

Guide de l'utilisateur

AWS Well-Architected Tool



AWS Well-Architected Tool: Guide de l'utilisateur

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

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

Table of Contents

.....	vii
Qu'est-ce qu'AWS Well-Architected Tool ?	1
Le framework AWS Well-Architected	2
Définitions	2
Premiers pas	4
Fournir un accès à AWS WA Tool	4
Activation des intégrations	5
Activation AppRegistry	6
Activation Trusted Advisor	6
Définition d'une charge de travail	13
Documenter une charge de travail	16
Consulter la page de charge de travail	17
Trusted Advisor chèques	18
Enregistrer un jalon	19
Didacticiel	21
Étape 1 : définir une charge de travail	21
Étape 2 : Documenter l'état de la charge de travail	22
Étape 3 : Réviser le plan d'amélioration	24
Étape 4 : Apporter des améliorations et mesurer les progrès	25
Charges de travail	27
Problèmes à risque élevé et problèmes à risque moyen	28
Définition d'une charge de travail	29
Afficher une charge de travail	30
Modification d'une charge de travail	31
Partage d'une charge de travail	31
Considérations sur le partage	34
Supprimer l'accès partagé	35
Modification de l'accès partagé	35
Acceptation et rejet des invitations à des charges de travail	36
Supprimer une charge de travail	37
Génération d'un rapport de charge de travail	38
Informations détaillées sur la charge	38
Onglet Overview (Présentation)	39
Onglet Jalestones	39

Onglet Propriétés	40
Onglet Partages	40
Cadres	42
Ajouter un objectif	42
Retrait d'un objectif	43
Détails de l'objectif	43
Onglet Overview (Présentation)	44
Onglet Plan d'amélioration	44
Onglet Partages	44
Verres personnalisés	44
Visualisation d'objectifs personnalisés	45
Création d'un objectif	46
Prévisualisation d'un objectif	47
Publier un objectif	48
Publier une mise à jour de l'objectif	48
Partage d'un objectif	50
Ajouter des tags à un objectif	52
Supprimer un objectif	52
Spécification du format de l'objectif	53
Améliorations d'objectifs	60
Sélection d'une amélioration de l'objectif	61
Mise à niveau d'un objectif	62
Catalogue d'objectifs	63
Modèles d'avis	66
Création d'un modèle d'avis	66
Modification d'un modèle d'avis	67
Partage d'un modèle d'avis	68
Définition d'une charge de travail à partir d'un modèle	69
Supprimer un modèle d'avis	70
Profils	72
Création d'un profil	72
Modification d'un profil	73
Partage d'un profil	73
Ajouter un profil à une charge de travail	74
Supprimer un profil d'une charge de travail	75
Suppression d'un profil	75

Jira	77
Configuration du connecteur	78
Configuration du connecteur	79
Synchronisation d'une charge de travail	82
Désinstallation du connecteur	82
Jalons	85
Enregistrement d'un jalon	85
Affichage des jalons	85
Génération d'un rapport de jalon	86
Partagez des invitations	87
Accepter une invitation à partager	88
Rejet d'une invitation à partager	89
Notifications	90
Notifications relatives à	90
Notifications de profil	90
Tableau de bord	92
Récapitulatif	92
Problèmes liés à Well-Architected Framework par pilier	93
Problèmes de framework Well-Architected par charge de travail	93
Problèmes liés au framework Well-Architected par élément du plan d'amélioration	94
Sécurité	96
Protection des données	97
Chiffrement au repos	98
Chiffrement en transit	98
Comment AWS utilisent vos données	98
Gestion des identités et des accès	99
Public ciblé	99
Authentification par des identités	100
Gestion des accès à l'aide de politiques	104
Comment AWS Well-Architected Tool fonctionne avec IAM	106
Exemples de politiques basées sur l'identité	114
AWS politiques gérées	121
Résolution des problèmes	127
Réponse à l'incidence	128
Validation de conformité	128
Résilience	129

Sécurité de l'infrastructure	130
Analyse de la configuration et des vulnérabilités	130
Prévention du cas de figure de l'adjoint désorienté entre services	131
Partage de vos ressources	133
Activez le partage des ressources au sein de AWS Organizations	133
Balisage de vos ressources	136
Principes de base des balises	136
Balisage de vos ressources	137
Restrictions liées aux étiquettes	138
Gestion des étiquettes à l'aide de la console	139
Ajout de balises sur une ressource individuelle lors de la création	139
Ajout et suppression de balises sur une ressource individuelle	139
Utilisation des balises à l'aide de l'API	141
Journalisation	142
AWS WA Toolinformations dans CloudTrail	142
Présentation des AWS WA Tool entrées des fichiers journaux	143
EventBridge	146
Exemples d'événements àAWS WA Tool	147
Historique de la documentation	151
Glossaire AWS	158

Nous avons publié une nouvelle version du Well-Architected Framework. Nous avons également ajouté de nouveaux objectifs et des objectifs mis à jour au [catalogue](#) d'objectifs. [Apprenez-en davantage](#) sur les modifications.

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.

Qu'est-ce qu'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 Toolvous aide tout au long du cycle de vie du produit en :

- 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 Advisor](#)et [AWS Service Catalog AppRegistry](#)aide à découvrir plus facilement les informations nécessaires pour répondre aux questions de révision de Well-Architected.

Ce service est destiné aux personnes impliquées dans le développement de produits techniques, telles que les directeurs technologiques (CTO), les architectes, les développeurs et les membres de l'équipe opérationnelle. AWSles 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

- [Le framework AWS Well-Architected](#)

- [Définitions](#)

Le framework AWS Well-Architected

Le [AWSWell-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 [AWSWell-Architected](#).

Définitions

Dans AWS WA Tool et dans le cadre AWS Well-Architected :

- 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 et 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 (HRI) sont des choix architecturaux et opérationnels dont on a constaté qu'ils pouvaient 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 (IRM) sont des choix architecturaux et opérationnels susceptibles d'avoir un impact négatif sur les entreprises, mais dans une moindre mesure que les IRH. AWS

Pour plus d'informations, consultez [Problèmes à risque élevé et problèmes à risque moyen](#).

Commencer avec AWS Well-Architected Tool

Cette section décrit comment démarrer avec AWS WA Tool.

Rubriques

- [Fournir aux utilisateurs, aux groupes ou aux rôles l'accès à AWS WA Tool](#)
- [Activation du support pour d'autres AWS services](#)
- [Définition d'une charge de travail](#)
- [Documenter une charge de travail](#)
- [Enregistrer un jalon](#)

Fournir aux utilisateurs, aux groupes ou aux rôles l'accès à AWS WA Tool

Au cours de cette étape, vous accordez l'accès à AWS WA Tool.

Fournir un accès à 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. Pour plus d'informations, voir la rubrique [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) du Guide de l'utilisateur IAM.

- Utilisateurs IAM :

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

- (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique [Ajout d'autorisations à un utilisateur \(console\)](#) du Guide de l'utilisateur IAM.

2. Pour accorder un contrôle total, appliquez la politique `WellArchitectedConsoleFullAccess` gérée à l'ensemble d'autorisations ou au rôle.

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

3. Pour accorder un accès en lecture seule, appliquez la politique `WellArchitectedConsoleReadOnlyAccess` gérée à l'ensemble d'autorisations ou au rôle. Les directeurs dotés de ce rôle ne peuvent consulter que les ressources.

Pour plus d'informations sur ces politiques, consultez [AWS politiques gérées pour AWS Well-Architected Tool](#).

Activation du support pour d'autres AWS services

L'activation de l'accès AWS WA Tool à l'organisation permet de recueillir des informations sur la structure de votre organisation afin de partager les ressources plus facilement (voir [the section called "Activez le partage des ressources au sein de AWS Organizations"](#) pour plus d'informations). L'activation du support Discovery permet de recueillir des informations provenant de [AWS Trusted Advisor](#) ressources connexes (telles que les AWS CloudFormation piles dans les collections de AppRegistry ressources) afin de vous aider à découvrir plus facilement les informations nécessaires pour répondre aux questions de révision de Well-Architected et à adapter les contrôles à une charge de travail. [AWS Service Catalog AppRegistry](#) Trusted Advisor

L'activation de l' AWS Organizations assistance ou de l'activation de l'assistance Discovery crée automatiquement un rôle lié au service pour votre compte.

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

1. Pour recueillir des informations auprès de AWS Organizations, activez Activer le AWS Organizations support.
2. Activez le support Activate Discovery pour recueillir des informations auprès d'autres AWS services et ressources.
3. Sélectionnez Afficher les autorisations de rôle pour afficher les autorisations de rôle liées au service ou les politiques relatives aux relations de confiance.

4. Sélectionnez Enregistrer les paramètres.

Activation AppRegistry pour une charge de travail

L'utilisation AppRegistry est facultative, et les clients du support aux AWS entreprises et aux entreprises peuvent l'activer pour chaque charge de travail.

Chaque fois que le support Discovery est activé et associé à une charge de travail nouvelle ou existante, un groupe d'attributs géré par le service AppRegistry est AWS WA Tool créé. Le groupe d'attributs Metadata in 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 le support Discovery est activé, chaque fois que la charge de travail est modifiée, le groupe d'attributs est mis à jour.
- Lorsque le support Discovery est désactivé ou que l'application est supprimée de la charge de travail, les informations de charge de travail sont supprimées de AWS Service Catalog.

Si vous souhaitez qu'une AppRegistry application gère les données extraites Trusted Advisor, définissez la définition de la ressource de charge de travail sur AppRegistry sur Tout. Créez des rôles pour tous les comptes qui possèdent des ressources dans votre application en suivant les instructions de [the section called "Activation Trusted Advisor dans IAM"](#).

Activation AWS Trusted Advisor pour une charge de travail

L'intégration avec AWS Trusted Advisor est facultative et peut être activée au cas par charge de travail pour les clients AWS Business et Enterprise Support. L'intégration est gratuite AWS WA Tool, mais pour plus Trusted Advisor de détails sur les Trusted Advisor tarifs, consultez la section [Plans de AWS support](#).

Pour activer Trusted Advisor pour une charge de travail

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

4. Une notification indiquant que le rôle de service IAM sera créé s'affiche la première fois qu' Trusted Advisor il est activé pour une charge de travail. Si vous choisissez Afficher les autorisations, les autorisations du rôle IAM s'affichent. Vous pouvez consulter le nom du rôle, ainsi que les autorisations et les relations de confiance que le JSON a automatiquement créées pour vous dans IAM. Une fois le rôle créé, pour l'activation des charges de travail suivantes Trusted Advisor, seule la notification indiquant qu'une configuration supplémentaire est nécessaire est affichée.
5. Dans le menu déroulant Définition des ressources, vous pouvez sélectionner Métadonnées de charge de travail ou Toutes. AppRegistry La sélection de définition des ressources définit les données à partir desquelles les données AWS WA Tool sont extraites Trusted Advisor afin de vérifier le statut lors de l'examen de la charge de travail conformément aux meilleures pratiques de Well-Architected.

Métadonnées de charge de travail : la charge de travail est définie par des identifiants de compte et Régions AWS spécifiée dans la charge de travail.

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

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

6. Choisissez Suivant.
7. Appliquez le AWS Well-Architected Framework à votre charge de travail et choisissez Define workload. Trusted Advisor les chèques sont uniquement liés au AWS Well-Architected Framework, et non à d'autres objectifs.

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

Pour plus d'informations sur la création d'un rôle dans AWS Identity and Access Management (IAM), consultez la section [Création d'un rôle pour un AWS service \(console\)](#) dans le guide de l'utilisateur IAM.

Activation Trusted Advisor pour une charge de travail dans IAM

Note

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

Les propriétaires des comptes associés aux charges de travail activées Trusted Advisor doivent créer un rôle dans IAM pour consulter les Trusted Advisor informations. AWS WA Tool

Pour créer un rôle dans IAM afin d' AWS WA Tool obtenir des informations auprès de Trusted Advisor

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à <https://console.aws.amazon.com/iam/> l'adresse.
2. Dans le volet de navigation de la console IAM, choisissez Roles, puis Create role.
3. Sous Type d'entité fiable, sélectionnez Politique de confiance personnalisée.
4. Copiez et collez la politique de confiance 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 la charge de travail, puis choisissez Next.

```
{
  "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:*:WORKLOAD_OWNER_ACCOUNT_ID:workload/*"
    }
  }
}
]
}

```

Note

Le `aws:sourceArn` bloc de conditions de la politique de confiance personnalisée précédente

est `arn:aws:wellarchitected:*:WORKLOAD_OWNER_ACCOUNT_ID:workload/*`, qui est une condition générique indiquant que ce rôle peut être utilisé AWS WA Tool pour toutes les charges de travail du propriétaire de la charge de travail. Toutefois, l'accès peut être limité à un ARN de charge de travail spécifique ou à un ensemble d'ARN de charge de travail. Pour spécifier plusieurs ARN, consultez l'exemple de politique de confiance suivant.

```

{
  "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:REGION:WORKLOAD_OWNER_ACCOUNT_ID:workload/WORKLOAD_ID_1",

```



```

"arn:aws:wellarchitected:REGION:WORKLOAD_OWNER_ACCOUNT_ID:workload/
WORKLOAD_ID_2"
    ]
  }
}
]
}

```

5. Sur la page Ajouter des autorisations, pour les politiques d'autorisations, choisissez Créer une politique pour autoriser AWS WA Tool l'accès à la lecture des données 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 intégrée après avoir créé le rôle. Choisissez Afficher le rôle dans le message de création de rôle réussie, puis sélectionnez Créer une politique intégrée dans le menu déroulant Ajouter des autorisations de l'onglet Autorisations.

6. Copiez et collez la politique d'autorisations suivante dans le champ JSON. Dans l'ResourceARN, remplacez-le *YOUR_ACCOUNT_ID* par votre propre identifiant de compte, spécifiez la région ou un astérisque (*), puis choisissez Next:Tags.

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

```

{
  "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:*:YOUR_ACCOUNT_ID:checks/*"
    ]
}
]
}

```

7. S'il Trusted Advisor est activé pour une charge de travail et que la définition des ressources est définie sur AppRegistry sur Tout, tous les comptes qui possèdent une ressource dans l'AppRegistry application attachée à la charge de travail doivent ajouter l'autorisation suivante à la politique d'autorisations de leur Trusted Advisor rôle.

```

{
  "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. Passez en revue la politique, donnez-lui un nom, puis 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 Create role. Remplacez *WORKLOAD_OWNER_ACCOUNT_ID* par l'ID de compte du propriétaire de la charge de travail.

Vous devriez recevoir un message de confirmation en haut de la page vous informant que le rôle a été créé.

12. Pour consulter le rôle et la politique d'autorisation associée, dans le volet de navigation de gauche, sous Gestion des accès, sélectionnez Rôles et recherchez le `WellArchitectedRoleForTrustedAdvisor-WORKLOAD_OWNER_ACCOUNT_ID` nom. Sélectionnez le nom du rôle pour vérifier que les autorisations et les relations de confiance sont correctes.

Désactivation Trusted Advisor pour une charge de travail

Pour désactiver Trusted Advisor pour une charge de travail

Vous pouvez la désactiver Trusted Advisor pour n'importe quelle charge de travail depuis le AWS WA 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 Trusted Advisor depuis le AWS WA Tool ne supprime pas les rôles créés dans IAM. La suppression de rôles dans IAM nécessite une mesure de nettoyage distincte. Les propriétaires de charges de travail ou de comptes associés doivent supprimer les rôles IAM créés lors Trusted Advisor de leur désactivation dans AWS WA Tool, ou pour arrêter AWS WA Tool de collecter des Trusted Advisor données pour la charge de travail.

Pour supprimer le **WellArchitectedRoleForTrustedAdvisor** dans IAM

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à <https://console.aws.amazon.com/iam/> l'adresse.
2. Dans le volet de navigation de la console IAM, sélectionnez Rôles.
3. Recherchez `WellArchitectedRoleForTrustedAdvisor-WORKLOAD_OWNER_ACCOUNT_ID` et sélectionnez le nom du rôle.
4. Sélectionnez Delete (Supprimer). Dans la fenêtre contextuelle, tapez 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 la section [Suppression d'un rôle IAM \(console\)](#) dans le guide de l'utilisateur IAM.

Définition d'une charge de travail

L'étape suivante consiste à définir 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/](https://console.aws.amazon.com/wellarchitected/).
2. Si c'est la première fois que vous l'utilisez AWS WA Tool, une page vous présentant les fonctionnalités du service s'affiche. 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 de détails sur l' AWS utilisation de vos données de charge de travail, choisissez Pourquoi avez-vous AWS 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 Review owner (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.
 - Préproduction — La charge de travail s'exécute dans un environnement de pré-production.
7. Dans la section Regions (Régions), choisissez les régions pour votre charge de travail :
 - Régions AWS— Choisissez l' Régions AWS endroit où s'exécute votre charge de travail, un par un.

- AWS Non-régions : entrez les noms des régions situées en dehors de celles AWS où s'exécute votre charge de travail. 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 le champ Identifiants de compte, entrez les identifiants Comptes AWS associés à votre charge de travail. Vous pouvez spécifier jusqu'à 100 ID de comptes uniques, séparés par des virgules.

S'il Trusted Advisor est activé, tous les identifiants de compte spécifiés sont utilisés pour obtenir des données Trusted Advisor. Consultez la section [Activation d'une charge de travail AWS Trusted Advisor pour](#) accorder AWS WA Tool des autorisations permettant d'obtenir Trusted Advisor des données en votre nom au sein d'IAM.

9. (Facultatif) Dans le champ Application, entrez l'ARN de l'application [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 Architectural design (Conception architecturale) saisissez l'URL de votre conception architecturale.
11. (Facultatif) Dans la zone Industry type (Type de secteur d'activité) choisissez le type de secteur associé à votre charge de travail.
12. (Facultatif) Dans la zone Industry (Secteur d'activité), choisissez le secteur qui correspond le mieux à votre charge de travail.
13. (Facultatif) Dans la Trusted Advisor section, pour activer les Trusted Advisor vérifications relatives à 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 Trusted Advisor"](#) pour accorder AWS WA Tool les autorisations nécessaires pour obtenir Trusted Advisor des données en votre nom. Sélectionnez Métadonnées de charge de travail ou Tout sous Définition des ressources pour définir les ressources AWS WA Tool utilisées pour exécuter Trusted Advisor les vérifications. AppRegistry
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 [AWS Well-Architected Tool Connector for Jira](#) pour commencer à configurer et configurer le connecteur. Sélectionnez Ne pas synchroniser la charge de travail, Synchroniser la charge de travail - Manuel et Synchroniser la charge de

travail - Automatique, et entrez éventuellement une clé de projet Jira avec laquelle 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 les descriptions des AWS objectifs officiels, voir [Objectifs](#).

Les objectifs peuvent être sélectionnés parmi les [objectifs personnalisés](#) (objectifs que vous avez créés ou partagés avec vous Compte AWS), le [catalogue d'objectifs](#) (objectifs AWS officiels 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 verres personnalisés créés par un autre AWS utilisateur ou compte, vous reconnaissez que les verres personnalisés créés par d'autres

utilisateurs et partagés avec vous constituent du contenu tiers tel que défini dans le contrat AWS client.

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.

Documenter une charge de travail

Une fois qu'une charge de travail a été définie, vous documentez son état.

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 de révision de charge prioritaires que vous pouvez utiliser pour accélérer le processus de révision 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 obtenir des instructions supplémentaires, choisissez Info 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 obtenir des instructions supplémentaires sur n'importe quel élément, choisissez Info et consultez les informations dans le volet d'aide.

- b. (Facultatif) Si une ou plusieurs bonnes pratiques ne s'appliquent pas à votre charge de travail, choisissez Marquer les meilleures 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.

Pour revenir aux questions, accédez à la page des détails de la charge de travail et choisissez Continue reviewing (Continuer la vérification).

Consulter la page de charge de travail

La page de révision de la charge de travail comporte trois volets.

1. Le volet de navigation de gauche affiche les questions relatives à chaque pilier. Les questions auxquelles vous avez répondu sont marquées Terminées. 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, AWS WA Tool utilise les informations qu'il contient pour déterminer les questions prioritaires de l'examen de la charge de travail et celles qui ne s'appliquent pas à votre entreprise. Dans le volet de navigation de gauche, vous pouvez utiliser les questions prioritaires pour accélérer le processus de révision de la charge de

travail. Une icône de notification apparaît à côté des questions récemment ajoutées à la liste des questions prioritaires.

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 Ask an expert pour accéder à la communauté AWS Re:post dédiée à Well-Architected AWS](#) . AWS Re:post est un substitut question-and-answer communautaire basé sur des sujets pour 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 meilleures pratiques comme non applicables, choisissez Marquer les meilleures pratiques qui ne s'appliquent pas à cette charge de travail et sélectionnez-les.

Utilisez les boutons situés au bas de ce volet pour passer à la question suivante, revenir à la question précédente ou enregistrer vos modifications et quitter.

3. Le volet d'aide de droite affiche des informations supplémentaires et des ressources utiles. [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.

Trusted Advisor chèques

Si cette Trusted Advisor option est activée pour votre charge de travail, un onglet de Trusted Advisor vérification s'affiche à côté de Question. Si des vérifications sont disponibles pour la meilleure pratique, une notification indiquant que des Trusted Advisor vérifications sont disponibles s'affiche après la sélection de la question. Si vous sélectionnez Afficher les chèques, vous accédez à l'onglet Trusted Advisor Contrôles.

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

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

- Action recommandée (rouge) : Trusted Advisor recommande une action pour le contrôle.
- Enquête recommandée (jaune) : Trusted Advisor détecte un éventuel problème lors de la vérification.
- Aucun problème détecté (vert) : Trusted Advisor ne détecte aucun problème lors de 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 chèques proposés Trusted Advisor , voir [Afficher les catégories de chèques](#) dans le guide de AWS Support l'utilisateur.

La sélection du lien Info situé à côté de chaque Trusted Advisor vérification permet d'afficher les informations relatives à la vérification dans le volet des ressources d'aide. Pour plus d'informations, [AWS Trusted Advisor consultez la référence](#) dans le guide de AWS Support l'utilisateur.

Enregistrer un jalon

Vous pouvez enregistrer un jalon 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 est enregistré, vous ne pouvez pas modifier les données de la charge de travail qui ont été capturées dans ce jalon.

Pour plus d'informations, voir [Jalons](#).

Didacticiel

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](#)
- [Étape 2 : Documenter l'état de la charge de travail](#)
- [Étape 3 : Réviser le plan d'amélioration](#)
- [Étape 4 : Apporter des améliorations et mesurer les progrès](#)

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, consultez [the 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/](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 AWS, puis 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 case Identifiants de compte est facultative. N'en associez aucune Comptes AWS à cette charge de travail.
9. La case Application est facultative. N'entrez pas d'ARN d'application 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 Enregistrer.
4. Pour générer un rapport de charge de travail, sélectionnez le cadre souhaité et choisissez Generate report (Générer un rapport). Un fichier PDF 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, procédez comme suit :

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, procédez comme suit :

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.

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 de backend.

Une charge de travail peut consister en un sous-ensemble de ressources en une seule Compte AWS ou en un ensemble de plusieurs ressources réparties sur 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.

Propriétaire

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

AWS Well-Architected Tool Les problèmes à haut risque (HRI) identifiés dans le cadre des choix architecturaux et opérationnels identifiés peuvent avoir un impact négatif important sur une entreprise. AWS 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 meilleures pratiques correspondantes sont largement appliquées par AWS les AWS clients. Ces meilleures pratiques sont les directives définies par le AWS Well-Architected Framework et les lentilles.

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 d'appliquer une bonne pratique à la

charge de travail, le risque peut être inférieur à celui indiqué. AWS suggère aux clients de documenter ces raisons, ainsi que leur incidence sur les meilleures pratiques, dans les notes relatives à la charge de travail. Pour toutes les IRH et IRM identifiées, AWS suggère aux clients de mettre en œuvre les meilleures pratiques telles que définies dans le 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 meilleure pratique, AWS suggère qu'ils documentent l'approbation applicable au niveau de l'entreprise et les raisons pour lesquelles ils ne l'ont pas mise en œuvre.

Définition d'une charge de travail

Il existe deux manières de définir une charge de travail. Sur la page Charges de travail, AWS WA Tool vous pouvez définir une charge de travail sans modèle. Sur la page Modèles de révision, vous pouvez également utiliser un modèle de révision 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. Sélectionnez Workloads dans le volet de navigation de gauche.
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 de révision et que vous souhaitez définir une charge de travail à partir de celui-ci, choisissez Définir à partir du modèle de révision.
4. Suivez les instructions [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 lentilles.

Pour définir une charge de travail à partir de la page Modèles de révision

1. Sélectionnez Réviser les modèles dans le volet de navigation de gauche.
2. Sélectionnez le nom d'un modèle d'évaluation existant ou suivez les instructions [the section called “Création d'un modèle d'avis”](#) pour créer un nouveau modèle de révision.
3. Choisissez Définir la charge de travail à partir du modèle.
4. Suivez les instructions [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 de révision.

Afficher une charge de travail

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 Well-Architected Tool console AWS Management Console et ouvrez-la 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

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 Well-Architected Tool console AWS Management Console et ouvrez-la à l'[adresse https://console.aws.amazon.com/wellarchitected/](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](#).

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 Trusted Advisor activées doivent créer un rôle dans IAM. Pour plus de détails, consultez [the section called "Activation 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

Vous pouvez partager une charge de travail qui vous appartient avec d'autres utilisateursComptes AWS, une organisation et des unités organisationnelles (UO) au sein de la même organisationRégion AWS.

Note

Vous ne pouvez partager des charges de travail qu'au sein d'une même Région AWS entité.

Lorsque vous partagez une charge de travail avec une autre personne Compte AWS, si le destinataire n'a pas l'`wellarchitected:UpdateShareInvitation` autorisation, il ne peut pas accepter l'invitation de partage. Consultez [the section called “Fournir un accès à AWS WA Tool”](#) des exemples de politiques d'autorisation.

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

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/](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 pour les utilisateurs ou les comptes pour créer une invitation à une charge de travail.
5. Entrez l'Compte AWSID 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 Create pour envoyer une invitation de charge de travail à l'utilisateur 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 lui ont Compte AWS tous deux reçu des invitations à une charge de travail, l'invitation à une charge de travail dotée du 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 AWS Organizations l'accès](#).

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

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/](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 Create and Create shares to Organizations.
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 d'organisation.
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 Create pour partager la charge de travail.

Pour savoir qui a un accès partagé à une charge de travail, choisissez Shares (Partages) dans la page [Informations détaillées sur la charge](#).

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

Vous pouvez également partager des objectifs personnalisés que vous possédez avec d'autres utilisateurs Comptes AWS, votre organisation et des unités d'organisation dans le même cadre Région AWS. Pour plus de détails, reportez-vous à [Partage d'un objectif personnalisé](#).

Considérations sur le partage

Une charge de travail peut être partagée avec un maximum de 20 utilisateurs Comptes AWS et utilisateurs différents. Une charge de travail ne peut être partagée qu'avec des comptes et des utilisateurs identiques à Région AWS la charge de travail.

Pour partager une charge de travail dans une région introduite après le 20 mars 2019, vous et le partage Compte AWS devez activer la région dans leAWS Management Console. Pour plus d'informations, reportez-vous à la section [Infrastructure AWS mondiale](#).

Vous pouvez partager une charge de travail avec un Compte AWS utilisateur individuel d'un compte, ou les deux. Lorsque vous partagez une charge de travail avec unCompte 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 meilleure pratique qui consiste à accorder le moindre privilège et à partager la charge de travail individuellement avec ces utilisateurs.

Si un utilisateur Compte AWS et un utilisateur du compte sont invités à la charge de travail, l'invitation à la charge de travail avec les autorisations de niveau le plus élevé détermine l'autorisation de l'utilisateur sur la charge de travail. Si vous supprimez l'invitation de charge de travail pour l'utilisateur, l'accès de l'utilisateur est déterminé par l'invitation de charge de travail pourCompte 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 AWS Organizations l'accès.

Si vous partagez une charge de travail à la fois avec une organisation et une ou plusieurs unités d'organisation, l'invitation à la charge de travail avec les autorisations les plus élevées détermine l'autorisation du compte sur la charge de travail.

Pour activer AWS Organizations le partage

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/](https://console.aws.amazon.com/wellarchitected/).
2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Choisissez Activer AWS Organizations le support.
4. Choisissez Save settings (Enregistrer les paramètres).

Supprimer l'accès partagé

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 Well-Architected Tool console AWS Management Console et ouvrez-la à l'[adresse https://console.aws.amazon.com/wellarchitected/](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 lui-même Compte AWS ont reçu des invitations à une charge de travail, vous devez supprimer les deux invitations à une charge de travail pour retirer à l'utilisateur l'autorisation d'accéder à la charge de travail.

Modification de l'accès partagé

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 Well-Architected Tool console AWS Management Console et ouvrez-la à l'[adresse https://console.aws.amazon.com/wellarchitected/](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 à l'utilisateur Compte AWS or.

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 Save (Enregistrer).

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

Acceptation et rejet des invitations à des charges de travail

Une invitation à une charge de travail est une demande de partage d'une charge de travail appartenant à une autre personneCompte 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 ne peuvent être partagées qu'au sein d'un même Région AWS organisme.

Pour accepter ou rejeter une invitation de 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/](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 [Informations détaillées sur la charge](#) correspondant à la charge de travail.

Supprimer une charge de travail

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 Well-Architected Tool console AWS Management Console et ouvrez-la à l'[adresse https://console.aws.amazon.com/wellarchitected/](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

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 sont affichés 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 Well-Architected Tool console AWS Management Console et ouvrez-la à l'[adresse https://console.aws.amazon.com/wellarchitected/](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.

Informations détaillées sur la charge

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 Overview \(Présentation\)](#)
- [Onglet Jalestones](#)
- [Onglet Propriétés](#)
- [Onglet Partages](#)

Onglet Overview (Présentation)

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 Jalestones

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 :

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

Onglet Propriétés

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](#).

Onglet Partages

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 sont affichées pour chaque utilisateur Compte AWS disposant d'un accès partagé à la charge de travail :

Principal

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

État

Statut de l'invitation de charge de travail.

- En suspens

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.

Autorisation

L'autorisation accordée à l'utilisateur Compte AWS or.

- 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 utilisateur Compte AWS ou avec un autre utilisateur Région AWS, choisissez Create. Une charge de travail peut être partagée avec un maximum de 20 utilisateurs 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).

Cadres

Les cadres vous permettent d'évaluer continuellement vos architectures par rapport aux bonnes pratiques et d'identifier les points à améliorer. L'objectif AWS Well-Architected Framework 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 d'objectifs peuvent être appliqués à vos charges de travail : les objectifs Lens Catalog et les objectifs personnalisés.

- [Catalogue](#) d'objectifs : objectifs officiels créés et maintenus par AWS. Le catalogue d'objectifs est accessible à tous les utilisateurs et ne nécessite aucune installation supplémentaire pour être utilisé.
- [Objectifs personnalisés : objectifs](#) définis par l'utilisateur qui ne sont pas du contenu AWS officiel. Vous pouvez [créer des verres personnalisés](#) avec vos propres piliers, questions, meilleures pratiques et plans d'amélioration, ainsi que [partager des verres personnalisés](#) avec d'autres Comptes AWS.

Cinq lentilles peuvent être ajoutées à la fois à une charge de travail, avec un maximum de 20 lentilles appliquées 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.

Ajouter un objectif à une charge de travail

Pour ajouter un cadre à 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/](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 l'objectif à ajouter, puis cliquez sur Enregistrer.

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

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

Pour plus d'informations sur le catalogue d'AWS objectifs, rendez-vous sur [AWS Well-Architected Lenses](#). Notez que tous les livres blancs sur les objectifs ne sont pas fournis sous forme d'objectifs dans le catalogue d'objectifs.

Exclusion de responsabilité

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

Supprimer un objectif d'une charge de travail

Pour supprimer un cadre d'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/](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 l'objectif que vous souhaitez supprimer et choisissez Enregistrer.

L'objectif AWS Well-Architected Framework ne peut pas être retiré 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.

Détails de l'objectif

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 objectif personnalisé, l'onglet Shares fournit une liste des principaux IAM avec lesquels l'objectif a été partagé.

Verres personnalisés

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

Vous pouvez adapter les questions dans une perspective personnalisée pour qu'elles soient spécifiques à une technologie particulière, vous aider à répondre aux besoins de gouvernance au sein de votre organisation ou étendre les conseils fournis par le Well-Architected Framework et les lentilles. AWS À l'instar des objectifs existants, vous pouvez suivre les progrès au fil du temps en créant des jalons, et fournir un état périodique en générant des rapports.

Rubriques

- [Visualisation d'objectifs personnalisés](#)
- [Création d'un objectif personnalisé](#)
- [Prévisualisation d'un objectif personnalisé](#)
- [Publier un objectif personnalisé pour la première fois](#)

- [Publication d'une mise à jour sur un objectif personnalisé](#)
- [Partage d'un objectif personnalisé](#)
- [Ajouter des tags à un objectif personnalisé](#)
- [Supprimer un objectif personnalisé](#)
- [Spécification du format de l'objectif](#)

Visualisation d'objectifs personnalisés

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

Pour visualiser un objectif

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/](https://console.aws.amazon.com/wellarchitected/).
2. Dans le volet de navigation de gauche, choisissez Verres personnalisés.

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.

3. Choisissez les verres personnalisés que vous souhaitez voir :
 - Possédé par moi — Affiche les verres personnalisés que vous avez créés.
 - Partagé avec moi — Affiche les verres personnalisés qui ont été partagés avec vous.
4. Sélectionnez l'objectif personnalisé à visualiser de l'une des manières suivantes :
 - Choisissez le nom de l'objectif.
 - Sélectionnez l'objectif et choisissez Afficher les détails.

La [Détails de l'objectif](#) page s'affiche.

La page Objectifs personnalisés contient les champs suivants :

Nom

Le nom de l'objectif.

Propriétaire

L' Compte AWS identifiant propriétaire de l'objectif personnalisé.

Statut

Le statut PUBLISHED signifie que l'objectif personnalisé a été publié et peut être appliqué à des charges de travail ou partagé avec d'autres Comptes AWS.

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

Version

Le nom de version de l'objectif personnalisé.

Dernière mise à jour

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

Création d'un objectif personnalisé

Pour créer un objectif personnalisé

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/](https://console.aws.amazon.com/wellarchitected/).
2. Dans le volet de navigation de gauche, choisissez Verres personnalisés.
3. Choisissez Créer un objectif personnalisé.
4. Choisissez Télécharger le fichier pour télécharger le fichier modèle JSON.
5. Ouvrez le fichier modèle JSON avec votre éditeur de texte préféré et ajoutez les données pour votre objectif personnalisé. Ces données incluent vos piliers, vos questions, vos meilleures pratiques et les liens vers les plans d'amélioration.

Pour plus d'informations, consultez [Spécification du format de l'objectif](#). La taille d'un objectif personnalisé ne peut pas dépasser 500 Ko.

6. Choisissez Choisir un fichier pour sélectionner votre fichier JSON.
7. (Facultatif) Dans la section Tags, ajoutez les tags que vous souhaitez associer à l'objectif personnalisé.

8. Choisissez Soumettre et prévisualiser pour prévisualiser l'objectif personnalisé, ou Soumettre pour soumettre l'objectif personnalisé sans prévisualisation.

Si vous choisissez d'envoyer et de prévisualiser votre objectif personnalisé, vous pouvez sélectionner Suivant pour naviguer dans l'aperçu de l'objectif, ou sélectionner Quitter l'aperçu pour revenir aux objectifs personnalisés.

Si la validation échoue, modifiez votre fichier JSON et réessayez de créer l'objectif personnalisé.

Après avoir AWS WA Tool validé votre fichier JSON, votre objectif personnalisé est affiché dans Objectifs personnalisés.

Une fois qu'un objectif personnalisé a été créé, il passe au statut DRAFT. Vous devez [publier l'objectif](#) avant de l'appliquer à des charges de travail ou de le partager avec d'autres Comptes AWS.

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

Exclusion de responsabilité

N'incluez ni ne collectez d'informations personnelles identifiables (PII) d'utilisateurs finaux ou d'autres personnes identifiables dans ou via vos lentilles personnalisées. Si votre objectif personnalisé ou ceux partagés avec vous et utilisés dans votre compte incluent ou collectent des informations personnelles, vous devez : vous assurer que les informations personnelles 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 objectif personnalisé

Pour prévisualiser un objectif personnalisé

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/](https://console.aws.amazon.com/wellarchitected/).
2. Dans le volet de navigation de gauche, choisissez Verres personnalisés.
3. Seuls les objectifs en état DRAFT peuvent être prévisualisés. Sélectionnez l'objectif personnalisé DRAFT souhaité et choisissez Preview experience.
4. Choisissez Next pour naviguer dans l'aperçu de l'objectif.

5. (Facultatif) Vous pouvez revoir votre plan d'amélioration en sélectionnant les meilleures pratiques pour chaque question de l'aperçu, puis en choisissant Mettre à jour en fonction des 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 Exit Preview pour revenir à l'objectif personnalisé.

Note

Vous pouvez également prévisualiser un objectif personnalisé en sélectionnant Soumettre et prévisualiser lors de [la création d'un objectif personnalisé](#).

Publier un objectif personnalisé pour la première fois

Pour publier un objectif personnalisé

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/](https://console.aws.amazon.com/wellarchitected/).
2. Dans le volet de navigation de gauche, choisissez Verres personnalisés.
3. Sélectionnez l'objectif personnalisé souhaité, puis choisissez Publier l'objectif.
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 un objectif personnalisé.

Une fois qu'un objectif personnalisé a été publié, il passe à l'état PUBLIÉ.

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

Publication d'une mise à jour sur un objectif personnalisé

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

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/](https://console.aws.amazon.com/wellarchitected/).

2. Dans le volet de navigation de gauche, choisissez Verres personnalisés.
3. Sélectionnez l'objectif personnalisé souhaité et choisissez Modifier.
4. Si aucun fichier JSON mis à jour n'est prêt, choisissez Télécharger le fichier pour télécharger une copie de l'objectif personnalisé actuel. Modifiez le fichier JSON téléchargé avec 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 l'objectif personnalisé, ou Soumettre pour soumettre l'objectif personnalisé sans prévisualisation.

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

Après avoir AWS WA Tool validé votre fichier JSON, votre objectif personnalisé est affiché dans Objectifs personnalisés au statut DRAFT.

6. Sélectionnez à nouveau l'objectif personnalisé et choisissez Publier l'objectif.
7. Choisissez Vérifier les modifications avant de publier pour vérifier que les modifications apportées à votre objectif personnalisé sont correctes. Cela inclut la validation des éléments suivants :
 - Le nom de l'objectif personnalisé
 - Les noms des piliers
 - Les nouvelles questions, les questions mises à jour et les questions supprimées

Choisissez Suivant.

8. Spécifiez le type de changement de version.

Version majeure

Indique que des modifications importantes ont été apportées à l'objectif. À utiliser pour les modifications qui ont un impact sur la signification de l'objectif personnalisé.

Toute charge de travail associée à l'objectif sera informée qu'une nouvelle version de l'objectif personnalisé est disponible.

Les modifications de version majeures ne sont pas automatiquement appliquées aux charges de travail utilisant l'objectif.

Version mineure

Indique que des modifications mineures ont été apportées à l'objectif. À utiliser pour de petites modifications, telles que des modifications de texte ou des mises à jour des liens URL.

Les modifications de version mineures sont automatiquement appliquées aux charges de travail à l'aide de l'objectif 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 un objectif personnalisé.

Une fois qu'un objectif personnalisé a été publié, il passe à l'état PUBLIÉ.

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

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

Les mises à jour des versions mineures sont automatiquement appliquées sans aucune notification.

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

Partage d'un objectif personnalisé

Vous pouvez partager un objectif personnalisé avec Comptes AWS d'autres utilisateurs et unités organisationnelles (UO). AWS Organizations


Pour partager un objectif personnalisé avec Comptes AWS d'autres utilisateurs

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/](https://console.aws.amazon.com/wellarchitected/).
2. Dans le volet de navigation de gauche, choisissez Verres personnalisés.
3. Sélectionnez l'objectif personnalisé à partager, puis choisissez Afficher les détails.

4. Sur la [Détails de l'objectif](#) page, choisissez Shares. Choisissez ensuite Créer et créer des partages pour les utilisateurs ou les comptes pour créer une invitation au partage d'objectifs.
5. Entrez l' Compte AWS identifiant à 12 chiffres ou l'ARN de l'utilisateur avec lequel vous souhaitez partager l'objectif personnalisé.
6. Choisissez Créer pour envoyer une invitation au partage d'objectifs à l'utilisateur Compte AWS ou à l'utilisateur spécifié.

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

Si l'invitation au partage d'objectifs n'est pas acceptée dans les sept jours, elle expire automatiquement.

 Important

Avant de partager un objectif personnalisé avec une organisation ou des unités organisationnelles (UO), vous devez [activer AWS Organizations l'accès](#).

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

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/](https://console.aws.amazon.com/wellarchitected/).
2. Dans le volet de navigation de gauche, choisissez Verres personnalisés.
3. Sélectionnez l'objectif personnalisé à partager.
4. Sur la [Détails de l'objectif](#) page, choisissez Shares. Choisissez ensuite Create and Create shares to Organizations.
5. Sur la page Créer un partage d'objectif personnalisé, choisissez d'accorder des autorisations à l'ensemble de l'organisation ou à une ou plusieurs unités d'organisation.
6. Choisissez Créer pour partager l'objectif personnalisé.

Pour savoir qui a partagé l'accès à un objectif personnalisé, choisissez Shares [Détails de l'objectif](#) sur la page.

Exclusion de responsabilité

En partageant vos verres personnalisés avec d'autres personnes Comptes AWS, vous reconnaissez qu'ils AWS seront mis à la disposition de ces autres comptes. Ces autres comptes peuvent continuer à accéder à vos verres personnalisés partagés et à les utiliser même si vous supprimez les verres personnalisés des vôtres Compte AWS ou si vous résiliez les vôtres Compte AWS.

Ajouter des tags à un objectif personnalisé

Pour ajouter des balises à un objectif personnalisé

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/](https://console.aws.amazon.com/wellarchitected/).
2. Dans le volet de navigation de gauche, choisissez Verres personnalisés.
3. Sélectionnez l'objectif personnalisé que vous souhaitez mettre à jour.
4. Dans la section Tags, choisissez Gérer les tags.
5. Sélectionnez Ajouter une nouvelle balise et entrez la clé et la valeur pour chaque balise que vous souhaitez ajouter.
6. Sélectionnez Save.

Pour supprimer une étiquette, choisissez Supprimer à côté de la balise que vous souhaitez supprimer.

Supprimer un objectif personnalisé

Pour supprimer un objectif personnalisé

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/](https://console.aws.amazon.com/wellarchitected/).
2. Dans le volet de navigation de gauche, choisissez Verres personnalisés.
3. Sélectionnez l'objectif personnalisé à supprimer, puis choisissez Supprimer.
4. Sélectionnez Delete (Supprimer).

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

Exclusion de responsabilité

En partageant vos verres personnalisés avec d'autres personnes Comptes AWS, vous reconnaissez qu'ils AWS seront mis à la disposition de ces autres comptes. Ces autres comptes peuvent continuer à accéder à vos verres personnalisés partagés et à les utiliser même si vous supprimez les verres personnalisés des vôtres Compte AWS ou si vous résiliez les vôtres Compte AWS.

Spécification du format de l'objectif

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

Section de l'objectif

Cette section définit les attributs de l'objectif personnalisé lui-même. Voici son nom et sa description.

- `schemaVersion`: version du schéma d'objectif personnalisé à utiliser. Défini par le modèle, ne le modifiez pas.
- `name`: nom de l'objectif. Le nom peut comporter jusqu'à 128 caractères.
- `description`: Description textuelle de l'objectif. Ce texte s'affiche lorsque vous sélectionnez des objectifs à ajouter lors de la création de la charge de travail ou lorsque vous sélectionnez un objectif 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 des piliers

Cette section définit les piliers associés à l'objectif personnalisé. Vous pouvez associer vos questions aux piliers du AWS Well-Architected Framework, définir vos propres piliers, ou les deux.

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

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

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

- `operationalExcellence`
- `security`
- `reliability`
- `performance`
- `costOptimization`
- `sustainability`
- **name**: Nom du pilier. Le nom peut comporter jusqu'à 128 caractères.

```
"pillars": [  
  {  
    "id": "company_Privacy",  
    "name": "Privacy Excellence",  
    .  
    .  
    .  
  },  
  {  
    "id": "company_Security",  
    "name": "Security",  
    .  
    .  
    .  
  }  
]
```

Section des questions

Cette section définit les questions associées à un pilier.

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

- **id**: ID de la question. L'identifiant peut comporter de 3 à 128 caractères et ne contenir que des caractères alphanumériques et des traits de soulignement (« _ »). Les identifiants utilisés dans une question doivent être uniques.
- **title**: Titre de la question. Le titre peut comporter jusqu'à 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. Le texte peut comporter jusqu'à 2 048 caractères. 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 une charge de travail d'objectif personnalisée avec Jira, les questions affichent à la fois l'« identifiant » et le « titre » 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 des choix

Cette section définit les choix associés à une question.

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

- **id**: ID du choix. L'identifiant peut comporter entre 3 et 128 caractères et ne 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 de `_no` fera office de `None of these choix` pour la question.
- **title**: Titre du choix. Le titre peut comporter jusqu'à 128 caractères.
- **helpfulResource displayText** : Facultatif. Texte fournissant des informations utiles sur un choix. Le texte peut comporter jusqu'à 2 048 caractères. Doit être inclus si cela **helpfulResource url** est spécifié.
- **helpfulResource url** : Facultatif. Une ressource URL qui explique le choix de manière plus détaillée. L'URL doit commencer par `http://` ou `https://`.
- **improvementPlan displayText**: texte qui décrit comment un choix peut être amélioré. Le texte peut comporter jusqu'à 2 048 caractères. Un **improvementPlan** est requis pour chaque choix, à l'exception d'un `None of these choix`.
- **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` soit `IMPROVEMENT_PLAN`.
- `additionalResources content` : Facultatif. Spécifie les `url` valeurs `displayText` et 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. Le texte peut comporter jusqu'à 2 048 caractères. Doit être inclus si cela `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 d'objectif personnalisée avec Jira, les choix affichent l' « identifiant » de la question et du choix, ainsi que le « titre » 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_ipplan_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_ipplan_02.html"  
                },  
                {  
                    "displayText": "This is the third piece of improvement plan  
text.",  
                    "url": "https://example.com/popt02_ipplan_03.html"  
                }  
                {  
                    "displayText": "This is the fourth piece of improvement plan  
text.",  
                    "url": "https://example.com/popt02_ipplan_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 relatives aux risques

Cette section définit la manière dont 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 y avoir une règle de `default` risque pour chaque question.

- **risk**: indique le risque associé à la maladie. Les valeurs valides sont `HIGH_RISK`, `MEDIUM_RISK` et `NO_RISK`.

L'ordre de vos règles de risque est important. Le premier `condition` qui l'évalue `true` définit le risque associé à la question. Un schéma courant de mise en œuvre des règles relatives aux risques consiste à commencer par les règles les moins risquées (et généralement les plus détaillées), puis à suivre les 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 l'un ou l'autre choice_2 ou choice_3 est sélectionné et est sélectionné, le risque est moyen.
- Si choice_1 ce n'est pas le cas mais l'choice_3 est, le risque est également moyen.
- Si aucune de ces conditions préalables n'était vraie, le risque est élevé.

Améliorations d'objectifs

Le AWS Well-Architected Framework Lens et les autres objectifs fournis AWS par celui-ci sont mis à jour à mesure que de nouveaux services sont introduits, que les meilleures pratiques existantes pour les systèmes basés sur le cloud sont affinées et que de nouvelles meilleures pratiques sont ajoutées. Lorsqu'une nouvelle version d'un objectif est mise à disposition, elle AWS WA Tool est mise à niveau pour refléter les meilleures pratiques les plus récentes. Toutes les nouvelles charges de travail définies utilisent la nouvelle version de l'objectif.

Une mise à niveau d'objectif se produit également lorsqu'une nouvelle version majeure d'un objectif personnalisé que vous avez appliqué à une charge de travail ou à un modèle de révision est publiée.

Une amélioration de l'objectif peut consister en n'importe quelle combinaison 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
- Ajouter ou supprimer des piliers

Vos réponses aux questions existantes sont conservées.

Note

Vous ne pouvez pas annuler une mise à niveau de l'objectif. Une fois qu'une charge de travail a été mise à niveau vers la dernière version de l'objectif, vous ne pouvez pas revenir à la version précédente de l'objectif.

Sélection d'une amélioration de l'objectif

La page Notifications affiche des informations pour chaque charge de travail qui n'utilise pas la version d'objectif la plus récente.

Les informations suivantes sont affichées 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 d'un modèle de charge de travail ou de révision.

Ressource associée

Le nom de l'objectif.

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 de l'objectif qui ne reflète plus les meilleures pratiques. Procédez à la mise à niveau vers la version actuelle du cadre.
- Supprimé — La charge de travail utilise un objectif qui a été supprimé par son propriétaire.

Version en cours d'utilisation

Version du cadre actuellement utilisée pour la charge de travail.

Version actuelle disponible

La version de l'objectif disponible pour la mise à niveau, ou Aucune si l'objectif 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 objectif

Les lentilles peuvent être mises à niveau pour les charges de travail et les modèles de révision.

Note

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

Mise à niveau d'un objectif en fonction d'une charge de travail

1. Sur la page Notifications, sélectionnez une charge de travail à mettre à niveau, puis choisissez Mettre à niveau la version de l'objectif. 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 de mettre à niveau un objectif pour une charge de travail, un jalon est créé pour enregistrer l'état de votre charge de travail existante pour référence future. Entrez un nom unique pour le jalon dans le champ Nom du jalon.
3. Cochez la case Confirmation à côté de J'ai compris et j'accepte ces modifications, puis cliquez sur Enregistrer.

Une fois l'objectif amélioré, vous pouvez consulter la version précédente de l'objectif dans l'onglet Milestones.

Mise à niveau d'un objectif pour un modèle d'évaluation

1. Pour améliorer l'objectif d'un modèle d'évaluation, choisissez

2. Sur la page Notifications, sélectionnez un modèle d'évaluation à mettre à niveau, puis choisissez Mettre à niveau la version de l'objectif. 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 Aperçu du modèle de révision.

3. Cochez la case Confirmation à côté de J'ai compris et j'accepte ces modifications, puis choisissez Mettre à niveau et modifier le modèle de réponses pour ajuster les réponses aux meilleures pratiques pour votre modèle d'évaluation, ou Mettre à niveau pour améliorer l'objectif sans ajuster les réponses de votre modèle.

Catalogue d'objectifs

Le catalogue d'objectifs est une collection d'objectifs AWS créés officiellement AWS WA Tool qui offrent une up-to-date technologie et les meilleures pratiques axées sur l'industrie. Ces objectifs sont disponibles pour tous les utilisateurs et ne nécessitent aucune installation supplémentaire pour être utilisés.

Le tableau suivant décrit tous les objectifs AWS officiels actuellement disponibles dans le catalogue d'objectifs.

Nom de l'objectif	Description
AWS Framework Well-Architected	Appliqué par défaut à toutes les charges de travail. Recueil des meilleures pratiques architecturales pour concevoir et exploiter des systèmes fiables, sécurisés, efficaces, rentables et durables dans le cloud.
Mobilité connectée	Les meilleures pratiques pour intégrer la technologie dans les systèmes de transport et améliorer l'expérience globale de mobilité.

Nom de l'objectif	Description
Construction de conteneurs	Fournit les meilleures pratiques relatives à la conception et au processus de construction des conteneurs.
Analyses de données	Contient des informations issues d'études de cas réelles et vous aide à découvrir les principaux éléments de conception des charges de travail analytiques de Well-Architected, ainsi que des recommandations d'amélioration. AWS
DevOps	Décrit une approche structurée que les entreprises de toutes tailles peuvent suivre pour développer une culture axée sur la rapidité et axée sur la sécurité, capable de générer une valeur commerciale substantielle en utilisant les technologies modernes et DevOps les meilleures pratiques.
Secteur des services financiers	Meilleures pratiques pour structurer les charges de travail de votre secteur des services financiers sur. AWS
Gouvernement	Meilleures pratiques pour la conception et la prestation de services gouvernementaux sur AWS.
Secteur de la santé	Meilleures pratiques et conseils sur la manière de concevoir, déployer et gérer vos charges de travail dans le secteur de la santé dans le AWS Cloud.
IoT	Meilleures pratiques pour gérer vos charges de travail liées à l'Internet des objets (IoT) dans AWS.

Nom de l'objectif	Description
Fusions et acquisitions	Bonnes pratiques en matière d'intégration des charges de travail et de migration vers le cloud lors de fusions et d'acquisitions.
Machine Learning (apprentissage automatique)	Meilleures pratiques pour gérer vos ressources et charges de travail liées au Machine Learning dans AWS.
Migration	Bonnes pratiques pour la migration vers le AWS Cloud.
SaaS	Axé sur la conception, le déploiement et l'architecture de vos charges de travail logicielles en tant que service (SaaS) dans le AWS Cloud
SAP	Principes de conception et meilleures pratiques pour les charges de travail SAP dans le AWS Cloud.
Applications sans serveur	Meilleures pratiques pour créer des charges de travail sans serveur sur AWS. Couvre des scénarios tels que les microservices RESTful, les backends d'applications mobiles, le traitement des flux et les applications Web.

Modèles d'avis

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 utilisateur ou compte IAM, 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 de mettre en œuvre les meilleures pratiques courantes et de réduire la redondance entre vos charges de travail.

Création d'un modèle d'avis

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, consultez [Balisage 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

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

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 les utilisateurs ou les comptes 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 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

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, consultez [the section called "Mise à niveau d'un objectif"](#).

Note

Pour définir une charge de travail à partir d'un modèle de révision, vous devez disposer des autorisations IAM pour créer une charge de travail activées `:wellarchitected:CreateWorkload`, ainsi que des autorisations de modèle de révision suivantes :

`wellarchitected:GetReviewTemplate`, `wellarchitected:GetReviewTemplateAnswer`, `wellarchitected:GetReviewTemplateLensReview`. Pour plus d'informations sur les autorisations IAM, consultez le [guide de l'utilisateur AWS d'Identity and Access Management](#).

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 le 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 de plus amples informations, 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

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 de révision que vous avez supprimé avec d'autres utilisateurs, comptes ou organisations IAM, ils ne pourront pas créer de charges de travail à partir de celui-ci.

Profils

Vous pouvez créer des profils pour fournir le contexte de votre entreprise et identifier les objectifs que vous souhaitez atteindre lors d'une révision 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. Le fait d'associer un profil à votre charge de travail vous permet également de voir quels risques sont prioritaires et que vous devez traiter 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. Sélectionnez Profils dans le volet de navigation de gauche.
2. Choisissez Créer un profil.
3. Dans la section Propriétés du profil, saisissez le nom et la description de votre profil.
4. Pour affiner les informations classées par ordre de priorité pour votre entreprise dans le plan d'examen et d'amélioration de la charge de travail, sélectionnez les réponses les plus pertinentes pour votre entreprise dans la section Questions de 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 Save (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, notamment le nom, la description, l'ARN, les dates de création et de mise à jour, ainsi que les réponses aux questions du profil. Sur la page d'aperçu du profil, vous pouvez modifier, supprimer ou partager votre profil.

Modification d'un profil

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 d'aperçu du profil.
4. Apportez les mises à jour nécessaires aux questions du profil.
5. Choisissez Save (Enregistrer).

Partage d'un profil

Les profils peuvent être partagés avec des utilisateurs ou des comptes, ou ils peuvent être partagés avec l'ensemble d'une organisation ou d'une unité organisationnelle.

Pour partager un profil

1. Sélectionnez Profils dans le volet de navigation de gauche.
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 pour les utilisateurs ou les comptes IAM. Dans la zone Envoyer des invitations, spécifiez les ID d'utilisateur ou de compte, puis choisissez Créer.
5. Pour partager avec une organisation ou une unité organisationnelle, choisissez Créer, puis sélectionnez Créer des partages pour les organisations. 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 la case, puis choisissez Créer.

⚠ Important

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

Ajouter un profil à une charge de travail

Vous pouvez ajouter un profil à une charge de travail existante ou lors de la définition d'une charge de travail afin d'accélérer le processus de révision 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 lors 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 de 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 plus d'informations, veuillez consulter [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 la révision pour répondre aux questions prioritaires de l'examen de la charge de travail. Pour plus d'informations, veuillez consulter [the section called "Documenter 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.

Supprimer un profil d'une charge de travail

La suppression d'un profil de la charge de travail rétablit la version de la charge de travail 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, entrez le nom du profil dans le champ de saisie de texte.
3. Choisissez Remove (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 y était associé, et les questions et les risques liés à l'examen de la charge de travail ne sont plus prioritaires.

Supprimer un profil de 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 des profils qui étaient partagés et associés à une charge de travail avant la suppression. Toutefois, aucune nouvelle charge de travail ne peut être associée à un profil supprimé. [the section called "Notifications de profil"](#) sont envoyés aux propriétaires de charges de travail à l'aide de profils supprimés.

Exclusion de responsabilité

En partageant vos profils avec d'autres personnes Comptes AWS, vous reconnaissez que vos profils AWS seront accessibles à ces autres comptes. Ces autres comptes peuvent continuer à accéder à vos profils partagés et à les utiliser même si vous supprimez le profil du vôtre Compte AWS ou si vous résiliez votre Compte AWS.

Pour supprimer un profil de votre liste de profils

1. Sélectionnez Profils dans le volet de navigation de gauche.

2. Sélectionnez le nom du profil que vous souhaitez supprimer.
3. Choisissez Delete (Supprimer).
4. Pour confirmer la suppression, entrez le nom du profil dans le champ de saisie de texte.
5. Choisissez Delete (Supprimer).

Si vous souhaitez conserver un profil dans votre liste de profils, mais le supprimer d'une charge de travail, consultez [the section called "Supprimer 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'un Compte 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 objectif”](#) 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, voir [the 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

vosre 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.

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

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le [modèle de responsabilité partagée](#) décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de [AWS conformité Programmes](#) de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Well-Architected Tool, voir [AWS Services concernés par programme de conformitéAWS](#) .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service 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 son utilisation AWS WA Tool. Les rubriques suivantes expliquent comment procéder à la configuration AWS WA Tool pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos AWS WA Tool ressources.

Rubriques

- [Protection des données dans AWS Well-Architected Tool](#)
- [Gestion des identités et des accès pour AWS Well-Architected Tool](#)
- [Réponse aux incidents dans AWS Well-Architected Tool](#)
- [Validation de conformité pour AWS Well-Architected Tool](#)
- [Résilience dans AWS Well-Architected Tool](#)
- [Sécurité de l'infrastructure dans AWS Well-Architected Tool](#)
- [Analyse de configuration et de vulnérabilité dans AWS Well-Architected Tool](#)
- [Prévention du cas de figure de l'adjoint désorienté entre services](#)

Protection des données dans AWS Well-Architected Tool

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

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

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez [Federal Information Processing Standard \(FIPS\) 140-2](#) (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec AWS WA Tool ou d'autres Services AWS utilisateurs de la console, de l'API ou AWS des SDK. AWS CLI Toutes les données que vous

entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Chiffrement au repos

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

Chiffrement en transit

Toutes les données envoyées et sortantes AWS WA Tool sont cryptées en transit.

Comment AWS utilisent vos données

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

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

- 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 à :

- 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

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser AWS WA Tool les ressources. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- [Public ciblé](#)
- [Authentification par des identités](#)
- [Gestion des accès à l'aide de politiques](#)
- [Comment AWS Well-Architected Tool fonctionne avec IAM](#)
- [AWS Well-Architected Tool exemples de politiques basées sur l'identité](#)
- [AWS politiques gérées pour AWS Well-Architected Tool](#)
- [Résolution des problèmes AWS Well-Architected Tool d'identité et d'accès](#)

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez. AWS WA Tool

Utilisateur du service : si vous utilisez le AWS WA Tool service pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de nouvelles AWS WA Tool fonctionnalités pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans AWS WA Tool, consultez [Résolution des problèmes AWS Well-Architected Tool d'identité et d'accès](#).

Administrateur du service — Si vous êtes responsable des AWS WA Tool ressources de votre entreprise, vous avez probablement un accès complet à AWS WA Tool. C'est à vous de déterminer les AWS WA Tool fonctionnalités et les ressources auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM avec AWS WA Tool, voir [Comment AWS Well-Architected Tool fonctionne avec IAM](#).

Administrateur IAM – Si vous êtes un administrateur IAM, vous souhaitez peut-être en savoir plus sur la façon d'écrire des politiques pour gérer l'accès à AWS WA Tool. Pour consulter des exemples de politiques AWS WA Tool basées sur l'identité que vous pouvez utiliser dans IAM, consultez. [AWS Well-Architected Tool exemples de politiques basées sur l'identité](#)

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section [Comment vous connecter à votre compte Compte AWS dans](#) le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section [Signature des demandes AWS d'API](#) dans le guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez [Authentification multifactorielle](#) dans le Guide de l'utilisateur AWS IAM Identity Center et [Utilisation de l'authentification multifactorielle \(MFA\) dans l'interface AWS](#) dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez [Tâches nécessitant des informations d'identification d'utilisateur root](#) dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles 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. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, 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 au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès.

Pour plus d'informations, consultez [Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification](#) dans le Guide de l'utilisateur IAM.

Un [groupe IAM](#) est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez [Quand créer un utilisateur IAM \(au lieu d'un rôle\)](#) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un [rôle IAM](#) est une identité au sein de votre Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console [changeant de rôle](#). Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez [Utilisation de rôles IAM](#) dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique [Jeux d'autorisations](#) dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent

le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez [Accès intercompte aux ressources dans IAM](#) dans le Guide de l'utilisateur IAM.

- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
- Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez [Sessions de transmission d'accès](#).
- Rôle de service : il s'agit d'un [rôle IAM](#) attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du 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.
- Rôle lié à un service — 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 apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations,

consultez [Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2](#) dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez [Quand créer un rôle IAM \(au lieu d'un utilisateur\)](#) dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez [Vue d'ensemble des politiques JSON](#) dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, 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. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez [Création de politiques IAM](#) dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique 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. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. 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. Services AWS

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

Listes de contrôle d'accès (ACL)

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.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez [Vue d'ensemble des listes de contrôle d'accès \(ACL\)](#) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- **Limite d'autorisations** : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez [Limites d'autorisations pour des entités IAM](#) dans le Guide de l'utilisateur IAM.
- **Politiques de contrôle des services (SCP)** — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez [Fonctionnement des SCP](#) dans le Guide de l'utilisateur AWS Organizations .
- **Politiques de séance** : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez [politiques de séance](#) 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 savoir comment AWS détermine s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section [Logique d'évaluation des politiques](#) dans le guide de l'utilisateur IAM.

Comment AWS Well-Architected Tool fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à AWS WA Tool, découvrez les fonctionnalités IAM disponibles. AWS WA Tool

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

Fonction IAM	AWS WA Tool soutien
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
Autorisations de principal	Oui
Fonctions du service	Non
Rôles liés à un service	Non

Pour obtenir une vue d'ensemble de la façon dont AWS WA Tool les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section [AWS Services compatibles avec IAM](#) dans le Guide de l'utilisateur IAM.

AWS WA Tool Politiques basées sur l'identité

Soutient les actions politiques : Oui

Les administrateurs peuvent utiliser les politiques AWS JSON 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. Les actions de stratégie portent généralement le même nom

que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Politiques basées sur les ressources au sein de 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. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. 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. 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. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez [Accès intercompte aux ressources dans IAM](#) dans le Guide de l'utilisateur IAM.

Actions politiques pour AWS WA Tool

Soutient les actions politiques : Oui

Les administrateurs peuvent utiliser les politiques AWS JSON 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. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Les actions de politique en AWS WA Tool cours 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 consulter la liste des AWS WA Tool actions, reportez-vous à la section [Actions définies par AWS Well-Architected Tool](#) dans la référence d'autorisation de service.

Ressources de politique

Prend en charge les ressources politiques : Oui

Les administrateurs peuvent utiliser les politiques AWS JSON 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. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son [Amazon Resource Name \(ARN\)](#). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

Pour consulter la liste des types de AWS WA Tool ressources et de leurs ARN, voir [Ressources définies par AWS Well-Architected Tool](#) dans la référence d'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 AWS WA Tool de charge de travail possède l'ARN suivant :

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

Pour plus d'informations sur le format des ARN, consultez les sections [Amazon Resource Names \(ARN\)](#) et [AWS Service Namespaces](#).

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 AWS WA Tool actions, telles que celles relatives à la création et à la liste des charges de travail, ne peuvent pas être effectuées sur une ressource spécifique. Dans ces cas-là, vous devez utiliser le caractère générique (*).

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

Pour consulter la liste des types de AWS WA Tool ressources et de leurs ARN, consultez la section [Ressources définies par AWS Well-Architected Tool](#) dans la référence d'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 conditions 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 AWS JSON 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` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. 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.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération AND logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une OR opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez [Éléments d'une politique IAM : variables et identifications](#) dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de [contexte de condition AWS globales](#) 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 voir toutes les clés de condition AWS globales, voir Clés [contextuelles de condition AWS globales](#) dans la référence d'autorisation de service.

Les administrateurs peuvent utiliser les politiques AWS JSON 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` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. 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.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération AND logique. Si vous spécifiez

plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une OR opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez [Éléments d'une politique IAM : variables et identifications](#) dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de [contexte de condition AWS globales](#) dans le guide de l'utilisateur IAM.

ACL dans AWS WA Tool

Supporte 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

Supporte l'ABAC (balises dans les politiques) : Oui

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

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 l'ABAC, consultez [Qu'est-ce que le contrôle d'accès basé sur les attributs \(ABAC\) ?](#) 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 d'informations d'identification temporaires avec AWS WA Tool

Supporte les informations d'identification temporaires : Oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation [d'IAM](#) dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez [Changement de rôle \(console\)](#) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez [Informations d'identification de sécurité temporaires dans IAM](#).

Autorisations principales interservices pour AWS WA Tool

Supporte les sessions d'accès direct (FAS) : Oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal

appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez [Transmission des sessions d'accès](#).

Fonctions du service pour AWS WA Tool

Supporte les rôles de service : Non

Une fonction 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 une fonction du 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 aux services : 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 apparaissent dans votre Compte AWS répertoire et appartiennent au 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 Tool exemples 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 effectuer de tâches à l'aide de l' AWS API AWS Management Console AWS CLI, ou. 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 AWS Well-Architected Tool Connector for Jira](#)

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer AWS WA Tool des ressources 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 :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques 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.
- Accorder 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 de IAM pour appliquer des autorisations, consultez [politiques et autorisations dans IAM](#) dans le Guide de l'utilisateur IAM.

- Utiliser 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 par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez [Conditions pour éléments de politique JSON IAM](#) dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer 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 politique IAM Access Analyzer](#) dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez [Configuration de l'accès aux API protégé par 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 AWS Well-Architected Tool console, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les détails AWS WA Tool des ressources de votre Compte AWS. Si vous créez une stratégie 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 stratégie.

Pour garantir que ces entités peuvent toujours utiliser la AWS WA Tool console, associez également la politique AWS gérée 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.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. 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 permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "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 un accès Compte AWS complet à vos charges de travail. L'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.

```
{
  "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 un accès en Compte AWS 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.

```
{
  "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 région un accès en Compte AWS lecture seule à l'une de vos charges de travail 99999999999955555555555566666666, dans la région. us-west-2 777788889999 est votre ID de compte.

```

{
  "Version": "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:Get*",
        "wellarchitected:List*"
      ],
      "Resource": "arn:aws:wellarchitected:us-west-2:777788889999:workload/99999999999955555555555566666666"
    }
  ]
}

```

Utilisation d'une clé de condition spécifique au service pour le AWS Well-Architected Tool Connector for 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.

Ce qui suit décrit les utilisations pertinentes de la clé de condition :

- **CreateWorkload:** Lorsque vous postulez `wellarchitected:JiraProjectKey` à `CreateWorkload`, vous pouvez définir quels projets Jira personnalisés peuvent être liés à

n'importe quelle charge de travail 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 postulez `wellarchitected:JiraProjectKey` à `UpdateWorkload`, vous pouvez définir quels projets Jira personnalisés peuvent être liés à cette charge de travail particulière ou à n'importe quelle charge de travail. 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 postulez `wellarchitected:JiraProjectKey` à `UpdateGlobalSettings`, vous pouvez définir les projets Jira personnalisés qui 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.

```
{
  "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": "WORKLOAD_ARN",
  "Condition": {
    "StringEqualsIfExists": {
      "wellarchitected:JiraProjectKey": ["ABC, PQR"]
    }
  }
}
]
```

AWS politiques gérées pour AWS Well-Architected Tool

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées 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.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. 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 AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle politique Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez la section [Politiques gérées par AWS](#) dans le Guide de l'utilisateur IAM.

AWS politique gérée : WellArchitectedConsoleFullAccess

Vous pouvez associer la politique WellArchitectedConsoleFullAccess à vos identités IAM.

Cette politique accorde un accès complet à AWS Well-Architected Tool.

Détails de l'autorisation

```
{
```



```
"Version": "2012-10-17",
"Statement" : [
  {
    "Effect" : "Allow",
    "Action" : [
      "wellarchitected:*"
    ],
    "Resource": "*"
  }
]
```

AWS politique gérée : WellArchitectedConsoleReadOnlyAccess

Vous pouvez associer la politique WellArchitectedConsoleReadOnlyAccess à vos identités IAM.

Cette politique accorde un accès en lecture seule à AWS Well-Architected Tool

Détails de l'autorisation

```
{
  "Version": "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:Get*",
        "wellarchitected:List*",
        "wellarchitected:ExportLens"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS politique gérée : AWSWellArchitectedOrganizationsServiceRolePolicy

Vous pouvez associer la politique AWSWellArchitectedOrganizationsServiceRolePolicy à vos identités IAM.

Cette politique accorde les autorisations administratives nécessaires pour faciliter AWS Well-Architected Tool l'intégration avec les Organizations. AWS 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`— Permet aux principaux de vérifier si l'accès au AWS service est activé pour AWS WA Tool.
- `organizations:DescribeAccount`— Permet aux directeurs d'accéder aux informations relatives à un compte au sein de l'organisation.
- `organizations:DescribeOrganization`— Permet aux responsables de récupérer des informations sur la configuration de l'organisation.
- `organizations:ListAccounts`— Permet aux principaux de récupérer la liste des comptes appartenant à une organisation.
- `organizations:ListAccountsForParent`— Permet aux principaux de récupérer la liste des comptes appartenant à une organisation à partir d'un nœud racine donné de l'organisation.
- `organizations:ListChildren`— Permet aux principaux de récupérer la liste des comptes et des unités organisationnelles appartenant à une organisation à partir d'un nœud racine donné de l'organisation.
- `organizations:ListParents`— Permet aux directeurs d'école de récupérer la liste des parents immédiats spécifiée par l'unité d'organisation ou le compte au sein d'une organisation.
- `organizations:ListRoots`— Permet aux principaux de récupérer la liste de tous les nœuds racines d'une organisation.

```
{
  "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": "*"
    }
  ]
}
```

AWS politique gérée : AWSWellArchitectedDiscoveryServiceRolePolicy

Vous pouvez associer la politique `AWSWellArchitectedDiscoveryServiceRolePolicy` à vos identités IAM.

Cette politique permet AWS Well-Architected Tool d'accéder aux AWS services et aux ressources liés aux AWS WA Tool ressources.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `trustedadvisor:DescribeChecks`— Liste les Trusted Advisor chèques disponibles.
- `trustedadvisor:DescribeCheckItems`— Récupère les données de Trusted Advisor contrôle, y compris le statut et les ressources signalées par. Trusted Advisor
- `servicecatalog:GetApplication`— Récupère les détails d'une AppRegistry application.
- `servicecatalog:ListAssociatedResources`: répertorie les ressources associées à une AppRegistry application.
- `cloudformation:DescribeStacks`—Obtient les détails des AWS CloudFormation piles.
- `cloudformation:ListStackResources`: répertorie les ressources associées aux AWS CloudFormation piles.
- `resource-groups:ListGroupResources`—Répertorie les ressources provenant d'un ResourceGroup.
- `tag:GetResources`— Nécessaire 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 un service à une AppRegistry application.
- `servicecatalog:UpdateAttributeGroup`— Met à jour un groupe d'attributs géré par un service.

- `servicecatalog:DisassociateAttributeGroup`: dissocie un groupe d'attributs géré par un service d'une application. AppRegistry
- `servicecatalog>DeleteAttributeGroup`— Supprime un groupe d'attributs géré par un service lorsque cela est nécessaire.

```
{
  "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-*"
]
}
]
}

```

AWS WA Tool mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées AWS WA Tool depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page [Historique du AWS WA Tool document](#).

Modification	Description	Date
AWS WA Tool politique gérée modifiée	Ajout de "wellarchitected:Export*" à WellArchitectedConsoleReadOnlyAccess	22 juin 2023
AWS WA Tool politique de rôle de service ajoutée	Ajouté AWSWellArchitectedDiscoveryServiceRolePolicy pour permettre AWS Well-	3 mai 2023

Modification	Description	Date
	Architected Tool d'accéder aux AWS services et aux ressources liés aux AWS WA Tool ressources.	
AWS WA Tool autorisations ajoutées	Ajout d'une nouvelle action à accorder <code>ListAWSServiceAccessForOrganization</code> pour autoriser AWS WA Tool à vérifier si l'accès au AWS service est activé pour AWS WA Tool.	22 juillet 2022
AWS WA Tool a commencé à suivre les modifications	AWS WA Tool a commencé à suivre les modifications apportées AWS à ses politiques gérées.	22 juillet 2022

Résolution des problèmes AWS Well-Architected Tool d'identité et d'accès

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec AWS WA Tool 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

S'il vous AWS Management Console indique que vous n'êtes pas autorisé à effectuer 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 lorsque l'utilisateur de *mateojackson* essaie d'utiliser la console pour effectuer l'`DeleteWorkload` action, mais 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 AWS Well-Architected Tool est une AWS responsabilité. AWS dispose d'une politique et d'un programme formels et documentés qui régissent la réponse aux incidents.

AWS les problèmes opérationnels ayant un impact important sont publiés sur le [AWS Service Health Dashboard](#).

Les problèmes opérationnels sont également postés dans les comptes individuels via le AWS Health Dashboard. Pour plus d'informations sur l'utilisation du AWS Health Dashboard, consultez le [guide de AWS Health l'utilisateur](#).

Validation de conformité pour AWS Well-Architected Tool

Pour savoir si un [programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité](#) spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de [AWS conformité Programmes AWS](#) de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir [Téléchargement de rapports dans AWS Artifact](#) .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- [Guides de démarrage rapide sur la sécurité et la conformité](#) : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- [Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services](#) : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

Note

Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le [HIPAA Eligible Services Reference](#).

- AWS Ressources de <https://aws.amazon.com/compliance/resources/> de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- [AWS Guides de conformité destinés aux clients](#) — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans plusieurs cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- [Évaluation des ressources à l'aide des règles](#) du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- [AWS Security Hub](#)— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez [Référence des contrôles Security Hub](#).
- [Amazon GuardDuty](#) — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- [AWS Audit Manager](#)— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dans AWS Well-Architected Tool

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées,

connectées par un réseau à faible latence, à haut débit et hautement redondant. 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 zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section [Infrastructure AWS globale](#).

Sécurité de l'infrastructure dans AWS Well-Architected Tool

En tant que service géré, AWS Well-Architected Tool il est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section [Sécurité du AWS cloud](#). Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section [Protection de l'infrastructure](#) dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder 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.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser [AWS Security Token Service](#) (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Analyse de configuration et de vulnérabilité dans AWS Well-Architected Tool

La configuration et les contrôles informatiques sont une responsabilité partagée entre vous AWS et vous, notre client. Pour plus d'informations, consultez le [modèle de responsabilité AWS partagée](#).

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. En AWS, l'usurpation d'identité interservices peut entraîner la confusion des adjoints. 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 d'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 recommandons d'utiliser les clés de contexte de condition [aws:SourceAccount](#) globale [aws:SourceArn](#) et les clés contextuelles dans les politiques de ressources afin de limiter les autorisations qui AWS Well-Architected Tool accordent un autre service à la ressource. 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 de `aws:SourceArn` doit être une charge de travail ou un objectif.

L'exemple suivant montre comment vous pouvez utiliser les touches de contexte de condition `aws:SourceAccount` globale `aws:SourceArn` et globale AWS WA Tool pour éviter le problème de confusion des adjoints.

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

```
"Principal": {
  "Service": "wellarchitected.amazonaws.com"
},
"Action": "wellarchitected:ActionName",
"Resource": [
  "arn:aws:wellarchitected::ResourceName/*"
],
"Condition": {
  "ArnLike": {
    "aws:SourceArn": "arn:aws:wellarchitected:*:123456789012:*"
  },
  "StringEquals": {
    "aws:SourceAccount": "123456789012"
  }
}
}
```

Partage de vos AWS WA Tool ressources

Pour partager une ressource dont vous êtes propriétaire, procédez comme suit :

- [Activez le partage des ressources au sein de AWS Organizations](#) (facultatif)
- [Partage d'une charge de travail](#)
- [Partagez un objectif personnalisé](#)
- [Partager un profil](#)
- [Partager un modèle d'avis](#)

Remarques

- Le partage d'une ressource la rend disponible pour une utilisation par des personnes autres que celles Compte AWS qui ont 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 partenaires avec lesquels vous partagez peuvent accéder aux partages de ressources uniquement dans le pays Régions AWS dans lequel ils ont été créés.
- Pour partager des ressources dans une région introduite après le 20 mars 2019, vous et la personne partagée Compte AWS devez activer la région dans le AWS Management Console. Pour plus d'informations, reportez-vous à la section [Infrastructure AWS mondiale](#).

Activez le partage des ressources au sein de 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 appartient à une organisation, vous pouvez le partager avec des comptes individuels, ou avec tous les comptes de l'organisation ou d'une unité d'organisation sans avoir à énumérer chaque compte.

Pour partager des ressources au sein d'une organisation, vous devez d'abord utiliser la AWS WA Tool console ou 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

il n'envoie pas d'invitations aux principaux. Les responsables de votre organisation ont accès aux ressources partagées sans avoir à 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 ne peut être assumé que par le AWS WA Tool service et accorde AWS WA Tool l'autorisation de récupérer des informations sur l'organisation dont il est membre, à l'aide de la politique AWS gérée `AWSWellArchitectedOrganizationsServiceRolePolicy`.

Si vous n'avez plus besoin de partager des ressources avec l'ensemble de votre organisation ou de vos unités d'organisation, vous pouvez désactiver le partage des ressources.

Prérequis

- 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 de l'organisation doivent être activées. Pour plus d'informations, consultez la section [Activation de toutes les fonctionnalités de votre organisation](#) dans le Guide de AWS Organizations l'utilisateur.

Important

Vous devez activer le partage avec à AWS Organizations l'aide de la AWS WA Tool console. Cela garantit que le `AWSServiceRoleForWellArchitected` rôle lié à un service est créé. Si vous activez l'accès sécurisé à l'aide AWS Organizations de la AWS Organizations console ou de la [enable-aws-service-access](#) AWS CLI commande, le rôle `AWSServiceRoleForWellArchitected` lié au service 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 Well-Architected Tool console AWS Management Console et ouvrez-la à l'[adresse https://console.aws.amazon.com/wellarchitected/](https://console.aws.amazon.com/wellarchitected/).

Vous devez vous connecter en tant que principal au compte de gestion de l'organisation.

2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Choisissez Activer le AWS Organizations support.

4. Choisissez Save settings (Enregistrer les paramètres).

Pour désactiver le partage des ressources au sein de votre organisation

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/](https://console.aws.amazon.com/wellarchitected/).

Vous devez vous connecter en tant que principal au compte de gestion de l'organisation.

2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Désélectionnez Activer le AWS Organizations support.
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](#)
- [Balisage de vos ressources](#)
- [Restrictions liées aux étiquettes](#)
- [Gestion des étiquettes à l'aide de la console](#)
- [Utilisation des balises à l'aide de l'API](#)

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, les étiquettes associées à celle-ci seront 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 AWS Identity and Access Management (IAM), vous pouvez contrôler les utilisateurs autorisés à créer, modifier ou supprimer des balises. [Compte AWS](#)

Balisage de vos ressources

Vous pouvez étiqueter des AWS WA Tool ressources nouvelles ou existantes.

Si vous utilisez la AWS WA Tool console, vous pouvez appliquer des balises aux nouvelles ressources lors 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 de révision existants, vous pouvez appliquer des balises via l'onglet Vue d'ensemble.

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 plus d'informations, 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)
AWS WA Toolcharges de travail	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 Toolverres personnalisés	Oui	Non	Oui
AWS WA Toolprofils	Oui	Non	Oui
AWS WA Toolmodèles d'avis	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 comportant ce préfixe ne sont pas prises en compte dans votre tags-per-resource limite.

Gestion des étiquettes à l'aide de la console

À l'aide de la AWS WA Tool console, 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 AWS WA Tool ressources lorsque vous les créez.

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 Vue d'ensemble pour les objectifs, les profils et les modèles de révision personnalisés.

Pour ajouter ou supprimer une balise sur 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/](https://console.aws.amazon.com/wellarchitected/).
2. Dans la barre de navigation, choisissez la région à utiliser.
3. Dans le volet de navigation, sélectionnez Workloads.
4. Sélectionnez la charge de travail à modifier, puis choisissez Propriétés.
5. Dans la section Tags (Balises) choisissez Manage tags (Gérer les balises).
6. Ajoutez ou supprimez vos tags selon les besoins.
 - Pour ajouter un tag, choisissez Ajouter un nouveau tag et renseignez les champs Clé et Valeur.
 - Pour supprimer une balise, sélectionnez Remove (Supprimer).
7. Répétez ce processus pour chaque balise que vous souhaitez ajouter, modifier ou supprimer. Choisissez Save pour enregistrer les changements.

Pour ajouter ou supprimer un tag sur un objectif personnalisé

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/](https://console.aws.amazon.com/wellarchitected/).
2. Dans la barre de navigation, choisissez la région à utiliser.
3. Dans le volet de navigation, choisissez Verres personnalisés.

4. Sélectionnez le nom de l'objectif personnalisé à modifier.
5. Dans la section Balises de l'onglet Vue d'ensemble, choisissez Gérer les balises.
6. Ajoutez ou supprimez vos tags selon les besoins.
 - Pour ajouter un tag, choisissez Ajouter un nouveau tag et renseignez les champs Clé et Valeur.
 - Pour supprimer une balise, sélectionnez Remove (Supprimer).
7. Répétez ce processus pour chaque balise que vous souhaitez ajouter, modifier ou supprimer. Choisissez Save pour enregistrer les changements.

Pour ajouter ou supprimer un tag sur un profil

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/](https://console.aws.amazon.com/wellarchitected/).
2. Dans la barre de navigation, choisissez la région à utiliser.
3. Dans le volet de navigation, sélectionnez Profils.
4. Sélectionnez le nom du profil à modifier.
5. Dans la section Balises de l'onglet Vue d'ensemble, choisissez Gérer les balises.
6. Ajoutez ou supprimez vos tags selon les besoins.
 - Pour ajouter un tag, choisissez Ajouter un nouveau tag et renseignez les champs Clé et Valeur.
 - Pour supprimer une balise, sélectionnez Remove (Supprimer).
7. Répétez ce processus pour chaque balise que vous souhaitez ajouter, modifier ou supprimer. Choisissez Save pour enregistrer les changements.

Pour ajouter ou supprimer un tag dans un modèle d'avis

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/](https://console.aws.amazon.com/wellarchitected/).
2. Dans la barre de navigation, choisissez la région à utiliser.
3. Dans le volet de navigation, sélectionnez Réviser les modèles.
4. Sélectionnez le nom du modèle de révision à modifier.
5. Dans la section Balises de l'onglet Vue d'ensemble, choisissez Gérer les balises.

6. Ajoutez ou supprimez vos tags selon les besoins.
 - Pour ajouter un tag, choisissez Ajouter un nouveau tag et renseignez les champs Clé et Valeur.
 - Pour supprimer une balise, sélectionnez Remove (Supprimer).
7. Répétez ce processus pour chaque balise que vous souhaitez ajouter, modifier ou supprimer. Choisissez Save pour enregistrer les changements.

Utilisation des balises à l'aide de l'API

Utilisez les opérations AWS WA Tool d'API suivantes 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
Répertorie 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
Pour créer un profil	CreateProfile
Création d'un modèle d'avis	CreateReviewTemplate

Journalisation des appels d'API AWS WA Tool avec AWS CloudTrail

AWS Well-Architected Tool est intégré à AWS CloudTrail, service qui enregistre les actions accomplies par un utilisateur, un rôle ou un AWS service dans le AWS WA Tool. CloudTrail capture les appels d'API vers le AWS WA Tool 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 dans un compartiment Amazon S3, y compris des événements pour AWS WA Tool. Si vous ne configurez pas de journal d'activité, vous pouvez toujours afficher les événements les plus récents dans la CloudTrail console dans Event history (Historique des événements). Les informations collectées par CloudTrail, vous permettent de déterminer quelle demande a été envoyée à AWS WA Tool, l'adresse IP source à partir de laquelle la demande a été effectuée, qui a effectué la demande, quand, ainsi que d'autres informations.

Pour en savoir plus CloudTrail, consultez le [Guide de AWS CloudTrail l'utilisateur](#).

AWS WA Tool informations 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 CloudTrail événement avec d'autres événements de AWS services dans Event history (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 CloudTrail événements](#).

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 CloudTrail de suivi permet de livrer des fichiers journaux dans 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 d'activité consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Simple Storage Service (Amazon S3) de votre choix. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en profondeur les données d'événement collectées dans les CloudTrail journaux et prendre les mesures nécessaires. Pour en savoir plus, consultez les ressources suivantes :

- [Présentation de la création d'un journal d'activité](#)

- [CloudTrail Services et intégrations pris en charge](#)
- [Configuration des Notifications de Amazon SNS pour CloudTrail](#)
- [Réception des fichiers CloudTrail journaux de plusieurs régions](#) et [Réception des fichiers CloudTrail journaux de plusieurs comptes](#)

Toutes les AWS WA Tool actions sont enregistrées CloudTrail et documentées dans [Actions définies par AWS Well-Architected Tool](#). Par exemple, les appels aux `CreateWorkloadShare` actions `CreateWorkloadDeleteWorkload`, et génèrent des entrées dans les fichiers CloudTrail journaux.

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 :

- Si la demande a été effectuée avec les informations d'identification utilisateur ou 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 requête a été effectuée par un autre service AWS.

Pour plus d'informations, consultez la section [Élément `userIdentity` CloudTrail](#).

Présentation des AWS WA Tool entrées des fichiers journaux

Un journal d'activité est une configuration qui permet d'envoyer des événements sous forme de fichiers journaux à un compartiment Simple Storage Service (Amazon S3) que vous spécifiez. CloudTrail les fichiers journaux peuvent contenir une ou plusieurs entrées de journal. Un événement représente une demande individuelle émise à partir d'une source quelconque et comprend des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace de pile ordonnée des appels d'API publics. Ils ne suivent aucun ordre précis.

L'exemple suivant montre une entrée de CloudTrail journal qui illustre l'`CreateWorkload` action.

```
{
  "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 prises sur des ressources Well-Architected. Vous pouvez utiliser EventBridge et ces événements pour écrire des règles d'action, par exemple vous avertir, lorsqu'un changement de ressource se produit. Pour plus d'informations, consultez [Qu'est-ce qu'Amazon EventBridge ?](#)

Note

Les événements sont transmises dans la mesure du possible.

Les actions suivantes se traduisent par EventBridge événements :

- Lié à la 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 de l'état d'une invitation de partage
 - Ajout ou suppression de balises
 - Mise à jour d'une réponse
 - Mise à jour des notes de
 - Ajout ou suppression d'un cadre d'une charge de travail
- Lié à la lentille
 - Importation ou exportation d'un objectif personnalisé
 - Publication d'un cadre personnalisé
 - Suppression d'un cadre personnalisé
 - Partager ou annuler le partage d'un cadre personnalisé
 - Mise à jour de l'état d'une invitation de partage
 - Ajout ou suppression d'un cadre d'une charge de travail

Exemples d'événements àAWS 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":"ARO4JUSXMN5ZR6S7LZNP:sample-user",
      "arn":"arn:aws:sts::123456789012:assumed-role/Admin/example-user",
      "accountId":"123456789012",
      "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
      "sessionContext":{
        "sessionIssuer":{
          "type":"Role",
          "principalId":"ARO4JUSXMN5ZR6S7LZNP",
          "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 cadre 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":"ARO0A4JUSXMN5ZR6S7LZNP:example-user",
    "arn":"arn:aws:sts::123456789012:assumed-role/Admin/example-user",
    "accountId":"123456789012",
    "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
    "sessionContext":{
      "sessionIssuer":{
        "type":"Role",
        "principalId":"ARO0A4JUSXMN5ZR6S7LZNP",
        "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"  
  }  
}
```

Historique du document

Le tableau suivant décrit la documentation de cette version du AWS Well-Architected Tool.

- Version de l'API : dernière en date
- Dernière mise à jour de la documentation : 27 juin 2024

Modification	Description	Date
Objectifs nouveaux et mis à jour	Cette version a ajouté un nouvel objectif au catalogue d'objectifs et a mis à jour un autre objectif.	27 juin 2024
Jira	Cette version a ajouté le AWS Well-Architected Tool connecteur pour Jira.	16 avril 2024
Nouveaux verres	Cette version a ajouté de nouveaux objectifs au catalogue d'objectifs.	26 mars 2024
Fonctionnalités mises à jour	Cette version ajoute la fonctionnalité Lens Catalog à AWS WA Tool.	26 novembre 2023
Fonctionnalités mises à jour	Cette version ajoute la fonctionnalité Modèles de révision à AWS WA Tool.	3 octobre 2023
WellArchitectedConsoleReadOnlyAccess politique gérée mise à jour	Ajout de "wellarchitected:ExportLens" à WellArchitectedConsoleReadOnlyAccess	22 juin 2023

Fonctionnalités mises à jour	Cette version ajoute la fonctionnalité Profils à AWS WA Tool.	13 juin 2023
Fonctionnalités mises à jour	Cette version améliore l'AWS Service Catalog AppRegistry intégration AWS Trusted Advisor et les ajoute AWS WellArchitectedDiscoveryServiceRolePolicy aux politiques AWS gérées.	3 mai 2023
Mise à jour du contenu	La page du 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 de la WellArchitectedConsoleReadOnlyAccess politique corrigé.	19 janvier 2023
Mise à jour des directives 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
Fonctionnalités mises à jour	Cette version retire l'objectif FTR de l'outil.	14 décembre 2022

Fonctionnalités mises à jour	Cette version ajoute l' AWS Service Catalog AppRegistry intégration AWS Trusted Advisor et.	7 novembre 2022
Mise à jour du contenu	Correction d'un problème dans l'exemple JSON de l'objectif personnalisé pourchoices.	29 septembre 2022
Mise à jour du contenu	La choices section de la spécification JSON de l'objectif personnalisé a été mise à jour.	2 août 2022
Fonctionnalités mises à jour	Cette version ajoute le suivi des modifications AWS à ses politiques gérées et ajoute une nouvelle action pour accorder l'ListAWSServiceAccessForOrganization autorisation auAWSWellArchitected OrganizationsServiceRolePolicy .	22 juillet 2022
Partage d'organisation ajouté	Cette version ajoute la possibilité de partager des charges de travail et des objectifs personnalisés avec une organisation et des unités organisationnelles (UO).	30 juin 2022

Fonctionnalités mises à jour	Cette version ajoute la possibilité de spécifier des ressources supplémentaires pour les choix d'un objectif personnalisé, de prévisualiser un objectif personnalisé avant de le publier et d'ajouter des balises aux objectifs personnalisés.	21 juin 2022
Fonctionnalités mises à jour	Cette version ajoute la possibilité d'accéder à la communauté AWS Well-Architected sur Re:post. AWS	31 mai 2022
Fonctionnalités mises à jour	Cette version ajoute le pilier de durabilité et des mises à jour mineures au didacticiel.	31 mars 2022
EventBridge support ajouté	AWS WA Tool envoie désormais un événement à Amazon EventBridge lorsqu'une modification est apportée à une ressource Well-Architected.	3 mars 2022
Verres personnalisés ajoutés	La possibilité d'ajouter des verres personnalisés a été ajoutée.	29 novembre 2021
Fonctionnalités mises à jour	Les meilleures pratiques individuelles peuvent désormais être marquées comme non applicables.	14 juillet 2021
Marquage des ressources disponible	Cette version ajoute la possibilité d'ajouter des balises aux charges de travail.	3 mars 2021

L'API est désormais disponible	Cette version ajoute l' AWS WA Tool API. AWS CloudTrail informations de journalisation ajoutées.	16 décembre 2020
Fonctionnalités mises à jour	Cette version ajoute les objectifs 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'une fois que vous avez mis à niveau une charge de travail pour utiliser un nouvel objectif, vous ne pouvez pas revenir à la version précédente.	8 juillet 2020
Mise à jour du contenu	Le partage clarifié est Régions AWS introduit après le 20 mars 2019.	24 juin 2020
Fonctionnalités mises 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 l' AWS utilisation de vos données a été ajoutée.	21 mai 2020

Fonctionnalités mises à jour	Cette version ajoute un responsable de vérification à la charge globale.	1er avril 2020
Fonctionnalités mises à jour	Cette version ajoute un lien de schéma architectural vers la charge de travail.	10 mars 2020
Mise à jour du contenu	Il a été précisé que les parts de charge de travail sont Région AWS spécifiques.	10 janvier 2020
Fonctionnalités mises 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
Fonctionnalités mises à jour	Cette version rend les champs du secteur facultatifs lors de la définition d'une charge de travail.	19 août 2019
Fonctionnalités mises à jour	Cette version ajoute des éléments de plan d'amélioration à la charge de travail.	29 juillet 2019
Fonctionnalités mises à jour	La version ajoute l' DeleteWorkload action à la politique.	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

<u>Fonctionnalités mises à jour</u>	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
<u>Fonctionnalités mises à jour</u>	Cette version ajoute la possibilité de spécifier non-Régions AWS lors de la définition d'une charge de travail.	14 février 2019
<u>AWS Well-Architected Tool disponibilité générale</u>	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.