de politiques dans le Guide de l'utilisateur IAM.

Fonctionnement de AWS Well-Architected Tool avec IAM

Avant d'utiliser IAM pour gérer l'accès à AWS WA Tool, découvrez les fonctions IAM que vous pouvez utiliser avec AWS WA Tool.

Fonctions IAM que vous pouvez utiliser avec AWS Well-Architected Tool

Fonctionnalité IAM	AWS WA ToolPrise en charge de l'
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui
ACL	Non
ABAC (étiquettes dans les politiques)	Oui
Informations d'identification temporaires	Oui

Fonctionnalité IAM	AWS WA ToolPrise en charge de l'
Autorisations de principal	Oui
Rôles du service	Non
Rôles liés à un service	Non

Pour obtenir une vue d'ensemble de la façon dont AWS WA Tool et d'autres services AWS fonctionnent avec la plupart des fonctionnalités d'IAM, consultez Services AWS qui fonctionnent avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité AWS WA Tool

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser les politiques JSON AWS pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Politiques basées sur les ressources dans AWS WA Tool

Prend en charge les politiques basées sur les ressources : non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou des Services AWS.

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. Pour plus

d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Actions de politique pour AWS WA Tool

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser les politiques JSON AWS pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Les actions de politique dans AWS WA Tool utilisent le préfixe suivant avant l'action : `wellarchitected:`. Par exemple, pour autoriser une entité à définir une charge de travail, un administrateur doit attacher une stratégie qui autorise les actions `wellarchitected:CreateWorkload`. De même, pour éviter qu'une entité supprime des charges de travail, un administrateur peut attacher une stratégie qui refuse les actions `wellarchitected:DeleteWorkload`. Les déclarations de politique doivent inclure un élément `Action` ou `NotAction`. AWS WA Tool définit son propre ensemble d'actions qui décrivent les tâches que vous pouvez effectuer avec ce service.

Pour afficher la liste des actions AWS WA Tool, consultez Actions définies par AWS Well-Architected Tool dans la Référence de l'autorisation de service.

Ressources de politique

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser les politiques JSON AWS pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour afficher la liste des types de ressources AWS WA Tool et leurs ARN, consultez Ressources définies par AWS Well-Architected Tool dans la Référence de l'autorisation de service. Pour savoir grâce à quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par AWS Well-Architected Tool.

La ressource de charge de travail AWS WA Tool possède l'ARN suivant :

```
arn:${Partition}:wellarchitected:${Region}:${Account}:workload/${ResourceId}
```

Pour plus d'informations sur le format des ARN, consultez Noms ARN (Amazon Resource Name) et Espaces de noms du service AWS.

L'ARN se trouve sur la page Workload properties (Propriétés de la charge de travail) d'une charge de travail. Par exemple, pour spécifier une charge de travail spécifique :

```
"Resource": "arn:aws:wellarchitected:us-
west-2:123456789012:workload/11112222333344445555666677778888"
```

Pour spécifier toutes les charges de travail qui appartiennent à un compte spécifique, utilisez le caractère générique (*) :

```
"Resource": "arn:aws:wellarchitected:us-west-2:123456789012:workload/*"
```

Certaines actions AWS WA Tool, notamment celles pour créer et répertorier des charges de travail, ne peuvent pas être exécutées sur une ressource spécifique. Dans ces cas-là, vous devez utiliser le caractère générique (*).

```
"Resource": "*"
```

Pour afficher la liste des types de ressources AWS WA Tool et leurs ARN, consultez Ressources définies par AWS Well-Architected Tool dans la référence de l'autorisation de service. Pour savoir grâce à quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par AWS Well-Architected Tool.

Clés de condition de politique pour AWS WA Tool

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser les politiques JSON AWS pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` indique à quel moment les instructions s'exécutent en fonction de critères définis. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande. Pour afficher toutes les clés de condition globales AWS, consultez Clés de contexte de condition globales AWS dans le Guide de l'utilisateur IAM.

AWS WA Tool fournit une clé de condition spécifique au service (`wellarchitected:JiraProjectKey`) et prend en charge l'utilisation de certaines clés de condition globales. Pour afficher toutes les clés de condition AWS globales, consultez Clés de contexte de condition AWS globale dans la référence de l'autorisation de service.

Les administrateurs peuvent utiliser les politiques JSON AWS pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` indique à quel moment les instructions s'exécutent en fonction de critères définis. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande. Pour afficher toutes les clés de condition globales AWS, consultez Clés de contexte de condition globales AWS dans le Guide de l'utilisateur IAM.

ACL dans AWS WA Tool

Prend en charge les ACL : non

Les listes de contrôle d'accès (ACL) vérifie quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Autorisation basée sur les balises AWS WA Tool

Prise en charge d'ABAC (balises dans les politiques) : Oui

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs appelés balises. Vous pouvez attacher des balises aux entités IAM et aux

ressources AWS, puis concevoir des politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à celle de la ressource.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur ABAC, consultez Définition d'autorisations avec l'autorisation ABAC dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation des informations d'identification temporaires avec AWS WA Tool

Prend en charge les informations d'identification temporaires : oui

Les informations d'identification temporaires fournissent un accès à court terme aux ressources AWS et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. AWS recommande de générer des informations d'identification temporaires dynamiquement pour utiliser des clés d'accès à long terme. Pour plus d'informations, consultez la section Informations d'identification de sécurité temporaires dans IAM et Services AWS compatibles avec IAM dans le Guide de l'utilisateur IAM.

Autorisations de principal interservices pour AWS WA Tool

Prend en charge les sessions d'accès direct (FAS) : oui

Les sessions FAS utilisent les autorisations du principal en appelant un Service AWS, associé au Service AWS demandeur afin d'effectuer des demandes aux services en aval. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez la section Sessions de transmission d'accès.

Rôles de service pour AWS WA Tool

Prend en charge les rôles de service : Non

Un rôle de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

Rôles liés à un service pour AWS WA Tool

Prend en charge les rôles liés à un service : non

Un rôle lié à un service est un type de rôle de service lié à un Service AWS. Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service s'affichent dans votre Compte AWS et sont détenus par le service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM. Recherchez un service dans le tableau qui inclut un `Yes` dans la colonne Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

AWS Well-Architected ToolExemples de politiques basées sur l'identité

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou modifier les ressources AWS WA Tool. Ils ne peuvent pas non plus exécuter des tâches à l'aide de AWS Management Console, AWS CLI ou de l'API AWS. Un administrateur IAM doit créer des politiques IAM autorisant les utilisateurs et les rôles à exécuter des opérations d'API spécifiques sur les ressources spécifiées dont ils ont besoin. Il doit ensuite attacher ces stratégies aux utilisateurs ou aux groupes ayant besoin de ces autorisations.

Pour savoir comment créer une politique IAM basée sur l'identité à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console AWS WA Tool
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations
- Octroi d'un accès complet aux charges de travail

- Octroi d'un accès en lecture seule aux charges de travail
- Accès à une charge de travail
- Utilisation d'une clé de condition spécifique au service pour le Connecteur de l'AWS Well-Architected Tool pour Jira

Bonnes pratiques en matière de politiques

Les stratégies basées sur l'identité déterminent si une personne peut créer, consulter ou supprimer des ressources AWS WA Tool dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Démarrez avec les politiques gérées par AWS et évoluez vers les autorisations de moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et charges de travail, utilisez les politiques gérées par AWS qui accordent des autorisations dans de nombreux cas d'utilisation courants. Elles sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire encore les autorisations en définissant des politiques AWS gérées par le client qui sont propres à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées via un Service AWS spécifique, comme CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des

recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politiques avec IAM Access Analyzer dans le Guide de l'utilisateur IAM.

- Exigez l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur racine dans votre Compte AWS, activez l'authentification multifactorielle pour une sécurité renforcée. Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console AWS WA Tool

Pour accéder à la console AWS Well-Architected Tool, vous devez disposer d'un ensemble minimum d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les informations relatives aux ressources AWS WA Tool de votre Compte AWS. Si vous créez une politique basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette politique.

Pour garantir que ces entités pourront continuer à utiliser la console AWS WA Tool, attachez également la stratégie gérée AWS suivante aux entités :

```
WellArchitectedConsoleReadOnlyAccess
```

Pour autoriser la création, la modification et la suppression de charges de travail, attachez la stratégie AWS gérée suivante aux entités :

```
WellArchitectedConsoleFullAccess
```

Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

Vous n'avez pas besoin d'accorder les autorisations minimales de console pour les utilisateurs qui effectuent des appels uniquement à l'interface AWS CLI ou API AWS. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API que vous tentez d'effectuer.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations nécessaires pour réaliser cette action sur la console ou par programmation à l'aide de l'AWS CLI ou de l'API AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Octroi d'un accès complet aux charges de travail

Dans cet exemple, vous souhaitez accorder à un utilisateur de votre Compte AWS un accès complet à vos charges de travail. Un accès complet permet à l'utilisateur d'effectuer toutes les actions dans AWS WA Tool. Cet accès est nécessaire pour définir des charges de travail, supprimer des charges de travail, afficher les charges de travail et mettre à jour les charges de travail.

JSON

```
{
   "Version":"2012-10-17",
   "Statement" : [
     {
     "Effect" : "Allow",
     "Action" : [
          "wellarchitected:*"
     ],
     "Resource": "*"
     }
   ]
}
```

Octroi d'un accès en lecture seule aux charges de travail

Dans cet exemple, vous souhaitez accorder à un utilisateur de votre Compte AWS un accès en lecture seule à vos charges de travail. L'accès en lecture seule permet uniquement à l'utilisateur d'afficher les charges de travail dans AWS WA Tool.

JSON

```
{
   "Version":"2012-10-17",
   "Statement" : [
     {
     "Effect" : "Allow",
     "Action" : [
          "wellarchitected:Get*",
          "wellarchitected:List*"
     ],
```

```
      "Resource": "*"
      }
   ]
}
```

Accès à une charge de travail

Dans cet exemple, vous souhaitez accorder à un utilisateur de votre Compte AWS un accès en lecture seule à l'une de vos charges de travail, 99999999999955555555555566666666, dans la région `us-west-2`. L'ID de compte est 777788889999.

JSON

```
{
   "Version":"2012-10-17",
   "Statement" : [
     {
     "Effect" : "Allow",
     "Action" : [
          "wellarchitected:Get*",
          "wellarchitected:List*"
     ],
     "Resource": "arn:aws:wellarchitected:us-
west-2:777788889999:workload/99999999999955555555555666666666"
     }
   ]
}
```

Utilisation d'une clé de condition spécifique au service pour le Connecteur de l'AWS Well-Architected Tool pour Jira

Cet exemple montre comment utiliser la clé de condition spécifique au service `wellarchitected:JiraProjectKey` pour contrôler quels projets Jira peuvent être liés aux charges de travail de votre compte.

Des utilisations pertinentes de la clé de condition sont décrites ci-dessous :

- **`CreateWorkload`:** lorsque vous appliquez `wellarchitected:JiraProjectKey` à `CreateWorkload`, vous pouvez définir quels projets Jira personnalisés peuvent être liés à une

charge de travail quelconque créée par l'utilisateur. Par exemple, si un utilisateur essaie de créer une nouvelle charge de travail avec le projet ABC, mais que la politique spécifie uniquement le projet PQR, l'action est refusée.

- **`UpdateWorkload`:** lorsque vous appliquez `wellarchitected:JiraProjectKey` à `UpdateWorkload`, vous pouvez définir quels projets Jira personnalisés peuvent être liés à cette charge de travail particulière ou à une charge de travail quelconque. Par exemple, si un utilisateur essaie de mettre à jour une charge de travail existante avec le projet ABC, mais que la politique spécifie le projet PQR, l'action est refusée. En outre, si l'utilisateur a une charge de travail liée au projet PQR et essaie de mettre à jour la charge de travail pour qu'elle soit liée au projet ABC, l'action est refusée.
- **`UpdateGlobalSettings`:** lorsque vous appliquez `wellarchitected:JiraProjectKey` à `UpdateGlobalSettings`, vous pouvez définir quels projets Jira personnalisés peuvent être liés au Compte AWS. Le paramètre au niveau du compte protège les charges de travail de votre compte qui ne remplacent pas les paramètres Jira au niveau du compte. Par exemple, si un utilisateur a accès à `UpdateGlobalSettings`, il ne peut pas lier les charges de travail de votre compte à des projets non spécifiés dans la politique.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
  {
   "Sid": "VisualEditor0",
   "Effect": "Allow",
   "Action": [
    "wellarchitected:UpdateGlobalSettings",
    "wellarchitected:CreateWorkload"
   ],
   "Resource": "*",
   "Condition": {
    "StringEqualsIfExists": {
     "wellarchitected:JiraProjectKey": ["ABC, PQR"]
    }
   }
  },
  {
   "Sid": "VisualEditor1",
```

```
    "Effect": "Allow",
    "Action": [
     "wellarchitected:UpdateWorkload"
    ],
    "Resource": "arn:aws:wellarchitected:us-east-1:111122223333:workload/example-
workload",
    "Condition": {
     "StringEqualsIfExists": {
      "wellarchitected:JiraProjectKey": ["ABC, PQR"]
     }
    }
   }
  ]
}
```

Politiques gérées par AWS pour AWS Well-Architected Tool

Une politique gérée par AWS est une politique autonome créée et administrée par AWS. Les politiques gérées par AWS sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

Gardez à l'esprit que les politiques gérées par AWS peuvent ne pas accorder les autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont disponibles pour tous les clients AWS. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques gérées par AWS. Si AWS met à jour les autorisations définies dans une politique gérée par AWS, la mise à jour affecte toutes les identités de principal (utilisateurs, groupes et rôles) auxquelles la politique est associée. AWS est plus susceptible de mettre à jour une politique gérée par AWS lorsqu'un nouveau Service AWS est lancé ou lorsque de nouvelles opérations API deviennent accessibles pour les services existants.

Pour plus d'informations, consultez Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS Politique gérée par: WellArchitectedConsoleFullAccess

Vous pouvez associer la politique `WellArchitectedConsoleFullAccess` à vos identités IAM.

Cette politique accorde à un accès total à AWS Well-Architected Tool.

Détails de l'autorisation

JSON

```
{
   "Version":"2012-10-17",
   "Statement" : [
     {
     "Effect" : "Allow",
     "Action" : [
          "wellarchitected:*"
     ],
     "Resource": "*"
     }
   ]
}
```

AWS Politique gérée par: WellArchitectedConsoleReadOnlyAccess

Vous pouvez associer la politique `WellArchitectedConsoleReadOnlyAccess` à vos identités IAM.

Cette politique accorde un accès en lecture seule à l'AWS Well-Architected Tool.

Détails de l'autorisation

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "wellarchitected:Get*",
                "wellarchitected:List*",
                "wellarchitected:ExportLens"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

AWS Politique gérée par: AWSWellArchitectedOrganizationsServiceRolePolicy

Vous pouvez associer la politique `AWSWellArchitectedOrganizationsServiceRolePolicy` à vos identités IAM.

Cette politique accorde les autorisations administratives dans AWS Organizations qui sont nécessaires pour prendre en charge l'intégration de l'AWS Well-Architected Tool à Organizations. Ces autorisations permettent au compte de gestion de l'organisation d'activer le partage des ressources avec AWS WA Tool.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `organizations:ListAWSServiceAccessForOrganization` : autorise les principaux à vérifier si l'accès aux services AWS est activé pour l'AWS WA Tool.
- `organizations:DescribeAccount` : autorise les principaux à extraire des informations sur un compte dans l'organisation.
- `organizations:DescribeOrganization` : autorise les principaux à extraire des informations sur la configuration de l'organisation.
- `organizations:ListAccounts` : autorise les principaux à extraire la liste des comptes appartenant à une organisation.
- `organizations:ListAccountsForParent` : autorise les principaux à extraire la liste des comptes appartenant à une organisation à partir d'un nœud racine donné dans l'organisation.
- `organizations:ListChildren` : autorise les principaux à extraire la liste des comptes et des unités d'organisation appartenant à une organisation à partir d'un nœud racine donné dans l'organisation.
- `organizations:ListParents` : autorise les principaux à extraire la liste des parents immédiats spécifiés par l'unité d'organisation ou le compte au sein d'une organisation.
- `organizations:ListRoots` : autorise les principaux à extraire la liste de tous les nœuds racines au sein d'une organisation.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListChildren",
                "organizations:ListParents",
                "organizations:ListRoots"
            ],
            "Resource": "*"
        }
    ]
}
```

Politique gérée par AWS : AWSWellArchitectedDiscoveryServiceRolePolicy

Vous pouvez associer la politique `AWSWellArchitectedDiscoveryServiceRolePolicy` à vos identités IAM.

Cette politique autorise l'AWS Well-Architected Tool à accéder aux services et aux ressources AWS liés aux ressources de l'AWS WA Tool.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `trustedadvisor:DescribeChecks` : dresse la liste des vérifications Trusted Advisor disponibles.
- `trustedadvisor:DescribeCheckItems` : récupère les données des vérifications Trusted Advisor, y compris le statut et les ressources signalés par Trusted Advisor.
- `servicecatalog:GetApplication` : récupère les détails d'une application AppRegistry.

- `servicecatalog:ListAssociatedResources` : répertorie les ressources associées à une application AppRegistry.
- `cloudformation:DescribeStacks` : obtient les détails des piles CloudFormation.
- `cloudformation:ListStackResources` : dresse la liste des ressources associées aux piles CloudFormation.
- `resource-groups:ListGroupResources` : dresse la liste des ressources d'un ResourceGroup.
- `tag:GetResources` : requis pour ListGroupResources.
- `servicecatalog:CreateAttributeGroup` : crée un groupe d'attributs géré par le service lorsque cela est nécessaire.
- `servicecatalog:AssociateAttributeGroup` : associe un groupe d'attributs géré par le service à une application AppRegistry.
- `servicecatalog:UpdateAttributeGroup` : met à jour un groupe d'attributs géré par le service.
- `servicecatalog:DisassociateAttributeGroup` : dissocie un groupe d'attributs géré par le service d'une application AppRegistry.
- `servicecatalog:DeleteAttributeGroup` : supprime un groupe d'attributs géré par le service lorsque cela est nécessaire.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "trustedadvisor:DescribeChecks",
    "trustedadvisor:DescribeCheckItems"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Effect": "Allow",
```

```
   "Action": [
    "cloudformation:DescribeStacks",
    "cloudformation:ListStackResources",
    "resource-groups:ListGroupResources",
    "tag:GetResources"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "servicecatalog:ListAssociatedResources",
    "servicecatalog:GetApplication",
    "servicecatalog:CreateAttributeGroup"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "servicecatalog:AssociateAttributeGroup",
    "servicecatalog:DisassociateAttributeGroup"
   ],
   "Resource": [
    "arn:*:servicecatalog:*:*:/applications/*",
    "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "servicecatalog:UpdateAttributeGroup",
    "servicecatalog:DeleteAttributeGroup"
   ],
   "Resource": [
    "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
   ]
  }
 ]
```

```
}
```

Mises à jour AWS WA Tool vers des politiques gérées par AWS

Consultez le détail des mises à jour des politiques gérées par AWS pour AWS WA Tool depuis que ce service a commencé à suivre ces modifications. Pour obtenir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la Page de révisions du document AWS WA Tool.

Modification	Description	Date
Politique gérée modifiée par l'AWS WA Tool	Ajout de `"wellarchitected:Export*"` à `WellArchitectedConsoleReadOnlyAccess` .	22 juin 2023
Politique de rôle de service ajoutée par l'AWS WA Tool	La politique `AWSWellArchitectedDiscoveryServiceRolePolicy` a été ajoutée pour autoriser l'AWS Well-Architected Tool à accéder aux services et aux ressources AWS liés aux ressources de l'AWS WA Tool.	3 mai 2023
Autorisations ajoutées par AWS WA Tool	Une nouvelle action a été ajoutée pour accorder la politique `ListAWSServiceAccessForOrganization` afin d'autoriser l'AWS WA Tool à vérifier si l'accès aux services AWS est activé pour l'AWS WA Tool.	22 juillet 2022
AWS WA Tool a démarré le suivi des modifications	AWS WA Tool a commencé à suivre les modifications	22 juillet 2022

Modification	Description	Date
	pour ses politiques gérées par AWS.	

Résolution des problèmes d'identité et d'accès avec AWS Well-Architected Tool

Utilisez les informations suivantes pour identifier et résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec AWS WA Tool et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans AWS WA Tool

Je ne suis pas autorisé à effectuer une action dans AWS WA Tool

Si la AWS Management Console indique que vous n'êtes pas autorisé à exécuter une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni vos informations de connexion.

L'exemple d'erreur suivant se produit quand l'utilisateur *mateojackson* essaie d'utiliser la console pour effectuer l'action `DeleteWorkload`, mais qu'il ne dispose pas des autorisations nécessaires.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
 perform: wellarchitected:DeleteWorkload on resource: 11112222333344445555666677778888
```

Pour cet exemple, demandez à votre administrateur de mettre à jour vos stratégies pour vous permettre d'accéder à la ressource `11112222333344445555666677778888` à l'aide de l'action `wellarchitected:DeleteWorkload`.

Réponse aux incidents dans AWS Well-Architected Tool

La réponse aux incidents pour AWS Well-Architected Tool est de la responsabilité d'AWS. AWS dispose d'une politique et d'un programme officiels et documentés qui régissent la réponse aux incidents.

Les problèmes opérationnels AWS avec des répercussions majeures sont publiés dans le AWS Service Health Dashboard.

Les problèmes opérationnels sont également postés dans les comptes individuels via le Tableau de bord AWS Health. Pour plus d'informations sur la façon d'utiliser le Tableau de bord Health, consultez le Guide de l'utilisateur AWS Health.

Validation de la conformité pour AWS Well-Architected Tool

Pour savoir si un Service AWS fait partie du champ d'application de programmes de conformité spécifiques, consultez Services AWS concernés par le programme de conformité et choisissez le programme de conformité qui vous intéresse. Pour obtenir des renseignements généraux, consultez Programmes de conformité AWS.

Vous pouvez télécharger les rapports de l'audit externe avec AWS Artifact. Pour plus d'informations, consultez Téléchargement de rapports dans AWS Artifact.

Votre responsabilité de conformité lors de l'utilisation de Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise, ainsi que par la législation et la réglementation applicables. Pour plus d'informations sur votre responsabilité en matière de conformité lors de l'utilisation des Services AWS, consultez la documentation de sécurité AWS.

Résilience dans AWS Well-Architected Tool

L'infrastructure mondiale d'AWS est construite autour de zones de disponibilité et de Régions AWS. Les Régions AWSfournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone de disponibilité à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les Régions AWS et les zones de disponibilité, consultez Infrastructure mondiale d'AWS.

Sécurité de l'infrastructure dans AWS Well-Architected Tool

En tant que service géré, AWS Well-Architected Tool est protégé par les procédures de sécurité du réseau mondial AWS. Pour plus d'informations sur les services de sécurité AWS et la manière

dont AWS protège l'infrastructure, consultez la section Sécurité du cloud AWS. Pour concevoir votre environnement AWS en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le Security Pillar AWS Well-Architected Framework (Pilier de sécurité de l'infrastructure Well-Architected Framework).

Vous utilisez les appels d'API publiés AWS pour accéder à AWS WA Tool via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

Analyse de la configuration et des vulnérabilités dans AWS Well-Architected Tool

La configuration et les contrôles informatiques sont une responsabilité partagée entre AWS et vous, notre client. Pour plus d'informations, consultez Modèle de responsabilité partagée AWS.

Prévention du cas de figure de l'adjoint désorienté entre services

Le problème de député confus est un problème de sécurité dans lequel une entité qui n'est pas autorisée à effectuer une action peut contraindre une entité plus privilégiée à le faire. Dans AWS, l'emprunt d'identité entre services peut entraîner le problème de député confus. L'usurpation d'identité entre services peut se produire lorsqu'un service (le service appelant) appelle un autre service (le service appelé). Le service appelant peut être manipulé et ses autorisations utilisées pour agir sur les ressources d'un autre client auxquelles on ne serait pas autorisé à accéder autrement. Pour éviter cela, AWS fournit des outils qui vous aident à protéger vos données pour tous les services avec des principaux de service qui ont eu accès aux ressources de votre compte.

Nous vous recommandons d'utiliser les clés de contexte de condition globale `aws:SourceArn` et `aws:SourceAccount` dans les politiques de ressources afin de limiter les autorisations à la ressource octroyées par AWS Well-Architected Tool à un autre service. Utilisez `aws:SourceArn` si vous souhaitez qu'une seule ressource soit associée à l'accès entre services. Utilisez `aws:SourceAccount` si vous souhaitez autoriser l'association d'une ressource de ce compte à l'utilisation interservices.

Le moyen le plus efficace de se protéger contre le problème de député confus consiste à utiliser la clé de contexte de condition globale `aws:SourceArn` avec l'ARN complet de la ressource. Si vous ne connaissez pas l'ARN complet de la ressource ou si vous spécifiez plusieurs ressources, utilisez la clé de contexte de condition globale `aws:SourceArn` avec des caractères génériques (*) pour les parties inconnues de l'ARN. Par exemple, `arn:aws:wellarchitected:*:123456789012:*`.

Si la valeur `aws:SourceArn` ne contient pas l'ID du compte, tel qu'un ARN de compartiment Amazon S3, vous devez utiliser les deux clés de contexte de condition globale pour limiter les autorisations.

La valeur d'`aws:SourceArn` doit être une charge de travail ou une section Lens.

L'exemple suivant montre comment utiliser les clés de contexte de condition globale `aws:SourceArn` et `aws:SourceAccount` dans AWS WA Tool afin d'éviter le problème de l'adjoint confus.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "wellarchitected.amazonaws.com"
    },
    "Action": "wellarchitected:CreateWorkload",
    "Resource": [
    "arn:aws:wellarchitected:us-east-1:111122223333:ResourceName/*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:wellarchitected:*:123456789012:*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

Partage de vos ressources AWS WA Tool

Pour partager une ressource dont vous êtes propriétaire, procédez comme suit :

- Activation du partage des ressources au sein d'AWS Organizations (facultatif)
- Partage d'une charge de travail
- Partage d'un objectif personnalisé
- Partage d'un profil
- Partage d'un modèle d'examen

Remarques

- Le partage d'une ressource la rend disponible pour une utilisation par des principaux en dehors du Compte AWS qui a créé la ressource. Le partage ne modifie aucune autorisation qui s'applique à la ressource dans le compte qui l'a créée.
- AWS WA Tool est un service régional. Les principaux avec lesquels vous partagez peuvent accéder aux partages de ressources uniquement dans les Régions AWS où ils ont été créés.
- Pour partager des ressources dans une région introduite après le 20 mars 2019, vous et le Compte AWS partagé devez activer la région dans la AWS Management Console. Pour plus d'informations, consultez Infrastructure mondiale AWS.

Activation du partage des ressources au sein d'AWS Organizations

Lorsque votre compte est géré par AWS Organizations, vous pouvez en profiter pour partager des ressources plus facilement. Avec ou sans Organizations, un utilisateur peut partager avec des comptes individuels. Toutefois, si votre compte correspond à une organisation, vous pouvez partager avec des comptes individuels, ou avec tous les comptes de l'organisation ou d'une unité organisationnelle sans avoir à énumérer chaque compte.

Pour partager des ressources au sein d'une organisation, vous devez d'abord utiliser la console AWS WA Tool ou l'AWS Command Line Interface (AWS CLI) pour activer le partage avec AWS Organizations. Lorsque vous partagez des ressources au sein de votre organisation, AWS WA

Tool n'envoie pas d'invitations aux principaux. Les principaux de votre organisation ont accès aux ressources partagées sans échanger d'invitations.

Lorsque vous activez le partage des ressources au sein de votre organisation, AWS WA Tool crée un rôle lié à un service appelé `AWSServiceRoleForWellArchitected`. Ce rôle peut être assumé uniquement par le service AWS WA Tool et il accorde à AWS WA Tool l'autorisation d'extraire des informations sur l'organisation dont il est membre, à l'aide de la politique gérée par AWS `AWSWellArchitectedOrganizationsServiceRolePolicy`.

Si vous n'avez plus besoin de partager des ressources avec l'ensemble de votre organisation ou de vos unités organisationnelles, vous pouvez désactiver le partage des ressources.

Exigences

- Vous ne pouvez effectuer ces étapes que lorsque vous êtes connecté en tant que principal dans le compte de gestion de l'organisation.
- Toutes les fonctionnalités doivent être activées pour l'organisation. Pour plus d'informations, consultez Activation de toutes les fonctionnalités de votre organisation dans le Guide de l'utilisateur AWS Organizations.

> **Important**
>
> Vous devez activer le partage avec AWS Organizations à l'aide de la console AWS WA Tool. Cela garantit que le`AWSServiceRoleForWellArchitected` rôle lié à un service est créé. Si vous activez l'accès approuvé avec AWS Organizations à l'aide de la console AWS Organizations ou de la commande AWS CLI enable-aws-service-access, le rôle lié à un service `AWSServiceRoleForWellArchitected` n'est pas créé et vous ne pouvez pas partager de ressources au sein de votre organisation.

Pour activer le partage des ressources au sein de votre organisation

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.

   Vous devez vous connecter en tant que principal dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Choisissez Activer la prise en charge AWS Organizations.

4. Choisissez Save settings (Enregistrer les paramètres).

Pour désactiver le partage des ressources au sein de votre organisation

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.

   Vous devez vous connecter en tant que principal dans le compte de gestion de l'organisation.
2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Désélectionnez Activer la prise en charge AWS Organizations.
4. Choisissez Save settings (Enregistrer les paramètres).

Balisage de vos ressources AWS WA Tool

Pour vous aider à gérer vos ressources AWS WA Tool, vous pouvez attribuer vos propres métadonnées à chaque ressource sous la forme de balises. Cette rubrique décrit les balises et vous explique comment les créer.

Table des matières

Principes de base des balises

Une balise est une étiquette que vous affectez à une ressource AWS. Chaque balise est constituée d'une clé et d'une valeur facultative que vous définissez.

Les balises vous permettent de classer vos ressources AWS par catégorie, objectif, propriétaire ou environnement, par exemple. Lorsque vous avez de nombreuses ressources de même type, vous pouvez rapidement identifier une ressource spécifique en fonction des balises que vous lui avez attribuées. Par exemple, vous pouvez définir un ensemble de balises pour vos services AWS WA Tool afin de vous aider à suivre le propriétaire et le niveau de pile de chaque service. Nous vous recommandons de concevoir un ensemble cohérent de clés de balise pour chaque type de ressource.

Les balises ne sont pas automatiquement affectées à vos ressources. Une fois que vous avez ajouté une balise, vous pouvez modifier les clés et valeurs de balise ou supprimer les balises d'une ressource à tout moment. Si vous supprimez une ressource, ses balises sont également supprimées.

Les balises n'ont pas de signification sémantique pour AWS WA Tool et sont interprétées strictement comme des chaînes de caractères. Vous pouvez définir la valeur d'une balise sur une chaîne vide, mais vous ne pouvez pas définir la valeur d'une balise sur null. Si vous ajoutez une balise ayant la même clé qu'une balise existante sur cette ressource, la nouvelle valeur remplace l'ancienne valeur.

Vous pouvez gérer les balises à l'aide de la AWS Management Console, de l'AWS CLI et de l'API AWS WA Tool.

Si vous utilisez Gestion des identités et des accès AWS (IAM), vous pouvez contrôler quels utilisateurs de votre Compte AWS sont autorisés à créer, modifier ou supprimer des balises.

Identification de vos ressources

Vous pouvez appliquer des balises aux ressources AWS WA Tool nouvelles ou existantes.

Si vous utilisez la console AWS WA Tool, vous pouvez appliquer des balises aux nouvelles ressources au moment de leur création ou aux ressources existantes à tout moment. Pour les charges de travail existantes, vous pouvez appliquer des balises via l'onglet Propriétés. Pour les objectifs personnalisés, les profils et les modèles d'examen existants, vous pouvez appliquer des balises via l'onglet Présentation.

Si vous utilisez l'API AWS WA Tool, l'AWS CLI ou un kit AWS SDK, vous pouvez appliquer les balises aux nouvelles ressources à l'aide du paramètre `tags` sur l'action d'API correspondante ou utiliser l'action d'API `TagResource`. Pour en savoir plus, consultez TagResource.

En outre, certaines actions de création de ressources vous permettent de spécifier des balises pour une ressource lors de la création de cette dernière. Si des balises ne peuvent pas être appliquées au cours de la création de ressources, le processus de création de ressources échoue. Cela garantit que les ressources que vous vouliez baliser lors de la création sont créées avec des balises spécifiées ou ne sont pas créées du tout. Si vous balisez des ressources au moment de la création, vous n'avez pas besoin d'exécuter de scripts de balisage personnalisés après la création des ressources.

Le tableau suivant décrit les ressources AWS WA Tool qui peuvent porter des balises, et les ressources qui peuvent porter des balises dès la création.

Prise en charge du balisage pour les ressources AWS WA Tool

Ressource	Prend en charge les étiquettes	Prend en charge la propagation des étiquettes	Prend en charge le balisage au moment de la création (API AWS WA Tool, AWS CLI, kit AWS SDK)
charges de travail AWS WA Tool	Oui	Non	Oui
objectifs personnalisés AWS WA Tool	Oui	Non	Oui

Ressource	Prend en charge les étiquettes	Prend en charge la propagation des étiquettes	Prend en charge le balisage au moment de la création (API AWS WA Tool, AWS CLI, kit AWS SDK)
AWS WA ToolProfils	Oui	Non	Oui
modèles d'examen AWS WA Tool	Oui	Non	Oui

Restrictions liées aux étiquettes

Les restrictions de base suivantes s'appliquent aux balises :

- Nombre maximal de balises par ressource : 50
- Pour chaque ressource, chaque clé de balise doit être unique, et chaque clé de balise peut avoir une seule valeur.
- Longueur de clé maximale : 128 caractères Unicode en UTF-8
- Longueur de valeur maximale : 256 caractères Unicode en UTF-8
- Si votre schéma de balisage est utilisé pour plusieurs services et ressources AWS, n'oubliez pas que d'autres services peuvent avoir des restrictions concernant les caractères autorisés. Les caractères généralement autorisés sont les lettres, les chiffres et les espaces représentables en UTF-8, ainsi que les caractères suivants : + - = . _ : / @.
- Les clés et valeurs de balise sont sensibles à la casse.
- N'utilisez pas `aws:`, `AWS:`, ou n'importe quelle combinaison de majuscules ou minuscules comme préfixe pour des clés ou des valeurs, car il est réservé à AWS. Vous ne pouvez pas modifier ni supprimer des clés ou valeurs d'étiquette ayant ce préfixe. Les balises avec ce préfixe ne sont pas comptabilisées comme vos balises pour la limite de ressources.

Gestion des étiquettes à l'aide de la console

À l'aide de la console AWS WA Tool, vous pouvez gérer les balises associées aux ressources nouvelles ou existantes.

Ajout de balises sur une ressource individuelle lors de la création

Vous pouvez ajouter des balises aux ressources AWS WA Tool lors de leur création.

Ajout et suppression de balises sur une ressource individuelle

AWS WA Tool vous permet d'ajouter ou de supprimer des balises associées à vos ressources directement depuis l'onglet Propriétés pour une charge de travail, et depuis l'onglet Présentation pour les objectifs personnalisés, les profils et les modèles d'examen.

Pour ajouter ou supprimer une balise sur une charge de travail

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.
2. Dans la barre de navigation, choisissez la région à utiliser.
3. Dans le panneau de navigation, choisissez Charges de travail.
4. Sélectionnez la charge de travail à modifier et choisissez Propriétés.
5. Dans la section Balises choisissez Gérer les balises.
6. Ajoutez ou supprimez vos balises selon vos besoins.
   - Pour ajouter une balise, choisissez Ajouter une nouvelle balise, puis renseignez les champs Clé et Valeur.
   - Pour supprimer une balise, sélectionnez Remove (Supprimer).
7. Répétez cette procédure pour chaque balise que vous voulez ajouter, modifier ou supprimer. Choisissez Save pour enregistrer les changements.

Pour ajouter ou supprimer une balise sur un objectif personnalisé

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.
2. Dans la barre de navigation, choisissez la région à utiliser.
3. Dans le volet de navigation, choisissez Lentilles personnalisées.
4. Sélectionnez le nom de l'objectif personnalisé à modifier.
5. Dans la section Balises de l'onglet Présentation, choisissez Gérer les balises.
6. Ajoutez ou supprimez vos balises selon vos besoins.

- Pour ajouter une balise, choisissez Ajouter une nouvelle balise, puis renseignez les champs Clé et Valeur.
- Pour supprimer une balise, sélectionnez Remove (Supprimer).

7. Répétez cette procédure pour chaque balise que vous voulez ajouter, modifier ou supprimer. Choisissez Save pour enregistrer les changements.

Pour ajouter ou supprimer une balise sur un profil

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.
2. Dans la barre de navigation, choisissez la région à utiliser.
3. Dans le volet de navigation, choisissez Profils.
4. Sélectionnez le nom du profil à modifier.
5. Dans la section Balises de l'onglet Présentation, choisissez Gérer les balises.
6. Ajoutez ou supprimez vos balises selon vos besoins.

   - Pour ajouter une balise, choisissez Ajouter une nouvelle balise, puis renseignez les champs Clé et Valeur.
   - Pour supprimer une balise, sélectionnez Remove (Supprimer).

7. Répétez cette procédure pour chaque balise que vous voulez ajouter, modifier ou supprimer. Choisissez Save pour enregistrer les changements.

Pour ajouter ou supprimer une balise sur un modèle d'examen

1. Connectez-vous à la AWS Management Console et ouvrez la console de l'AWS Well-Architected Tool à l'adresse https://console.aws.amazon.com/wellarchitected/.
2. Dans la barre de navigation, choisissez la région à utiliser.
3. Dans le volet de navigation, choisissez Modèles d'examen.
4. Sélectionnez le nom du modèle d'examen à modifier.
5. Dans la section Balises de l'onglet Présentation, choisissez Gérer les balises.
6. Ajoutez ou supprimez vos balises selon vos besoins.

   - Pour ajouter une balise, choisissez Ajouter une nouvelle balise, puis renseignez les champs Clé et Valeur.

- Pour supprimer une balise, sélectionnez Remove (Supprimer).

7. Répétez cette procédure pour chaque balise que vous voulez ajouter, modifier ou supprimer. Choisissez Save pour enregistrer les changements.

Utilisation des balises à l'aide de l'API

Utilisez les opérations d'API AWS WA Tool pour ajouter, mettre à jour, répertorier et supprimer les balises de vos ressources.

Prise en charge du balisage pour les ressources AWS WA Tool

Tâche	Action d'API
Ajouter ou remplacer une ou plusieurs étiquettes.	TagResource
Supprimer une ou plusieurs étiquettes.	UntagResource
Répertoriez les balises d'une ressource.	ListTagsForResource

Certaines actions de création de ressources vous permettent de spécifier des étiquettes lorsque vous créez la ressource. Les actions suivantes prennent en charge l'identification lors de la création.

Tâche	Action d'API
Création d'une charge de travail	CreateWorkload
Importer un nouvel objectif	ImportLens
Créer un profil	CreateProfile
Création d'un modèle d'examen	CreateReviewTemplate

Journalisation des appels d'API AWS WA Tool avec AWS CloudTrail

AWS Well-Architected Tool est intégré avec AWS CloudTrail, un service qui fournit un registre des actions prises par un utilisateur, un rôle ou un service AWS dans AWS WA Tool. CloudTrail capture les appels d'API vers AWS WA Tool en tant qu'événements. Les appels capturés incluent des appels de la console AWS WA Tool et les appels de code vers les opérations d'API AWS WA Tool. Si vous créez un journal d'activité, vous pouvez activer la livraison continue d'événements CloudTrail à un compartiment Amazon S3, y compris des événements pour AWS WA Tool. Si vous ne configurez pas de journal de suivi, vous pouvez toujours afficher les événements les plus récents dans la console CloudTrail dans Historique des événements. Avec les informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été envoyée à l'AWS WA Tool, ainsi que l'adresse IP, l'auteur et date de la demande, ainsi que d'autres détails.

Pour en savoir plus sur CloudTrail, consultez le Guide de l'utilisateur AWS CloudTrail.

Informations AWS WA Tool dans CloudTrail

CloudTrail est activé dans votre Compte AWS lors de la création de ce dernier. Quand une activité a lieu dans AWS WA Tool, cette activité est enregistrée dans un événement CloudTrail avec d'autres événements de service AWS dans l'Historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre Compte AWS. Pour de plus amples informations, veuillez consulter Affichage des événements avec l'historique des événements CloudTrail.

Pour un enregistrement continu des événements dans votre Compte AWS, y compris les événements pour AWS WA Tool, créez un journal d'activité. Un journal d'activité permet à CloudTrail de distribuer les fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal de suivi consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres services AWS pour analyser et agir sur les données d'événements collectées dans les journaux CloudTrail. Pour plus d'informations, consultez les ressources suivantes :

- Vue d'ensemble de la création d'un journal d'activité
- Intégrations et services pris en charge par CloudTrail
- Configuration des notifications d'Amazon SNS pour CloudTrail

- Réception des fichiers journaux CloudTrail de plusieurs régions et Réception des fichiers journaux CloudTrail de plusieurs comptes

Toutes les actions AWS WA Tool sont consignées par CloudTrail et documentées dans Actions définies par AWS Well-Architected Tool. À titre d'exemple, les appels vers les actions `CreateWorkload`, `DeleteWorkload` et `CreateWorkloadShare` génèrent des entrées dans les fichiers journaux CloudTrail.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été effectuée avec des informations d'identification d'utilisateur ou d'utilisateur racine.
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été effectuée par un autre service AWS.

Pour plus d'informations, consultez Élément userIdentity CloudTrail.

Présentation des AWS WA Tool entrées des fichiers journaux

Un journal d'activité est une configuration qui permet d'envoyer les événements dans des fichiers journaux à un compartiment Amazon S3 que vous spécifiez. Les fichiers journaux CloudTrail peuvent contenir une ou plusieurs entrées. Un événement représente une demande unique provenant de n'importe quelle source et comprend des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. Les fichiers journaux CloudTrail ne constituent pas une série ordonnée retraçant les appels d'API publics. Ils ne suivent aucun ordre précis.

L'exemple suivant présente une entrée de journal CloudTrail qui illustre l'action `CreateWorkload`.

```
   {
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:dev-dsk-xiulan-2a-1111111c.us-
west-2.amazon.com",
```

```
        "arn": "arn:aws:sts::444455556666:assumed-role/well-architected-api-svc-integ-
test-read-write/dev-dsk-xiulan-2a-1111111c.us-west-2.amazon.com",
        "accountId": "444455556666",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::444455556666:role/well-architected-api-svc-integ-
test-read-write",
                "accountId": "444455556666",
                "userName": "well-architected-api-svc-integ-test-read-write"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-10-14T03:41:39Z"
            }
        }
    },
    "eventTime": "2020-10-14T04:43:13Z",
    "eventSource": "wellarchitected.amazonaws.com",
    "eventName": "CreateWorkload",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.178",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.848
 Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.262-b10
 java/1.8.0_262 vendor/Oracle_Corporation",
    "requestParameters": {
           "ClientRequestToken": "08af866a-0238-4070-89c2-b689ca8339f7",
           "Description": "***",
           "AwsRegions": [
               "us-west-2"
           ],
           "ReviewOwner": "***",
           "Environment": "PRODUCTION",
           "Name": "***",
           "Lenses": [
               "wellarchitected",
               "serverless"
           ]
    },
    "responseElements": {
```

```
        "Arn": "arn:aws:wellarchitected:us-
west-2:444455556666:workload/8cdcdf7add10b181fdd3f686dacffdac",
        "Id": "8cdcdf7add10b181fdd3f686dacffdac"
    },
    "requestID": "22bad4e3-aa51-4ff1-b480-712ee07cedbd",
    "eventID": "50849dfd-36ed-418e-a901-49f6ac7087e8",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "444455556666"
}
```

EventBridge

AWS Well-Architected Tool envoie des événements à Amazon EventBridge lorsque des actions sont entreprises sur des ressources Well-Architected. Vous pouvez utiliser EventBridge et ces événements pour écrire des règles qui prennent des mesures, telles que vous avertir, lors d'une modification de ressource. Pour plus d'informations, consultez Qu'est-ce qu'Amazon EventBridge ?

> **Note**
>
> Les événements sont fournis dans la mesure du possible.

Les actions suivantes génèrent des événements EventBridge :

- Liées à une charge de travail
  - Création ou suppression d'une charge de travail
  - Création d'un jalon
  - Mise à jour des propriétés d'une charge de travail
  - Partage ou annulation du partage d'une charge de travail
  - Mise à jour du statut d'une invitation de partage
  - Ajout ou suppression de balises
  - Mise à jour d'une réponse
  - Mise à jour des notes de vérification
  - Ajout ou suppression d'un objectif d'une charge de travail
- Liées à un objectif
  - Importation ou exportation d'un objectif personnalisé
  - Publication d'un objectif personnalisé
  - Suppression d'un objectif personnalisé
  - Partage ou annulation du partage d'un objectif personnalisé
  - Mise à jour du statut d'une invitation de partage
  - Ajout ou suppression d'un objectif d'une charge de travail

Exemples d'événement à partir de AWS WA Tool

Cette section inclut des exemples d'événements à partir de AWS Well-Architected Tool.

Mise à jour d'une réponse dans une charge de travail


```
{
  "version":"0",
  "id":"00de336a-83cc-b80b-f0e6-f44c88a96050",
  "detail-type":"AWS API Call via CloudTrail",
  "source":"aws.wellarchitected",
  "account":"123456789012",
  "time":"2022-02-17T08:01:25Z",
  "region":"us-west-2",
  "resources":[],
  "detail":{
     "eventVersion":"1.08",
     "userIdentity":{
        "type":"AssumedRole",
        "principalId":"AROA4JUSXMN5ZR6S7LZNP:sample-user",
        "arn":"arn:aws:sts::123456789012:assumed-role/Admin/example-user",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "sessionContext":{
           "sessionIssuer":{
              "type":"Role",
              "principalId":"AROA4JUSXMN5ZR6S7LZNP",
              "arn":"arn:aws:iam::123456789012:role/Admin",
              "accountId":"123456789012",
              "userName":"Admin"
           },
           "webIdFederationData":{},
           "attributes":{
              "creationDate":"2022-02-17T07:21:54Z",
              "mfaAuthenticated":"false"
           }
        }
     },
     "eventTime":"2022-02-17T08:01:25Z",
     "eventSource":"wellarchitected.amazonaws.com",
     "eventName":"UpdateAnswer",
     "awsRegion":"us-west-2",
```

```
      "sourceIPAddress":"10.246.162.39",
      "userAgent":"aws-internal/3 aws-sdk-java/1.12.127
 Linux/5.4.156-94.273.amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/25.312-b07
 java/1.8.0_312 vendor/Oracle_Corporation cfg/retry-mode/standard",
      "requestParameters":{
         "Status":"Acknowledged",
         "SelectedChoices":"***",
         "ChoiceUpdates":"***",
         "QuestionId":"priorities",
         "WorkloadId":"ee73fda518f9bd4aa804c6252e4e37b0",
         "IsApplicable":true,
         "LensAlias":"wellarchitected",
         "Reason":"NONE",
         "Notes":"***"
      },
      "responseElements":{
         "Answer":"***",
         "LensAlias":"wellarchitected",
         "WorkloadId":"ee73fda518f9bd4aa804c6252e4e37b0"
      },
      "requestID":"7bae1153-26a8-4dc0-9307-68b17b107619",
      "eventID":"8339c258-4ddd-48aa-ab21-3f82ce9d79cd",
      "readOnly":false,
      "eventType":"AwsApiCall",
      "managementEvent":true,
      "recipientAccountId":"123456789012",
      "eventCategory":"Management"
   }
}
```


Publication d'un objectif personnalisé


```
{
   "version":"0",
   "id":"4054a34b-60a9-53c1-3146-c1a384dba41b",
   "detail-type":"AWS API Call via CloudTrail",
   "source":"aws.wellarchitected",
   "account":"123456789012",
   "time":"2022-02-17T08:58:34Z",
   "region":"us-west-2",
   "resources":[],
```

```
   "detail":{
      "eventVersion":"1.08",
      "userIdentity":{
         "type":"AssumedRole",
         "principalId":"AROA4JUSXMN5ZR6S7LZNP:example-user",
         "arn":"arn:aws:sts::123456789012:assumed-role/Admin/example-user",
         "accountId":"123456789012",
         "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
         "sessionContext":{
            "sessionIssuer":{
               "type":"Role",
               "principalId":"AROA4JUSXMN5ZR6S7LZNP",
               "arn":"arn:aws:iam::123456789012:role/Admin",
               "accountId":"123456789012",
               "userName":"Admin"
            },
            "webIdFederationData":{},
            "attributes":{
               "creationDate":"2022-02-17T07:21:54Z",
               "mfaAuthenticated":"false"
            }
         }
      },
      "eventTime":"2022-02-17T08:58:34Z",
      "eventSource":"wellarchitected.amazonaws.com",
      "eventName":"CreateLensVersion",
      "awsRegion":"us-west-2",
      "sourceIPAddress":"10.246.162.39",
      "userAgent":"aws-internal/3 aws-sdk-java/1.12.127
 Linux/5.4.156-94.273.amzn2int.x86_64 OpenJDK_64-Bit_Server_VM/25.312-b07
 java/1.8.0_312 vendor/Oracle_Corporation cfg/retry-mode/standard",
      "requestParameters":{
         "IsMajorVersion":true,
         "LensVersion":"***",
         "ClientRequestToken":"03f46163-e95c-4455-8479-266373aa09c7",
         "LensAlias":"***"
      },
      "responseElements":{
         "LensArn":"arn:aws:wellarchitected:us-
west-2:123456789012:lens/6261deecb9def44f9aecc938ca25d94e",
         "LensVersion":"***"
      },
      "requestID":"167b7051-980d-42ee-9967-0b4b3163e948",
      "eventID":"c7ef2b47-419d-45b7-8982-fbade9b558c7",
```

```
      "readOnly":false,
      "eventType":"AwsApiCall",
      "managementEvent":true,
      "recipientAccountId":"123456789012",
      "eventCategory":"Management"
   }
}
```

Révisions du document

Le tableau suivant décrit la documentation de cette version du AWS Well-Architected Tool.

- Version de l'API : dernière en date
- Dernière date de mise à jour de la documentation : 13 octobre 2025

Modification	Description	Date
Ajout de la section Révision du cadre Well-Architected (WAFR)	Ajout d'une nouvelle section contenant des instructions sur la réalisation d'une WAFR à l'aide du AWS Well-Arch itected Tool.	13 octobre 2025
Nouveau cadre	Cette version a ajouté un nouveau cadre au catalogue Lens.	17 avril 2025
Cadres nouveaux et mis à jour	Cette version a ajouté un nouveau cadre au catalogue Lens et a mis à jour un autre cadre.	27 juin 2024
Jira	Cette version a ajouté le connecteur de l'AWS Well-Architected Tool pour Jira.	16 avril 2024
Nouveaux cadres	Cette version a ajouté de nouveaux cadres au catalogue Lens.	26 mars 2024
Fonctionnalité mise à jour	Cette version ajoute la fonctionnalité de catalogue Lens à AWS WA Tool.	26 novembre 2023

Fonctionnalité mise à jour	Cette version ajoute la fonctionnalité Modèles de révision à AWS WA Tool.	3 octobre 2023
Politique gérée WellArchitectedConsoleReadOnlyAccess mise à jour	Ajout de `"wellarchitected:ExportLens"` à `WellArchitectedConsoleReadOnlyAccess` .	22 juin 2023
Fonctionnalité mise à jour	Cette version ajoute la fonctionnalité Profils à AWS WA Tool.	13 juin 2023
Fonctionnalité mise à jour	Cette version améliore l'intégration d'AWS Trusted Advisor et d'AWS Service Catalog AppRegistry, et ajoute la politique `AWSWellArchitectedDiscoveryServiceRolePolicy` aux politiques AWS gérées.	3 mai 2023
Mise à jour du contenu	La page Tableau de bord a été mise à jour pour inclure des informations détaillées sur les risques et le plan d'amélioration. La possibilité de créer un rapport consolidé sur la charge de travail a également été ajoutée.	30 mars 2023
Mise à jour du contenu	Nom corrigé de la politique WellArchitectedConsoleReadOnlyAccess.	19 janvier 2023

Mise à jour des recommandations IAM pour AWS WA Tool	Mise à jour du guide s'aligner sur les bonnes pratiques IAM. Pour de plus amples informations, veuillez consulter Bonnes pratiques de sécurité dans IAM.	4 janvier 2023
Fonctionnalité mise à jour	Cette version supprime le cadre FTR de l'outil.	14 décembre 2022
Fonctionnalité mise à jour	Cette version ajoute l'intégration d'AWS Trusted Advisor et d'AWS Service Catalog AppRegistry.	7 novembre 2022
Mise à jour du contenu	Correction d'un problème dans l'exemple JSON du cadre personnalisé pour `choices`.	29 septembre 2022
Mise à jour du contenu	La section `choices` de la spécification JSON du cadre personnalisé a été mise à jour.	2 août 2022
Fonctionnalité mise à jour	Cette version ajoute le suivi des modifications pour ses politiques gérées par AWS et ajoute une nouvelle action pour accorder l'autorisation `ListAWSServiceAccessForOrganization` à `AWSWellArchitectedOrganizationsServiceRolePolicy` .	22 juillet 2022

Partage d'organisation ajouté	Cette version ajoute la possibilité de partager des charges de travail et des cadres personnalisés avec une organisation et des unités d'organisation (UO).	30 juin 2022
Fonctionnalité mise à jour	Cette version ajoute la possibilité de spécifier des ressources supplémentaires comme choix de cadre personnalisé, de prévisualiser un cadre personnalisé avant de le publier et d'ajouter des balises aux cadres personnalisés.	21 juin 2022
Fonctionnalité mise à jour	Cette version ajoute la possibilité d'accéder à la communauté AWS Well-Architected sur AWS Re:post.	31 mai 2022
Fonctionnalité mise à jour	Cette version ajoute le pilier Durabilité et des mises à jour mineures au didacticiel.	31 mars 2022
Ajout de la prise en charge d'EventBridge	AWS WA Tool envoie désormais un événement à Amazon EventBridge lorsqu'une modification est apportée à une ressource Well-Architected.	3 mars 2022
Fonctionnalité mise à jour	Les bonnes pratiques individuelles peuvent désormais être marquées comme non applicables.	14 juillet 2021

Balisage des ressources disponible	Cette version ajoute la possibilité d'ajouter des balises aux charges de travail.	3 mars 2021
API désormais disponible	Cette version ajoute l'API AWS WA Tool. Les informations de journalisation AWS CloudTrail sont ajoutées.	16 décembre 2020
Fonctionnalité mise à jour	Cette version ajoute les cadres FTR et SaaS à l'outil.	3 décembre 2020
Protection des données mise à jour	Informations sur la protection des données mises à jour.	5 novembre 2020
Mise à jour du contenu	Il a été précisé qu'après avoir mis à niveau une charge de travail pour utiliser un nouveau cadre, vous ne pouvez pas revenir à la version précédent e.	8 juillet 2020
Mise à jour du contenu	Partage clarifié dans les Régions AWS introduites après le 20 mars 2019.	24 juin 2020
Fonctionnalité mise à jour	L'accès à un partage de charge de travail est supprimé immédiatement lorsqu'une invitation de partage de charge de travail est rejetée. L'accès partagé est accordé lorsque le partage est accepté.	17 juin 2020
Mise à jour du contenu	Ajout de la définition des problèmes à risque élevé et des problèmes à risque moyen.	12 juin 2020

Mise à jour du contenu	Une section sur la façon dont AWS utilise vos données a été ajoutée.	21 mai 2020
Fonctionnalité mise à jour	Cette version ajoute un responsable de vérification à la charge globale.	1er avril 2020
Fonctionnalité mise à jour	Cette version ajoute un lien de schéma architectural vers la charge de travail.	10 mars 2020
Mise à jour du contenu	Clarification du fait que les partages de charge de travail sont spécifiques à la Région AWS.	10 janvier 2020
Fonctionnalité mise à jour	Cette version ajoute le partage des charges de travail.	9 janvier 2020
Mise à jour du contenu	Section sécurité mise à jour avec les dernières instructions.	6 décembre 2019
Fonctionnalité mise à jour	Cette version rend les champs du secteur facultatifs lors de la définition d'une charge de travail.	19 août 2019
Fonctionnalité mise à jour	Cette version ajoute des éléments de plan d'amélior ation à la charge de travail.	29 juillet 2019
Fonctionnalité mise à jour	La version ajoute l'action DeleteWorkload à la stratégie.	18 juillet 2019
Mise à jour du contenu	Le contenu de ce guide a fait l'objet de corrections mineures.	19 juin 2019

Mise à jour du contenu	Le contenu de ce guide a fait l'objet de corrections mineures.	30 mai 2019
Fonctionnalité mise à jour	Cette version prend en charge la mise à niveau de la version du cadre utilisée pour un examen des charges de travail.	1er mai 2019
Fonctionnalité mise à jour	Cette version ajoute la possibilité de spécifier des non-Régions AWS lors de la définition d'une charge de travail.	14 février 2019
AWS Well-Architected Tool Disponibilité générale de l	Cette version présente l' AWS Well-Architected Tool.	29 novembre 2018

Glossaire AWS

Pour connaître la terminologie la plus récente d'AWS, consultez le Glossaire AWS dans la Référence Glossaire AWS.