



Guide de mise en route

AWS Management Console



Version 1.0

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Management Console: Guide de mise en route

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

Qu'est-ce que c'est AWS Management Console ?	1
Caractéristiques de AWS Management Console	1
Consoles AWS de service individuelles	2
Accès au AWS Management Console	2
Accès au AWS Management Console avec des appareils mobiles	3
Mise en route avec un service	4
Navigation unifiée	5
Accès au menu Services	6
Recherche de produits, services, fonctions et plus	6
Recherche de AWS produits	7
Affiner votre recherche	8
Afficher les fonctionnalités d'un service	8
Lancement AWS CloudShell	9
Accès aux AWS notifications et aux événements de santé	9
Obtention de support	10
Configuration du AWS Management Console	11
Configuration des paramètres unifiés	11
Configuration de régions et de services visibles	14
Choix de votre région	16
Favoris	18
Modifier votre mot de passe	22
Modification de la langue du AWS Management Console	25
Accès à vos AWS informations	27
Accès aux informations du compte	28
Accès aux informations de l'organisation	28
Accès aux informations sur les quotas de service	29
Accès aux informations de facturation	29
Connexion à plusieurs comptes	30
Utilisation des actions recommandées	31
Caractéristiques des actions AWS recommandées	31
Utilisation des actions recommandées	32
Surveillance à l'aide de CloudTrail journaux	32
AWS Console Home	35
Afficher tous les AWS services	35

Utilisation de widgets	36
Gestion des widgets	36
Mes candidatures	38
Fonctionnalités de myApplications	38
Services connexes	39
Accès à myApplications	40
Tarification	40
Régions prises en charge	40
Applications	41
Ressources	49
Tableau de bord myApplications	53
Discuter avec Amazon Q	58
Commencez avec Amazon Q	58
Exemples de questions	58
AWS Management Console Accès privé	59
Consoles Régions AWS de service et fonctionnalités prises en charge	59
Vue d'ensemble des contrôles de sécurité des accès AWS Management Console privés	65
Restrictions relatives aux comptes AWS Management Console depuis votre réseau	65
Connectivité entre votre réseau et Internet	65
Points de terminaison de VPC et configuration DNS requis	66
Configuration de l'DNS	66
Points de terminaison VPC et configuration des services DNS AWS	69
Mise en œuvre de politiques de contrôle des services et de politiques de points de terminaison de VPC	70
Politiques de contrôle des services	70
Politiques de point de terminaison d'un VPC	71
Mise en œuvre de politiques basées sur l'identité et d'autres types de politiques	73
Clés contextuelles de condition AWS globale prises en charge	73
Comment fonctionne AWS Management Console Private Access avec AWS : SourceVpc	73
Comment les différents chemins réseau sont reflétés dans CloudTrail	75
Essayez l'accès AWS Management Console privé	75
Configuration test avec Amazon EC2	76
Configuration des tests avec Amazon WorkSpaces	90
Configuration test du VPC avec des politiques IAM	107
Architecture de référence	109
AWS Personnalisation de l'expérience utilisateur	111

Prise en main	112
Conditions préalables	112
Accès aux paramètres UXC dans le AWS Management Console	112
Accès aux paramètres UXC par programmation	113
Surveillance à l'aide de CloudTrail journaux	113
Événements de gestion UXC dans CloudTrail	114
Exemples d'événements UXC	33
Sécurité	115
Gestion de l'identité et des accès	116
AWS politiques gérées	127
AWSManagementConsoleBasicUserAccess	127
AWSManagementConsoleAdministratorAccess	128
Mises à jour des politiques	130
Markdown dans AWS	132
Paragraphe, espacement de ligne et lignes horizontales	132
En-têtes	133
Mise en forme d'un texte	133
Liens	134
Lists	134
Tableaux et boutons (CloudWatch tableaux de bord)	134
Résolution des problèmes	136
La page ne se charge pas correctement.	136
Mon navigateur affiche un message d'erreur « accès refusé » lors de la connexion au AWS Management Console	137
Mon navigateur affiche des erreurs de temporisation lors de la connexion au AWS Management Console	138
Je souhaite changer la langue du AWS Management Console mais je ne trouve pas le menu de sélection de langue en bas de page	139
Historique du document	140
.....	cxliv

Qu'est-ce que c'est AWS Management Console ?

[AWS Management Console](#) Il s'agit d'une application Web qui contient et fournit un accès centralisé à toutes les consoles AWS de service individuelles. Vous pouvez utiliser la navigation unifiée AWS Management Console pour rechercher des services, consulter les notifications AWS CloudShell, accéder aux informations de compte et de facturation, et personnaliser les paramètres généraux de votre console. La page d'accueil du AWS Management Console s'appelle AWS Console Home. À partir de là AWS Console Home, vous pouvez gérer vos AWS applications et accéder à toutes les autres consoles de service individuelles. Vous pouvez également le personnaliser AWS Console Home pour afficher d'autres informations utiles sur vos ressources AWS et autres informations utiles à l'aide de widgets. Vous pouvez ajouter, supprimer et réorganiser des widgets tels que Recently Visited, AWS Health, etc.

Rubriques

- [Caractéristiques de AWS Management Console](#)
- [Consoles AWS de service individuelles dans le AWS Management Console](#)
- [Accès au AWS Management Console](#)
- [Accès au AWS Management Console avec des appareils mobiles](#)

Caractéristiques de AWS Management Console

Les caractéristiques importantes de ce AWS Management Console produit sont les suivantes :

- Accédez aux consoles de AWS service : vous pouvez utiliser la navigation unifiée pour accéder aux consoles de service récemment visitées, afficher et ajouter des services à votre liste de favoris, accéder aux paramètres de votre console et y accéder Notifications des utilisateurs AWS.
- Recherchez AWS des services et d'autres AWS informations : utilisez la recherche unifiée pour rechercher AWS des services et des fonctionnalités, ainsi que des produits du AWS marché.
- Personnalisation de la console : vous pouvez utiliser les paramètres unifiés pour personnaliser divers aspects du AWS Management Console. Cela inclut la langue, la région par défaut, etc.
- Exécuter les commandes CLI : AWS CloudShell accessible directement depuis la console. Vous pouvez l'utiliser CloudShell pour exécuter des commandes AWS CLI sur vos services préférés.
- Accédez à toutes les notifications d' AWS événements — Vous pouvez utiliser le AWS Management Console pour accéder aux notifications depuis Notifications des utilisateurs AWS et AWS Health.

- Personnaliser AWS Console Home — Vous pouvez personnaliser complètement votre AWS Console Home expérience à l'aide de widgets.
- Création et gestion AWS des applications : gérez et surveillez le coût, l'intégrité, le niveau de sécurité et les performances de vos applications à l'aide de MyApplications dans AWS Console Home.
- Discutez avec Amazon Q — Vous pouvez obtenir des réponses à vos Service AWS questions grâce à l'intelligence artificielle générative (IA) directement depuis la console. Vous pouvez également vous connecter à un agent en direct pour obtenir une assistance supplémentaire.
- Contrôlez l'accès aux AWS comptes sur votre réseau — Vous pouvez utiliser l'accès AWS Management Console privé pour limiter l'accès AWS Management Console à un ensemble spécifique de AWS comptes connus lorsque le trafic provient de votre réseau.

Consoles AWS de service individuelles dans le AWS Management Console

Chaque AWS service possède sa propre console de service individuelle à laquelle vous pouvez accéder dans le AWS Management Console. Les paramètres que vous choisissez dans les paramètres unifiés AWS Management Console, tels que le mode visuel et la langue par défaut, sont appliqués à toutes les AWS consoles individuelles. AWS les consoles de service proposent un large éventail d'outils pour le cloud computing, ainsi que des informations sur votre compte et sur votre [facturation](#). Si vous souhaitez en savoir plus sur un service spécifique et sa console, par exemple Amazon Elastic Compute Cloud, accédez à sa console à l'aide de la recherche unifiée dans la barre de AWS Management Console navigation et accédez à la EC2 documentation Amazon depuis le [site Web de AWS documentation](#).

Lorsque vous accédez à la console d'un AWS service individuel, vous pouvez toujours accéder aux fonctionnalités d' AWS Management Console utilisation de la navigation unifiée en haut de la console. Vous pouvez laisser des commentaires pour la console d'un service individuel en accédant à cette console et en choisissant Commentaires dans le pied de page de la page.

Accès au AWS Management Console

Vous pouvez accéder AWS Management Console à l'adresse <https://console.aws.amazon.com/>.

Accès au AWS Management Console avec des appareils mobiles

[AWS Management Console](#) est conçu pour fonctionner sur les tablettes ainsi que sur d'autres types d'appareils mobiles :

- L'espace horizontal et vertical est optimisé pour afficher plus d'informations sur votre écran.
- Les boutons et les sélecteurs sont plus grands, pour une meilleure expérience tactile.

Pour y accéder AWS Management Console sur un appareil mobile, vous devez utiliser le AWS Console Mobile Application. Cette application est disponible pour Android et iOS. L'Application Console Mobile fournit des tâches pertinentes pour les appareils mobiles qui complètent parfaitement l'expérience Web. Par exemple, vous pouvez facilement consulter et gérer vos EC2 instances Amazon existantes et vos CloudWatch alarmes Amazon depuis votre téléphone. Pour plus d'informations, voir [Qu'est-ce que le AWS Console Mobile Application ?](#) dans le guide de AWS Console Mobile Application l'utilisateur.

Vous pouvez télécharger l'application Console Mobile [sur Amazon Appstore](#), [Google Play](#) et [iOS App Store](#).

Commencer à utiliser un service dans le AWS Management Console

[AWS Management Console](#) propose différentes manières d'accéder aux consoles de chaque service.

Pour ouvrir la console d'un service

Effectuez l'une des actions suivantes :

- Dans la zone de recherche de la barre de navigation, saisissez tout ou partie du nom du service. Sous Services,, choisissez le service souhaité dans la liste des résultats de recherche. Pour de plus amples informations, veuillez consulter [Vous recherchez des produits, des services, des fonctionnalités et bien plus encore à l'aide de la recherche unifiée dans AWS Management Console](#).
- Dans le widget Recently visited services (Services récemment visités), choisissez un nom de service.
- Dans le widget Services récemment visités, choisissez Afficher tous les AWS services. Ensuite, sur la page Tous les AWS services, choisissez un nom de service.
- Dans la barre de navigation, choisissez Services pour ouvrir une liste complète des services. Ensuite, choisissez un service sous Visité récemment ou Tous les services.

Utilisation de la barre AWS Management Console de navigation via la navigation unifiée

Cette rubrique décrit comment utiliser la navigation unifiée. La navigation unifiée fait référence à la barre de navigation qui fait office d'en-tête et de pied de page de la console. Vous pouvez utiliser la navigation unifiée pour :

- Recherchez et accédez à AWS des services, des fonctionnalités, des produits, etc.
- Lancez AWS Cloudshell.
- Accédez aux AWS notifications et aux événements AWS de santé.
- Obtenez de l'aide auprès de diverses sources de AWS connaissances.
- Configurez le AWS Management Console en choisissant votre langue par défaut, votre mode visuel, votre région, etc.
- Accédez aux informations relatives au compte, à l'organisation, au quota de service et à la facturation.

Rubriques

- [Accès au menu Services dans le AWS Management Console](#)
- [Vous recherchez des produits, des services, des fonctionnalités et bien plus encore à l'aide de la recherche unifiée dans AWS Management Console](#)
- [Lancement AWS CloudShell depuis la barre de navigation du AWS Management Console](#)
- [Accès aux AWS notifications et aux événements de santé](#)
- [Obtention de support](#)
- [Configuration de l' AWS Management Console utilisation des paramètres unifiés](#)
- [Accès à votre AWS compte, à votre organisation, à votre quota de service et à vos informations de facturation dans le AWS Management Console](#)
- [Connexion à plusieurs comptes](#)
- [AWS Actions recommandées dans le AWS Management Console](#)

Accès au menu Services dans le AWS Management Console

Vous pouvez utiliser le menu Services situé à côté de la barre de recherche pour accéder aux services que vous avez récemment visités, consulter votre liste de favoris et consulter tous les AWS services. Vous pouvez également afficher les services par type en choisissant un type de service, par exemple Analytics ou Application Integration.

La procédure suivante décrit comment accéder au menu Services.

Pour accéder au menu Services

1. Connectez-vous à la [AWS Management Console](#).
2. Dans la barre de navigation, choisissez Services ().
3. (Facultatif) Choisissez Visites récentes pour afficher les services et applications avec lesquels vous avez récemment interagi.
4. (Facultatif) Choisissez Favoris pour afficher votre liste de favoris.
5. (Facultatif) Choisissez Toutes les applications pour afficher vos applications MyApplications.
6. (Facultatif) Choisissez Tous les services pour afficher la liste alphabétique de tous les AWS services.
7. (Facultatif) Choisissez un type de service pour afficher AWS les services par type.

Vous recherchez des produits, des services, des fonctionnalités et bien plus encore à l'aide de la recherche unifiée dans AWS Management Console

Le champ de recherche de la barre de navigation fournit un outil de recherche unifié permettant de trouver AWS des services et des fonctionnalités, de la documentation des services, des AWS Marketplace produits, etc. Entrez simplement quelques caractères ou une question pour commencer à générer des résultats à partir de tous les types de contenu disponibles. Chaque mot que vous saisissez affine encore plus vos résultats. Les types de contenu disponibles sont les suivants :

- Services
- Caractéristiques
- Documents

- Blogs
- Articles de connaissances
- Événements
- Tutoriels
- Marketplace
- Ressources

Note

Vous pouvez filtrer les résultats de recherche pour n'afficher que les ressources en effectuant une recherche ciblée. Pour effectuer une recherche ciblée, entrez `/Ressources` au début de votre requête dans la barre de recherche et choisissez `/Ressources` dans le menu déroulant. Entrez ensuite le reste de votre requête.

Rubriques

- [Recherche de AWS produits dans AWS Management Console](#)
- [Affiner votre recherche dans le AWS Management Console](#)
- [Afficher les fonctionnalités d'un service dans AWS Management Console](#)

Recherche de AWS produits dans AWS Management Console

La procédure suivante explique comment rechercher des AWS produits à l'aide de l'outil de recherche.

Pour rechercher un service, une fonctionnalité, une documentation ou un AWS Marketplace produit

1. Dans le champ de recherche de la barre de navigation du [AWS Management Console](#), saisissez votre requête.
2. Choisissez n'importe quel lien pour accéder à votre destination prévue.

Tip

Vous pouvez également utiliser votre clavier pour accéder rapidement au résultat de recherche le plus élevé. Premièrement, appuyez sur Appuyez sur les touches Alt+s

(Windows) ou Option+s (macOS) pour accéder à la barre de recherche. Commencez ensuite à saisir votre terme de recherche. Lorsque le résultat souhaité s'affichera en haut de la liste, appuyez sur la touche Entrée. Par exemple, pour accéder rapidement à la console Amazon EC2, saisissez ec2 et appuyez sur la touche Entrée.

Affiner votre recherche dans le AWS Management Console

Vous pouvez affiner votre recherche par type de contenu et consulter des informations supplémentaires sur les résultats de recherche.

Pour affiner votre recherche en fonction d'un type de contenu spécifique

1. Dans le champ de recherche de la barre de navigation du [AWS Management Console](#), saisissez votre requête.
2. Choisissez l'un des types de contenu à côté des résultats de recherche.
3. (Facultatif) Pour voir tous les résultats d'une catégorie spécifique :
 - Choisissez Afficher plus. Un nouvel onglet s'ouvre pour afficher les résultats.
4. (Facultatif) Pour afficher des informations supplémentaires sur les résultats de votre recherche :
 - a. Dans les résultats de recherche, placez votre curseur sur un résultat de recherche.
 - b. Consultez les informations supplémentaires disponibles.

Afficher les fonctionnalités d'un service dans AWS Management Console

Vous pouvez consulter les fonctionnalités d'un service dans les résultats de recherche.

Pour afficher les fonctionnalités d'un service

1. Dans le champ de recherche de la barre de navigation du [AWS Management Console](#), saisissez votre requête.
2. Dans les résultats de recherche, passez votre curseur sur un service dans Services.
3. Choisissez l'un des liens dans Fonctionnalités principales.

Lancement AWS CloudShell depuis la barre de navigation du AWS Management Console

AWS CloudShell est un shell pré-authentifié basé sur un navigateur que vous pouvez lancer directement depuis la barre de navigation. AWS Management Console Vous pouvez exécuter AWS CLI des commandes sur des services à l'aide de votre shell préféré (shell Bash ou Z). PowerShell

Vous pouvez lancer CloudShell depuis le AWS Management Console en utilisant l'une des deux méthodes suivantes :

- Choisissez l' CloudShell icône dans le pied de page de la console.
- Cliquez sur l' CloudShell icône dans la barre de navigation de la console.

Pour plus d'informations sur ce service, consultez le [Guide de l'utilisateur AWS CloudShell](#).

Pour plus d'informations sur les Régions AWS endroits où ils AWS CloudShell sont disponibles, consultez la [liste des services AWS régionaux](#). La sélection de la région de console est synchronisée avec la CloudShell région. S'il CloudShell n'est pas disponible dans une région sélectionnée, il CloudShell fonctionnera dans la région la plus proche.

Accès aux AWS notifications et aux événements de santé

Vous pouvez accéder à certaines de vos AWS notifications et consulter les événements de santé depuis la barre de navigation. Vous pouvez également accéder Notifications des utilisateurs AWS à toutes vos AWS notifications et au AWS Health tableau de bord depuis la barre de navigation.

Pour plus d'informations, voir [Qu'est-ce que c'est Notifications des utilisateurs AWS ?](#) dans le guide de Notifications des utilisateurs AWS l'utilisateur et [qu'est-ce que c'est AWS Health ?](#) dans le guide de AWS Health l'utilisateur

La procédure suivante décrit comment accéder aux informations de votre AWS événement.

Pour accéder aux informations relatives à votre AWS événement

1. Connectez-vous à la [AWS Management Console](#).
2. Dans la barre de navigation, choisissez l'icône en forme de cloche.
3. Consultez vos notifications et vos événements de santé.

4. (Facultatif) Choisissez Afficher toutes les notifications pour accéder à la Notifications des utilisateurs console.
5. (Facultatif) Choisissez Afficher tous les événements de santé pour accéder à la AWS Health console.

Obtention de support

Vous pouvez obtenir de l'aide en cliquant sur l'icône en forme de point d'interrogation dans la barre de navigation. Dans le menu d'assistance, vous pouvez choisir de :

- Accédez à la console de service du Support Center
- Obtenez l'aide d'un expert d' AWS IQ
- Consultez les connaissances sélectionnées dans les articles de la communauté et dans le centre de connaissances de Re:Post AWS
- Accéder à la AWS documentation
- Accédez aux AWS formations
- Accédez au centre de ressources AWS pour la mise en route
- Laissez des commentaires pour toute console de service à laquelle vous accédez actuellement

Note

Cela peut également être fait en choisissant Feedback dans le pied de page de la console. Le titre du modal qui s'ouvre indique pour quelle console vous êtes en train de laisser des commentaires

Vous pouvez également obtenir de l'aide à tout moment dans la console, vous connecter à un agent en direct et poser des questions AWS en discutant avec AWS Q. Pour de plus amples informations, veuillez consulter [???](#).

Configuration de l' AWS Management Console utilisation des paramètres unifiés

Cette rubrique décrit comment vous configurer à AWS Management Console l'aide de la page des paramètres unifiés pour définir les valeurs par défaut qui s'appliquent à toutes les consoles de service.

Rubriques

- [Configuration des paramètres unifiés dans le AWS Management Console](#)
- [Configuration de régions et de services visibles dans AWS Management Console](#)
- [Choix de votre région](#)
- [Favoris dans le AWS Management Console](#)
- [Modification de votre mot de passe dans AWS Management Console](#)
- [Modification de la langue du AWS Management Console](#)

Configuration des paramètres unifiés dans le AWS Management Console

Vous pouvez configurer les paramètres et les valeurs par défaut, tels que l'affichage, la langue et la région, à partir de la page des paramètres AWS Management Console unifiés. Vous pouvez accéder aux paramètres unifiés via la barre de navigation dans Unified Navigation. Le mode visuel et la langue par défaut peuvent également être définis directement dans la barre de navigation. Ces modifications s'appliqueront à toutes les consoles de service.

Important

Pour garantir la persistance de vos paramètres, de vos services favoris et des services récemment visités dans le monde entier, ces données sont stockées dans tous les pays Régions AWS, y compris dans les régions désactivées par défaut. Ces Régions sont Afrique (Le Cap), Asie-Pacifique (Hong Kong), Asie-Pacifique (Hyderabad), Asie-Pacifique (Jakarta), Europe (Milan), Europe (Espagne), Europe (Zurich), Moyen-Orient (Bahreïn) et Moyen-Orient (EAU). Vous devez toujours [Activer manuellement une région](#) pour y accéder, puis y créer et y gérer des ressources. Si vous ne souhaitez pas enregistrer toutes ces données Régions AWS, choisissez Réinitialiser tout pour effacer vos paramètres, puis désactivez la mémorisation des services récemment visités dans la gestion des paramètres.

Rubriques

- [Accès aux paramètres unifiés dans le AWS Management Console](#)
- [Réinitialisation des paramètres unifiés dans AWS Management Console](#)
- [Modification des paramètres unifiés dans AWS Management Console](#)
- [Modification du mode visuel du AWS Management Console](#)

Accès aux paramètres unifiés dans le AWS Management Console

La procédure suivante décrit comment accéder aux paramètres unifiés.

Pour accéder aux paramètres unifiés

1. Connectez-vous à la [AWS Management Console](#).
2. Dans la barre de navigation, choisissez l'icône représentant une roue dentée (#).
3. Pour ouvrir la page des paramètres unifiés, choisissez Afficher tous les paramètres utilisateur.

Réinitialisation des paramètres unifiés dans AWS Management Console

Vous pouvez supprimer toutes les configurations de paramètres unifiés et restaurer les paramètres par défaut en réinitialisant les paramètres unifiés.

Note

Cela concerne de nombreux domaines AWS, notamment les services favoris dans la navigation et le menu Services, les services récemment visités sur les widgets Console Home et dans le AWS Console Mobile Application, ainsi que tous les paramètres qui s'appliquent à tous les services, tels que la langue par défaut, la région par défaut et le mode visuel.

Pour réinitialiser tous les paramètres unifiés

1. Connectez-vous à la [AWS Management Console](#).
2. Dans la barre de navigation, choisissez l'icône représentant une roue dentée (#).
3. Ouvrez la page des paramètres unifiés en choisissant Afficher tous les paramètres utilisateur.
4. Choisissez Tout réinitialiser.

Modification des paramètres unifiés dans AWS Management Console

La procédure suivante décrit comment modifier vos paramètres préférés.

Pour modifier les paramètres unifiés

1. Connectez-vous à la [AWS Management Console](#).
2. Dans la barre de navigation, choisissez l'icône représentant une roue dentée (#).
3. Ouvrez la page des paramètres unifiés en choisissant Afficher tous les paramètres utilisateur.
4. Choisissez Edit (Modifier) à côté de vos paramètres préférés :
 - Localization and default Region : (Localisation et région par défaut :)
 - Langue vous permet de sélectionner la langue par défaut pour le texte de la console.
 - Default Region (Région par défaut) vous permet de sélectionner une région par défaut qui s'applique chaque fois que vous vous connectez. Vous pouvez sélectionner n'importe laquelle des régions disponibles pour votre compte. Vous pouvez également sélectionner la dernière région utilisée comme région par défaut.

Pour en savoir plus sur le routage des régions dans la [AWS Management Console](#), consultez [Choix d'une région](#).

- Display : (Affichage :)
 - Visual mode (Mode visuel) vous permet de régler votre console dans le mode clair, le mode sombre ou le mode d'affichage par défaut de votre navigateur.

Le mode sombre est une fonctionnalité bêta qui peut ne pas s'appliquer à toutes les consoles de service AWS .

- L'option Affichage de la barre des favoris vous permet de choisir d'afficher le nom complet du service avec son icône ou uniquement l'icône du service dans la barre Favoris.
- L'option Taille de l'icône de la barre des favoris vous permet de choisir entre une taille d'icône de service petite (16 x 16 pixels) ou grande (24 x 24 pixels) dans la barre Favoris.
- Gestion des paramètres :
 - Mémoriser les services récemment visités vous permet de choisir s'il AWS Management Console se souvient des services que vous avez récemment visités. La désactivation de cette option supprime également l'historique des services que vous avez récemment visités, de sorte que vous ne verrez plus les services récemment visités dans le menu Service ou sur les widgets d'accueil de la console. **AWS Console Mobile Application**

5. Sélectionnez Enregistrer les modifications.

Modification du mode visuel du AWS Management Console

Votre mode visuel met votre console en mode clair, en mode sombre ou en mode d'affichage par défaut de votre navigateur.

Pour modifier le mode visuel dans la barre de navigation

1. Connectez-vous à la [AWS Management Console](#).
2. Dans la barre de navigation, choisissez l'icône représentant une roue dentée (#).
3. Pour Mode visuel, choisissez Clair pour le mode clair, Sombre pour le mode sombre ou Paramètre par défaut du navigateur pour le mode d'affichage par défaut de votre navigateur.

Configuration de régions et de services visibles dans AWS Management Console

Les administrateurs de compte peuvent contrôler quels AWS services Régions AWS et quels services sont visibles dans la AWS Management Console navigation. Ces paramètres au niveau du compte sont disponibles dans l'onglet Paramètres du compte de la page des paramètres unifiés. Lorsque vous masquez une région, elle est supprimée du sélecteur de région pour tous les utilisateurs du compte. Lorsque vous masquez un service, il apparaît comme non disponible dans une section distincte du menu Services pour tous les utilisateurs du compte. Les services masqués sont également grisés dans les résultats de recherche unifiée et dans les widgets « Visites récentes » et « Favoris » de la console d'accueil.

Si un utilisateur accède directement à une région ou à un service masqué via une URL, il voit une superposition l'informant que la région ou le service est masqué au niveau du compte.

Note

La navigation vers la page des paramètres unifiés est toujours disponible, de sorte que les administrateurs ne peuvent pas s'empêcher d'accéder à ces paramètres. Si un utilisateur ne dispose pas des autorisations requises ou si le service de personnalisation de AWS l'expérience utilisateur n'est pas disponible, toutes les régions et tous les services sont visibles par défaut.

Rubriques

- [Conditions préalables à la configuration de régions et de services visibles](#)
- [Configuration des régions visibles dans le AWS Management Console](#)
- [Configuration des services visibles dans le AWS Management Console](#)

Conditions préalables à la configuration de régions et de services visibles

Pour afficher et modifier les paramètres des régions et des services visibles, vous avez besoin d'autorisations IAM spécifiques.

- Pour consulter les paramètres, vous devez disposer de cette `uxc:GetAccountCustomizations` autorisation.
- Pour modifier les paramètres, vous avez besoin de l'`uxc:UpdateAccountCustomizations` autorisation.

Les politiques AWS `AWSManagementConsoleBasicUserAccess` gérées `AWSManagementConsoleAdministratorAccess` incluent ces autorisations.

Pour de plus amples informations, veuillez consulter [???](#).

Configuration des régions visibles dans le AWS Management Console

Vous pouvez choisir celles qui Régions AWS apparaissent dans le sélecteur de région pour tous les utilisateurs de votre compte.

Pour configurer les régions visibles

1. Connectez-vous à la [AWS Management Console](#).
2. Dans la barre de navigation, choisissez l'icône représentant une roue dentée (#).
3. Choisissez Afficher tous les paramètres utilisateur pour ouvrir la page des paramètres unifiés.
4. Choisissez l'onglet Paramètres du compte.
5. Pour les régions visibles, cochez les cases correspondant aux régions que vous souhaitez afficher ou décochez-les pour les régions que vous souhaitez masquer.
6. Sélectionnez Enregistrer les modifications.

Après avoir enregistré, les régions masquées sont supprimées du sélecteur de région pour tous les utilisateurs du compte.

Configuration des services visibles dans le AWS Management Console

Vous pouvez choisir les AWS services qui apparaissent dans le menu Services pour tous les utilisateurs de votre compte.

Pour configurer les services visibles

1. Connectez-vous à la [AWS Management Console](#).
2. Dans la barre de navigation, choisissez l'icône représentant une roue dentée (#).
3. Choisissez Afficher tous les paramètres utilisateur pour ouvrir la page des paramètres unifiés.
4. Choisissez l'onglet Paramètres du compte.
5. Pour les services visibles, cochez les cases correspondant aux services que vous souhaitez afficher ou décochez-les pour les services que vous souhaitez masquer.
6. Sélectionnez Enregistrer les modifications.

Une fois que vous avez enregistré, les services masqués apparaissent comme non disponibles dans une section distincte du menu Services pour tous les utilisateurs du compte. Les services masqués sont également grisés dans les résultats de recherche unifiée et dans les widgets « Visites récentes » et « Favoris » de la console d'accueil.

Choix de votre région

Pour de nombreux services, vous pouvez choisir un Région AWS qui indique où vos ressources sont gérées. Les régions sont des ensembles de AWS ressources situés dans la même zone géographique. Vous n'avez pas besoin de choisir une région pour [AWS Management Console](#) ou pour certains services, tels que Gestion des identités et des accès AWS. Pour en apprendre davantage sur les Régions AWS, consultez [Gestion des Régions AWS](#) dans le Références générales AWS.

Note

Si vous avez créé AWS des ressources mais que vous ne les voyez pas dans la console, celle-ci affiche peut-être des ressources d'une autre région. Certaines ressources (par

exemple, les instances Amazon EC2) sont spécifiques à la région dans laquelle elles ont été créées.

Rubriques

- [Choisir une région dans la barre de navigation du AWS Management Console](#)
- [Définition de la région par défaut dans AWS Management Console](#)

Choisir une région dans la barre de navigation du AWS Management Console

La procédure suivante explique comment modifier votre région à partir de la barre de navigation.

Pour choisir une région dans la barre de navigation

1. Connectez-vous à la [AWS Management Console](#).
2. Sur la barre de navigation, choisissez le nom de la région actuellement affichée.
3. Choisissez une région vers laquelle passer.

Définition de la région par défaut dans AWS Management Console

La procédure suivante explique comment modifier votre région par défaut à partir de la page des paramètres unifiés.

Pour définir votre région par défaut

1. Dans la barre de navigation, choisissez l'icône représentant une roue dentée (#).
2. Choisissez Afficher tous les paramètres utilisateur pour accéder à la page des paramètres unifiés.
3. Choisissez Edit (Modifier) à côté de Localization and default Region (Localisation et région par défaut).
4. Dans Région par défaut, choisissez une région.

Note

Si vous ne sélectionnez pas de région par défaut, la dernière région que vous aurez visitée sera votre région par défaut.

5. Choisissez Save settings (Enregistrer les paramètres).
6. (Facultatif) Choisissez Accéder à la nouvelle région par défaut pour accéder immédiatement à votre nouvelle région par défaut.

Favoris dans le AWS Management Console

Pour accéder plus rapidement aux services et applications que vous utilisez fréquemment, vous pouvez enregistrer leurs consoles de service dans une liste de favoris. Vous pouvez ajouter et supprimer des favoris à l'aide du AWS Management Console. Lorsque vous ajoutez un service ou une application à vos favoris, il apparaît dans la barre rapide des favoris.

Rubriques

- [Ajouter des favoris dans AWS Management Console](#)
- [Accès aux favoris dans AWS Management Console](#)
- [Supprimer des favoris dans AWS Management Console](#)

Ajouter des favoris dans AWS Management Console

Vous pouvez ajouter des services et des applications à vos favoris depuis le menu Services et le menu Visites récentes. Vous pouvez également ajouter des services à vos favoris en utilisant la page des résultats de recherche dans le champ de recherche. Les services et applications que vous ajoutez à vos favoris apparaissent dans la barre rapide des favoris.

Rubriques

- [Barre rapide des favoris dans le AWS Management Console](#)
- [Ajouter des services à vos favoris dans le AWS Management Console](#)
- [Ajouter des applications à vos favoris dans le AWS Management Console](#)

Barre rapide des favoris dans le AWS Management Console

La barre rapide des favoris apparaît lorsque vous avez ajouté au moins un AWS service ou une application à vos favoris. La barre rapide des favoris se trouve après la barre de navigation et est visible dans toutes les consoles de AWS service, ce qui vous permet d'accéder rapidement à vos services et applications préférés. Vous pouvez réorganiser l'ordre des services et des applications dans la barre rapide des favoris en faisant glisser un service ou une application vers la gauche ou vers la droite.

Ajouter des services à vos favoris dans le AWS Management Console

Vous pouvez ajouter des services à vos favoris depuis le menu Services ou depuis la page des résultats de recherche depuis le champ de recherche.

Services menu

Pour ajouter des favoris depuis le menu Services

1. Ouvrez la [AWS Management Console](#).
2. Dans la barre de navigation, choisissez Services ().
3. (Facultatif) Ajoutez un service récemment visité à vos favoris :
 - a. Dans Visites récentes, passez votre curseur sur un service.
 - b. Sélectionnez l'étoile à côté du nom du service.
4. Choisissez Tous les services.
5. Passez votre curseur sur le service que vous avez choisi.
6. Sélectionnez l'étoile à côté du nom du service.

Search box

Pour ajouter des favoris depuis le champ de recherche

1. Ouvrez la [AWS Management Console](#).
2. Entrez le nom d'un service dans le champ de recherche.
3. Sur la page des résultats de recherche, sélectionnez l'étoile à côté du nom du service.

Note

Une fois que vous avez ajouté un service à vos favoris, il est ajouté à la barre rapide des favoris après la barre de navigation.

Ajouter des applications à vos favoris dans le AWS Management Console

Vous pouvez ajouter des applications à vos favoris depuis le menu Services.

Pour ajouter des favoris depuis le menu Services

1. Ouvrez la [AWS Management Console](#).
2. Dans la barre de navigation, choisissez Services ().
3. (Facultatif) Ajoutez une application récemment visitée à vos favoris :
 - a. Dans Visites récentes, passez votre curseur sur une application.
 - b. Sélectionnez l'étoile à côté du nom de l'application.
4. Choisissez Applications.
5. Passez le curseur sur l'application que vous avez choisie.
6. Sélectionnez l'étoile à côté du nom de l'application.

Note

Une fois que vous avez ajouté une application à vos favoris, elle est ajoutée à la barre rapide des favoris après la barre de navigation.

Accès aux favoris dans AWS Management Console

Vous pouvez accéder aux services et aux applications ajoutés à vos favoris depuis le menu Services, la barre rapide des favoris et le widget Favoris.

Services menu

Pour accéder à vos favoris depuis le menu Services

1. Ouvrez la [AWS Management Console](#).
2. Dans la barre de navigation, choisissez Services ().
3. Choisissez Favoris.
4. Consultez les services et applications que vous avez ajoutés à vos favoris.
5. (Facultatif) Afficher les ressources de l'application :
 - a. Sélectionnez une application.
 - b. (Facultatif) Sélectionnez une [vue](#).
 - c. Consultez vos ressources.

- d. (Facultatif) Sélectionnez un filtre. Vous pouvez filtrer vos ressources par propriétés ou par balises. Pour plus d'informations, consultez [la section Référence de syntaxe des requêtes de recherche pour Resource Explorer](#) dans le guide de Explorateur de ressources AWS l'utilisateur.
- e. (Facultatif) Sélectionnez une ressource pour l'afficher dans la console de service correspondante.

 Tip

Vous pouvez continuer à parcourir les ressources là où vous vous êtes arrêté en sélectionnant Services (). Les filtres de recherche que vous avez appliqués seront également conservés.

Favorites quickbar

Pour accéder à vos favoris depuis la barre rapide des favoris

1. Ouvrez la [AWS Management Console](#).
2. Consultez les services et applications dans la barre rapide des favoris.

Favorites widget

Pour accéder à vos favoris depuis le widget Favoris

1. Ouvrez la [AWS Management Console](#).
2. (Facultatif) Ajoutez le widget Favoris si vous ne l'avez pas :
 - a. Cliquez sur le bouton + Ajouter des widgets sur la page d'accueil de la console.
 - b. Dans le menu Ajouter des widgets, faites glisser le widget Favoris à l'aide de l'icône et placez-le sur la page d'accueil de votre console.
3. Consultez les services et les applications dans le widget Favoris.

Pour plus d'informations sur les widgets, consultez [the section called "Utilisation de widgets"](#).

Supprimer des favoris dans AWS Management Console

Vous pouvez supprimer des services et des applications de vos favoris à l'aide du menu Services. Vous pouvez également supprimer des services en utilisant la page des résultats de recherche de la barre de recherche.

Services menu

Pour supprimer des favoris du menu Services

1. Ouvrez la [AWS Management Console](#).
2. Dans la barre de navigation, choisissez Services.
3. Choisissez Favoris.
4. Désélectionnez l'étoile à côté du service ou de l'application.

Search box

Note

Actuellement, vous ne pouvez supprimer des services qu'à l'aide de la page des résultats de recherche de la barre de recherche.

Pour supprimer les favoris du champ de recherche

1. Ouvrez la [AWS Management Console](#).
2. Entrez le nom d'un service dans le champ de recherche.
3. Sur la page des résultats de recherche, désélectionnez l'étoile à côté du nom du service.

Modification de votre mot de passe dans AWS Management Console

Vous pouvez peut-être modifier votre mot de passe [AWS Management Console](#) en fonction de votre type d'utilisateur et de vos autorisations. La rubrique suivante décrit comment modifier votre mot de passe pour chaque type d'utilisateur.

Rubriques

- [Router les utilisateurs dans AWS Management Console](#)

- [Les utilisateurs d'IAM dans AWS Management Console](#)
- [Les utilisateurs de l'IAM Identity Center dans le AWS Management Console](#)
- [Les identités fédérées dans le AWS Management Console](#)

Router les utilisateurs dans AWS Management Console

Les utilisateurs root peuvent modifier leur mot de passe directement depuis le AWS Management Console. Un utilisateur root est le propriétaire du compte avec un accès complet à tous les AWS services et ressources. Vous êtes l'utilisateur root si vous avez créé le AWS compte et que vous vous connectez à l'aide de votre adresse e-mail et de votre mot de passe d'utilisateur root. Pour plus d'informations, consultez [la section Utilisateur root](#) dans le Guide de AWS IAM Identity Center l'utilisateur.

Pour modifier votre mot de passe en tant qu'utilisateur root

1. Connectez-vous à la [AWS Management Console](#).
2. Dans la barre de navigation, choisissez le nom de votre compte.
3. Choisissez Informations d'identification de sécurité.
4. Les options affichées varient en fonction de votre Compte AWS type. Suivez les instructions indiquées sur la console pour changer votre mot de passe.
5. Saisissez une fois votre mot de passe actuel et deux fois le nouveau mot de passe.

Le nouveau mot de passe doit comporter au moins huit caractères et inclure les éléments suivants :

- Au moins un symbole
 - Au moins un chiffre
 - Au moins une lettre en majuscules
 - Au moins une lettre en minuscules
6. Choisissez Change Password (Modifier le mot de passe) ou Save changes (Enregistrer les modifications).

Les utilisateurs d'IAM dans AWS Management Console

Les utilisateurs IAM peuvent être en mesure de modifier leur mot de passe en AWS Management Console fonction de leurs autorisations. Dans le cas contraire, ils doivent utiliser un portail AWS

d'accès. Un utilisateur IAM est une identité au sein de votre AWS compte à laquelle des autorisations personnalisées spécifiques ont été accordées. Vous êtes un utilisateur IAM si vous n'avez pas créé le AWS compte et que votre administrateur ou un employé du service d'assistance vous a fourni vos informations de connexion, notamment un identifiant de compte ou un alias de AWS compte, un nom d'utilisateur IAM et un mot de passe. Pour plus d'informations, consultez la section [Utilisateur IAM](#) dans le Guide de l'Connexion à AWS utilisateur.

Si vous disposez d'autorisations conformément à la politique suivante [AWS: Autorise les utilisateurs IAM à modifier leur propre mot de passe de console sur la page Informations d'identification de sécurité](#), vous pouvez modifier votre mot de passe depuis la console. Pour plus d'informations, consultez la section [Comment un utilisateur IAM modifie son propre mot de passe](#) dans le Guide de l'Gestion des identités et des accès AWS utilisateur.

Si vous ne disposez pas des autorisations requises pour modifier votre mot de passe, AWS Management Console consultez la section [Réinitialisation de votre mot de passe AWS IAM Identity Center utilisateur](#) dans le Guide de l'AWS IAM Identity Center utilisateur.

Les utilisateurs de l'IAM Identity Center dans le AWS Management Console

AWS IAM Identity Center les utilisateurs doivent modifier leur mot de passe depuis un portail AWS d'accès. Pour plus d'informations, consultez la section [Réinitialisation de votre mot de passe AWS IAM Identity Center utilisateur](#) dans le guide de AWS IAM Identity Center l'utilisateur.

Un utilisateur du IAM Identity Center est un utilisateur dont le AWS compte fait partie et AWS Organizations qui se connecte via le portail AWS d'accès avec une URL unique. Ces utilisateurs peuvent être créés directement dans les utilisateurs d'IAM Identity Center ou dans Active Directory ou dans un autre fournisseur d'identité externe. Pour plus d'informations, consultez la section [AWS IAM Identity Center utilisateur](#) dans le guide de Connexion à AWS l'utilisateur.

Les identités fédérées dans le AWS Management Console

Les utilisateurs d'identité fédérée doivent modifier leur mot de passe depuis un portail d' AWS accès. Pour plus d'informations, consultez la section [Réinitialisation de votre mot de passe AWS IAM Identity Center utilisateur](#) dans le guide de AWS IAM Identity Center l'utilisateur.

Les utilisateurs d'identité fédérée se connectent à l'aide d'un fournisseur d'identité externe (IdP). Vous êtes une identité fédérée si vous :

- Accédez à votre AWS compte ou à des ressources avec des identifiants tiers tels que Login with Amazon, Facebook ou Google.

- Utilisez les mêmes informations d'identification pour vous connecter aux systèmes et AWS services de l'entreprise et vous pouvez vous connecter à AWS un portail d'entreprise personnalisé.

Pour plus d'informations, consultez la section [Identité fédérée](#) dans le guide de l'Connexion à AWS utilisateur. .

Modification de la langue du AWS Management Console

L' AWS Console Home expérience inclut la page des paramètres unifiés où vous pouvez modifier la langue par défaut pour les AWS services dans le AWS Management Console. Vous pouvez également modifier rapidement la langue par défaut dans le menu des paramètres de la barre de navigation.

Note

Les procédures suivantes modifient la langue de toutes les consoles AWS de service, mais pas celle de AWS la documentation. Pour changer la langue utilisée pour la documentation, utilisez le menu des langues en haut à droite de la page de la documentation.

Rubriques

- [Langues prises en charge](#)
- [Modification de la langue par défaut depuis la barre de navigation du AWS Management Console](#)
- [Modification de la langue par défaut via les paramètres unifiés dans le AWS Management Console](#)

Langues prises en charge

Les langues suivantes AWS Management Console sont actuellement prises en charge :

- Anglais (États-Unis)
- Anglais (Royaume-Uni)
- Bahasa Indonésie
- Allemand
- Espagnol
- Français
- Japonais

- Italien
- Portugais
- Coréen
- Chinois (simplifié)
- Chinois (Traditionnel)
- Turc

Modification de la langue par défaut depuis la barre de navigation du AWS Management Console

La procédure suivante explique comment modifier votre langue par défaut directement depuis la barre de navigation.

Pour modifier la langue par défaut dans la barre de navigation

1. Connectez-vous à la [AWS Management Console](#).
2. Dans la barre de navigation, choisissez l'icône représentant une roue dentée (#).
3. Pour Langue, choisissez Paramètre par défaut du navigateur ou votre langue préférée dans la liste déroulante.

Modification de la langue par défaut via les paramètres unifiés dans le AWS Management Console


La procédure suivante explique comment modifier votre langue par défaut depuis la page des paramètres unifiés.

Pour changer la langue par défaut dans Paramètres unifiés

1. Connectez-vous à la [AWS Management Console](#).
2. Dans la barre de navigation, choisissez l'icône représentant une roue dentée (#).
3. Pour ouvrir la page des paramètres unifiés, choisissez Afficher tous les paramètres utilisateur.
4. Dans Unified Settings (Paramètres unifiés), choisissez Edit (Modifier) à côté de Localization and default Region (Localisation et région par défaut).
5. Pour sélectionner la langue que vous souhaitez utiliser pour la console, choisissez l'une des options suivantes :

- Choisissez le Paramètre par défaut du navigateur dans la liste déroulante, puis Enregistrer les paramètres.

Le texte de la console pour tous les AWS services apparaît dans la langue préférée que vous avez définie dans les paramètres de votre navigateur.

 Note


Par défaut, le navigateur ne prend en charge que les langues prises en charge par la AWS Management Console.

- Choisissez la langue préférée dans la liste déroulante, puis Enregistrer les paramètres.

Le texte de la console pour tous les AWS services apparaît dans la langue de votre choix.

Accès à votre AWS compte, à votre organisation, à votre quota de service et à vos informations de facturation dans le AWS Management Console

Si vous disposez des autorisations nécessaires, vous pouvez accéder aux informations relatives à votre AWS compte, aux quotas de service, à l'organisation et aux informations de facturation depuis la console.

 Note

Le AWS Management Console seul donne accès au compte, à l'organisation, au quota de service et aux informations de facturation. Ces services disposent de leurs propres consoles distinctes. Pour plus d'informations, consultez les ressources suivantes :

- [Gérez votre AWS compte](#) dans le guide Gestion de compte AWS de référence.
- [Qu'est-ce que c'est AWS Organizations ?](#) dans le guide de AWS Organizations l'utilisateur.
- [Qu'est-ce que les Quotas de Service ?](#) dans le Guide de l'utilisateur du Service Quotas.
- [À l'aide de la page d' AWS Billing and Cost Management accueil](#) du guide AWS de l'utilisateur de facturation.

i Tip

Vous pouvez également obtenir plus d'informations sur l'un de ces sujets en vous adressant à Amazon Q. Pour plus d'informations, consultez [Chat avec un développeur Amazon Q](#).

Rubriques

- [Accès aux informations du compte dans le AWS Management Console](#)
- [Accès aux informations relatives à l'organisation dans le AWS Management Console](#)
- [Accès aux informations relatives aux quotas de service dans le AWS Management Console](#)
- [Accès aux informations de facturation dans le AWS Management Console](#)

Accès aux informations du compte dans le AWS Management Console

Si vous disposez des autorisations nécessaires, vous pouvez accéder aux informations relatives à votre AWS compte depuis la console.

Pour accéder aux informations de votre compte

1. Connectez-vous à la [AWS Management Console](#).
2. Sur la barre de navigation, choisissez le nom de votre compte.
3. Choisissez Account.
4. Consultez les informations de votre compte.

i Note

Si vous souhaitez fermer votre AWS compte, consultez la section [Fermer un AWS compte](#) dans le Guide de Gestion de compte AWS référence.

Accès aux informations relatives à l'organisation dans le AWS Management Console

Si vous disposez des autorisations nécessaires, vous pouvez accéder aux informations relatives à vos AWS organisations depuis la console.

Pour accéder aux informations de l'organisation

1. Connectez-vous à la [AWS Management Console](#).
2. Sur la barre de navigation, choisissez le nom de votre compte.
3. Choisissez Organizations.
4. Consultez les informations de votre organisation.

Accès aux informations relatives aux quotas de service dans le AWS Management Console

Si vous disposez des autorisations nécessaires, vous pouvez accéder aux informations relatives aux quotas de service depuis la console.

Pour accéder aux informations sur les quotas de service

1. Connectez-vous à la [AWS Management Console](#).
2. Sur la barre de navigation, choisissez le nom de votre compte.
3. Choisissez Service Quotas (Quotas de service).
4. Consultez et gérez les informations relatives à vos quotas de service.

Accès aux informations de facturation dans le AWS Management Console

Si vous disposez des autorisations nécessaires, vous pouvez accéder aux informations relatives à vos AWS frais depuis la console.

Pour accéder à vos informations de facturation

1. Connectez-vous à la [AWS Management Console](#).
2. Sur la barre de navigation, choisissez le nom de votre compte.
3. Choisissez Billing and Cost Management.
4. Utilisez le AWS Billing and Cost Management tableau de bord pour trouver un résumé et une ventilation de vos dépenses mensuelles.

Connexion à plusieurs comptes

Vous pouvez vous connecter à un maximum de cinq identités différentes simultanément dans un seul navigateur Web dans le AWS Management Console. Il peut s'agir de n'importe quelle combinaison de rôles root, IAM ou fédérés dans différents comptes ou dans le même compte. Chaque identité à laquelle vous vous connectez ouvre sa propre instance AWS Management Console dans un nouvel onglet.

Lorsque vous activez la prise en charge multissession, l'URL de la console contient un sous-domaine (par exemple, <https://000000000000-aaaaaaa.us-east-1.console.aws.amazon.com/console/home?region=us-east-1>). Assurez-vous de mettre à jour vos favoris et vos liens vers la console.

Note

[Vous devez souscrire à l'assistance multissession en choisissant Activer la multissession dans le menu du compte ou en choisissant Activer la AWS Management Console multissession sur/ <https://console.aws.amazon.com>](#) Vous pouvez désactiver les sessions multiples à tout moment en choisissant Désactiver les sessions multiples <https://console.aws.amazon.comsur/> ou en effaçant les cookies de votre navigateur. L'opt-in est spécifique au navigateur.

Pour vous connecter à plusieurs identités

1. Connectez-vous à la [AWS Management Console](#).
2. Dans la barre de navigation, choisissez le nom de votre compte.
3. Choisissez Ajouter une session, puis cliquez sur Se connecter. Un nouvel onglet s'ouvrira pour vous permettre de vous connecter.

Note

Pour plus d'informations sur la connexion en tant qu'utilisateur root ou IAM, consultez la section [Se connecter AWS Management Console au guide](#) de l'utilisateur de AWS connexion.

4. Saisissez vos informations d'identification .

5. Choisissez Sign in (Connexion). Les AWS Management Console charges dans cet onglet correspondent à l' AWS identité que vous avez choisie.
6. (Facultatif) Pour créer des rôles supplémentaires
 - a. Dans le portail AWS IAM Identity Center d'accès ou sur votre portail d'authentification unique (SSO), connectez-vous au rôle supplémentaire.
 - b. Dans le, AWS Management Console choisissez le nom de votre compte.
 - c. Consultez les sessions supplémentaires que vous pouvez choisir.

AWS Actions recommandées dans le AWS Management Console

AWS Les actions recommandées vous aident à travailler plus efficacement dans le domaine en AWS Management Console fournissant des suggestions contextuelles pour effectuer les tâches et mettre en œuvre les meilleures pratiques. Lorsque des recommandations pertinentes sont disponibles, un bouton dynamique apparaît que vous pouvez utiliser pour agir rapidement en fonction de ces suggestions.

Note

AWS Recommended Actions analyse l'état des ressources pour fournir des suggestions, mais ne traite pas les données utilisateur.

Rubriques

- [Caractéristiques des actions AWS recommandées](#)
- [Utilisation des actions recommandées](#)
- [Enregistrement des appels d'API relatifs aux actions AWS recommandées à l'aide de AWS CloudTrail](#)

Caractéristiques des actions AWS recommandées

- Recommandations d'action — Obtenez des suggestions pertinentes en fonction de l'état des ressources, des meilleures pratiques et des modèles d'utilisation courants
- Actions en un clic : effectuez les actions recommandées directement à partir des messages de réussite ou des affichages de ressources

- Panneau latéral droit intégré — Accédez à un panneau latéral intégré pour mettre en œuvre les suggestions sans perturber votre flux de travail
- Support multiservice : obtenez des recommandations sur plusieurs AWS services

Utilisation des actions recommandées

Pour utiliser les actions recommandées

1. Connectez-vous au [AWS Management Console](#)
2. Recherchez le bouton # Actions recommandées.

Note

Le bouton des actions recommandées peut apparaître n'importe où dans le AWS Management Console et n'est accessible que lorsque les actions recommandées sont disponibles.

3. Cliquez sur le bouton pour afficher les actions disponibles.
4. Exécutez les recommandations directement ou via le panneau latéral.

Enregistrement des appels d'API relatifs aux actions AWS recommandées à l'aide de AWS CloudTrail

AWS Les actions recommandées sont intégrées à [AWS CloudTrail](#) un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un Service AWS. CloudTrail capture tous les appels d'API pour les actions AWS recommandées sous forme d'événements. Les appels capturés incluent les appels provenant des appels de code AWS Management Console et vers les opérations de l'API Actions AWS recommandées. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été envoyée à AWS Recommended Actions, l'adresse IP à partir de laquelle la demande a été faite, la date à laquelle elle a été faite et des informations supplémentaires.

CloudTrail est actif dans votre compte Compte AWS lorsque vous créez le compte et vous avez automatiquement accès à l'historique des CloudTrail événements. L'historique des CloudTrail événements fournit un enregistrement consultable, consultable, téléchargeable et immuable des 90 derniers jours des événements de gestion enregistrés dans un. Région AWS Pour plus

d'informations, consultez la section [Utilisation de l'historique des CloudTrail événements](#) dans le guide de AWS CloudTrail l'utilisateur. La consultation de CloudTrail l'historique des événements est gratuite.

Pour un enregistrement continu des événements de vos 90 Compte AWS derniers jours, créez un magasin de données sur les événements de Trail ou [CloudTrailLake](#).

AWS Événements de gestion des actions recommandées dans CloudTrail

[Les événements de gestion](#) fournissent des informations sur les opérations de gestion effectuées sur les ressources de votre Compte AWS. Ils sont également connus sous le nom opérations de plan de contrôle. Par défaut, CloudTrail enregistre les événements de gestion.

AWS Les actions recommandées enregistrent toutes les opérations du plan de contrôle des actions AWS recommandées en tant qu'événements de gestion.

AWS Exemples d'événements relatifs aux actions recommandées

Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'opération d'API demandée, la date et l'heure de l'opération, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics. Les événements n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre un CloudTrail événement illustrant l'opération.

```
{
  "awsRegion": "us-east-2",
  "eventCategory": "Management",
  "eventID": "3510a29e-8070-4cbc-b6a0-9e11f18e26ec",
  "eventName": "ListRecommendedActions",
  "eventSource": "action-recommendations.amazonaws.com",
  "eventTime": "2025-09-03T03:52:02Z",
  "eventType": "AwsApiCall",
  "eventVersion": "1.09",
  "managementEvent": true,
  "readOnly": true,
  "recipientAccountId": "123456789098",
  "requestID": "ec431c91-0315-413d-bdb6-d282fd4f6d83",
  "requestParameters": {
    "context": "*",
    "uxChannel": "EXAMPLE"
  }
},
```

```
"responseElements": null,
"sourceIPAddress": "192.0.2.0",
"userAgent": "EXAMPLE",
"userIdentity": {
  "type": "AssumedRole",
  "principalId": "AROARZDBH75ZCUYWFSTUS:EXAMPLE",
  "arn": "arn:aws:sts::123456789098:assumed-role/EXAMPLE",
  "accountId": "12345678909",
  "accessKeyId": "ASIAZDBEXAMPLE",
  "sessionContext": {
    "sessionIssuer": {
      "type": "Role",
      "principalId": "AROARZDBHEXAMPLE",
      "arn": "arn:aws:iam::12345678909:role/EXAMPLE",
      "accountId": "12345678909",
      "userName": "EXAMPLE"
    },
    "attributes": {
      "creationDate": "2025-09-03T03:52:00Z",
      "mfaAuthenticated": "false"
    }
  },
  "invokedBy": "action-recommendations.amazonaws.com"
}
```

Pour plus d'informations sur le contenu des CloudTrail enregistrements, voir [le contenu des CloudTrail enregistrements](#) dans le Guide de AWS CloudTrail l'utilisateur.

En utilisant AWS Console Home dans le AWS Management Console

Cette rubrique décrit comment l'utiliser AWS Console Home, notamment comment personnaliser la page d'accueil de votre console. La page d'accueil de la console est la page d'accueil du AWS Management Console. Lorsque vous vous connectez pour la première fois à la console, vous arrivez sur la page d'accueil de la console. Vous pouvez personnaliser la page d'accueil de votre console à l'aide de widgets et d'applications. Les widgets vous permettent d'ajouter des composants personnalisés qui suivent les informations relatives à vos AWS services et ressources. Les applications vous permettent de regrouper vos AWS ressources et vos métadonnées. Vous pouvez gérer les applications à l'aide de MyApplications. Vous pouvez également utiliser la console d'accueil pour consulter la liste de tous les AWS services et discuter avec Amazon Q.

Rubriques

- [Afficher tous les AWS services dans AWS Console Home](#)
- [Utilisation de widgets dans AWS Console Home](#)
- [À quoi sert MyApplications ? AWS Console Home](#)
- [Discuter avec le développeur Amazon Q dans AWS Console Home](#)

Afficher tous les AWS services dans AWS Console Home

Vous pouvez consulter la liste de tous les AWS services et accéder à leurs consoles depuis Console Home.

Pour accéder à la liste complète des AWS services

1. Connectez-vous à la [AWS Management Console](#).
2. Développez le menu d'accueil de la console en choisissant l'icône du hamburger (☰).
3. Choisissez Tous les services.
4. Sélectionnez un AWS service pour accéder à sa console.

Utilisation de widgets dans AWS Console Home

Le tableau de bord de la console d'accueil inclut des widgets qui affichent des informations importantes sur votre AWS environnement et fournissent des raccourcis vers vos services. Vous pouvez personnaliser votre expérience en ajoutant et en supprimant des widgets, en les réorganisant ou en modifiant leur taille.

Gestion des widgets

Vous pouvez gérer les widgets en les ajoutant, en les supprimant, en les réorganisant et en les redimensionnant. Les widgets par défaut peuvent être supprimés et ajoutés à nouveau. Vous pouvez également rétablir la disposition par défaut de votre console d'accueil et demander de nouveaux widgets.

Pour ajouter un widget

1. En haut ou en bas à droite du tableau de bord Page d'accueil de la console, cliquez sur le bouton **+Ajouter des widgets**
2. Choisissez l'indicateur de glissement, représenté par six points verticaux (⋮) dans le coin supérieur gauche de la barre de titre du widget, puis faites-le glisser vers le tableau de bord de votre console d'accueil.

Pour supprimer un widget

1. Choisissez l'ellipse, représentée par trois points verticaux (⋮) dans le coin supérieur droit de la barre de titre du widget.
2. Choisissez **Remove widget (Supprimer le widget)**.

Pour réorganiser vos widgets

- Choisissez l'indicateur de glissement, représenté par six points verticaux (⋮) dans le coin supérieur gauche de la barre de titre du widget, puis faites glisser le widget vers un nouvel emplacement sur le tableau de bord de votre console d'accueil.

Pour redimensionner un widget

- Sélectionnez l'icône de redimensionnement en bas à droite du widget, puis effectuez un glissement pour redimensionner le widget.

Si vous souhaitez reprendre à zéro l'organisation et la configuration de vos widgets, vous pouvez rétablir la disposition par défaut du tableau de bord Page d'accueil de la console. Vos modifications seront alors annulées, le tableau de bord Page d'accueil de la console reprendra sa disposition d'origine, et tous les widgets retrouveront leur emplacement et leur taille par défaut.

Pour rétablir la disposition par défaut de la page

1. Cliquez sur le bouton Réinitialiser la mise en page par défaut dans la partie supérieure droite de la page.
2. Pour confirmer, choisissez Réinitialiser.

Note

Cette action annulera toutes les modifications que vous avez apportées à la disposition du tableau de bord Page d'accueil de la console.

Pour demander un nouveau widget dans le tableau de bord Page d'accueil de la console

1. En bas à gauche du tableau de bord Page d'accueil de la console, sélectionnez Vous voulez voir un autre widget ? Dites-le-nous !

Décrivez le widget que vous souhaitez voir figurer dans le tableau de bord Page d'accueil de la console.

2. Sélectionnez Soumettre.

Note

Nous examinons régulièrement vos suggestions et nous pouvons ajouter de nouveaux widgets dans les futures mises à jour de la AWS Management Console.

À quoi sert MyApplications ? AWS Console Home

myApplications est une extension de la page d'accueil de la console qui vous permet de gérer et de surveiller le coût, l'état, le niveau de sécurité et les performances de vos applications sur AWS. Les applications vous permettent de regrouper les ressources et les métadonnées. Vous pouvez accéder à toutes les applications de votre compte, aux indicateurs clés de toutes les applications, ainsi qu'à une vue d'ensemble des indicateurs de coûts, de sécurité et d'exploitation et aux informations provenant de plusieurs consoles de service à partir d'une seule vue dans le AWS Management Console. MyApplications inclut les éléments suivants :

- Widget d'applications sur la page d'accueil de la console
- myApplications que vous pouvez utiliser pour afficher les coûts des ressources des applications et les résultats de sécurité
- Tableau de bord myApplications qui fournit une vue des métriques clés des applications, telles que les coûts, les performances et les résultats de sécurité

Rubriques

- [Fonctionnalités de myApplications](#)
- [Services connexes](#)
- [Accès à myApplications](#)
- [Tarification](#)
- [Régions prises en charge pour MyApplications](#)
- [Applications dans MyApplications](#)
- [Ressources disponibles dans MyApplications](#)
- [Tableau de bord MyApplications dans AWS Console Home](#)

Fonctionnalités de myApplications

- Créer des applications : créez de nouvelles applications et organisez leurs ressources. Vos applications sont automatiquement affichées dans MyApplications, afin que vous puissiez agir dans les CLI AWS Management Console APIs,, et SDKs. L'infrastructure en tant que code (IaC) est générée lorsque vous créez une application et accessible depuis le tableau de bord myApplications. IaC est utilisable dans les outils IaC, notamment AWS CloudFormation Terraform.

- Accéder à vos applications : vous pouvez accéder rapidement à n'importe laquelle de vos applications à partir du widget myApplications en le sélectionnant.
- Accédez à vos ressources : vous pouvez consulter rapidement les ressources de votre application dans le menu Services en sélectionnant l'application. Lorsque vous sélectionnez une ressource, vous accédez directement à la console de service correspondante. Votre place dans le tableau des ressources est enregistrée. Vous pouvez donc continuer à naviguer à tout moment depuis le menu Services.
- Comparer des métriques d'applications : utilisez myApplications pour comparer des métriques clés des applications, telles que le coût des ressources des applications et le nombre de résultats de sécurité critiques pour plusieurs applications.
- Surveillez et gérez les applications : évaluez l'état et les performances des applications à l'aide d'alarmes, de canaris, d'objectifs de niveau de service Amazon CloudWatch AWS Security Hub CSPM, de conclusions et d'tendances en matière de AWS Cost Explorer Service coûts. Vous pouvez également trouver des résumés et des optimisations des métriques de calcul et gérer la conformité des ressources et l'état de configuration sur. AWS Systems Manager

Services connexes

myApplications utilise les services suivants :

- AppRegistry
- AppManager
- Amazon CloudWatch
- Amazon EC2
- AWS Lambda
- Explorateur de ressources AWS
- AWS Security Hub CSPM
- Systems Manager
- AWS Service Catalog
- Identification

Accès à myApplications

Vous pouvez accéder à myApplications depuis la [AWS Management Console](#) en choisissant myApplications dans la barre latérale gauche.

Tarification

MyApplications on AWS est proposé sans frais supplémentaires. Il n'y a pas de frais d'installation ni d'engagement initial. Les frais d'utilisation des ressources et des services sous-jacents résumés dans le tableau de bord myApplications s'appliquent toujours aux tarifs publiés pour ces ressources.

Régions prises en charge pour MyApplications

MyApplications est disponible dans les formats suivants : Régions AWS

- USA Est (Ohio)
- USA Est (Virginie du Nord)
- USA Ouest (Californie du Nord)
- USA Ouest (Oregon)
- Asie-Pacifique (Mumbai)
- Asie-Pacifique (Osaka)
- Asia Pacific (Seoul)
- Asie-Pacifique (Singapour)
- Asie-Pacifique (Sydney)
- Asie-Pacifique (Tokyo)
- Canada (Centre)
- Europe (Francfort)
- Europe (Irlande)
- Europe (Londres)
- Europe (Paris)
- Europe (Stockholm)
- Amérique du Sud (São Paulo)

Régions d'activation

Les régions d'activation ne sont pas activées par défaut. Vous devez activer manuellement ces régions pour les utiliser avec myApplications. Pour plus d'informations à ce sujet Régions AWS, consultez [la section Gestion Régions AWS](#). Les régions d'adhésion suivantes sont prises en charge :

- Afrique (Le Cap)
- Asie-Pacifique (Hong Kong)
- Asie-Pacifique (Hyderabad)
- Asie-Pacifique (Jakarta)
- Asie-Pacifique (Melbourne)
- Europe (Milan)
- Europe (Espagne)
- Europe (Zurich)
- Middle East (Bahrain)
- Moyen-Orient (EAU)
- Israël (Tel Aviv)

Applications dans MyApplications

Les applications vous permettent de regrouper vos ressources et vos métadonnées. Vous pouvez gérer vos applications en les créant, en les intégrant, en les visualisant, en les modifiant ou en les supprimant. Vous pouvez également créer des extraits de code pour ajouter automatiquement de nouvelles ressources à une application.

Note

Vous pouvez également ajouter des applications à vos favoris pour en faciliter l'accès. Pour de plus amples informations, veuillez consulter [???](#).

Rubriques

- [Création d'applications dans MyApplications](#)
- [Intégrer des AppRegistry applications existantes dans MyApplications](#)

- [Affichage des applications dans MyApplications](#)
- [Modification d'applications dans MyApplications](#)
- [Supprimer des applications dans MyApplications](#)
- [Création d'extraits de code dans MyApplications](#)

Création d'applications dans MyApplications

Vous pouvez créer une nouvelle application ou la [the section called “Applications d'intégration”](#) créer avant le 8 novembre 2023 pour commencer à utiliser MyApplications. Lorsque vous créez une nouvelle application, vous pouvez ajouter des ressources en les recherchant et en les sélectionnant ou en utilisant des balises existantes.

Pour créer une application

1. Connectez-vous à la [AWS Management Console](#).
2. Développez la barre latérale gauche et choisissez MyApplications.
3. Choisissez Créer une application.
4. Entrez un nom d'application.
5. (Facultatif) Entrez une description de l'application.
6. (Facultatif) Ajoutez des [balises](#). Les balises sont des paires clé-valeur qui sont appliquées à des ressources pour contenir des métadonnées concernant ces ressources.

Note

La balise AWS d'application est automatiquement appliquée aux applications nouvellement créées. Pour plus d'informations, consultez [la section La balise AWS d'application](#) dans le guide de AWS Service Catalog AppRegistry l'administrateur.

7. (Facultatif) Ajoutez des [groupes d'attributs](#). Vous pouvez utiliser des groupes d'attributs pour stocker les métadonnées des applications.
8. Choisissez Suivant.
9. (Facultatif) Ajoutez des ressources :

Search and select resources

Note

Pour rechercher et ajouter des ressources, vous devez activer Explorateur de ressources AWS. Pour plus d'informations, consultez la section [Mise en route avec Explorateur de ressources AWS](#).

Toutes les ressources ajoutées sont étiquetées avec la balise AWS d'application.

Pour ajouter des ressources à l'aide de la recherche

1. Choisissez Rechercher, puis sélectionnez les ressources.
2. Choisissez Sélectionner les ressources.
3. (Facultatif) Choisissez une [vue](#).
4. Recherchez vos ressources. Vous pouvez effectuer une recherche par mot-clé, nom ou type, ou choisir un type de ressource.

Note

Si vous ne trouvez pas la ressource que vous recherchez, effectuez un dépannage avec Explorateur de ressources AWS. Pour plus d'informations, consultez [Résolution des problèmes de recherche de Resource Explorer](#) dans le Guide de l'utilisateur de Resource Explorer.

5. Cochez la case à côté des ressources que vous souhaitez ajouter.
6. Choisissez Ajouter.
7. Choisissez Suivant.
8. Vérifiez vos choix.

Automatically add resources using tags

Lorsque vous créez une application, vous pouvez intégrer des ressources en bloc en spécifiant une paire clé-valeur de balise existante. Avec cette méthode, applique AWS automatiquement la `awsApplication` balise à toutes les ressources étiquetées avec la paire clé-valeur spécifiée et crée une synchronisation des balises pour les ressources

de l'application par défaut. Lorsque la synchronisation des balises est activée, toutes les ressources étiquetées avec la paire clé-valeur de balise spécifiée sont automatiquement ajoutées à l'application. Pour plus d'informations sur la résolution des erreurs de synchronisation des balises, consultez [the section called “Résolution des erreurs de synchronisation des balises dans MyApplications”](#)

Note


L'ajout de ressources à une application à l'aide de balises nécessite des autorisations pour créer une AppRegistry application, regrouper et dissocier les ressources, ainsi que pour étiqueter et débaliser les ressources. Vous pouvez soit ajouter la politique [ResourceGroupsTaggingAPITagUntagSupportedResources](#) AWS gérée par Resource Groups, soit créer et gérer votre propre politique personnalisée. Les autorisations suivantes doivent être ajoutées à la déclaration de politique d'un utilisateur dans IAM :

- `servicecatalog:CreateApplication`
- `resource-groups:GroupResources`
- `resource-groups:UngroupResources`
- `tag:TagResources`
- `tag:UntagResources`

Pour ajouter des ressources à l'aide de balises existantes


1. Choisissez Ajouter automatiquement des ressources à l'aide de balises.
2. Sélectionnez une clé de balise et une valeur existantes :
 - a. Sélectionnez le rôle utilisé pour étiqueter les ressources. Pour plus d'informations, consultez la section [Autorisations requises pour la synchronisation des balises](#) dans le Guide de l' AppRegistry administrateur du AWS Service Catalog.
 - b. Sélectionnez une clé Tag.
 - c. Sélectionnez une valeur de tag.
 - d. (Facultatif) Choisissez Prévisualiser les ressources pour prévisualiser les ressources étiquetées avec la paire clé-valeur du tag.

- e. Lisez et acceptez le Je reconnais que les événements du cycle de vie du groupe seront activés pour créer un avis de synchronisation des balises. GLE permet AWS de remarquer les modifications apportées aux ressources étiquetées avec votre paire clé-valeur.
3. Choisissez Suivant.
4. Passez en revue les détails de votre application, la paire clé-valeur de balise sélectionnée et l'aperçu des ressources qui seront ajoutées à l'application.

 Note

Par défaut, la création d'une application à l'aide d'une paire clé-valeur de balise existante crée une synchronisation de balises. Après l'installation, tag-sync gère également en permanence les ressources de l'application, en ajoutant ou en supprimant des ressources lorsqu'elles sont étiquetées ou non avec la paire clé-valeur spécifiée. Vous pouvez gérer la synchronisation des balises depuis la page Gérer les ressources de l'application.

10. Si vous CloudFormation associez une pile, cochez la case en bas de page.

 Note

L'ajout d'une CloudFormation pile à l'application nécessite une mise à jour de la pile, car toutes les ressources ajoutées à votre application sont étiquetées avec la balise AWS d'application. Les configurations manuelles effectuées après la dernière mise à jour de la pile peuvent ne pas être reflétées après cette mise à jour. Cela peut entraîner des interruptions de service ou d'autres problèmes liés aux applications. Pour plus d'informations, consultez [Comportements de mise à jour des ressources d'une pile](#) dans le Guide de l'utilisateur CloudFormation .

11. Choisissez Créer une application.

Intégrer des AppRegistry applications existantes dans MyApplications

Vous pouvez intégrer une AppRegistry application existante créée avant le 8 novembre 2023 pour commencer à utiliser MyApplications.

Pour intégrer une AppRegistry application existante

1. Connectez-vous à la [AWS Management Console](#).
2. Dans la barre latérale gauche, choisissez myApplications.
3. Utilisez la barre de recherche pour trouver votre application.
4. Sélectionnez votre application.
5. Choisissez Onboard **application name**.
6. Si vous CloudFormation associez une pile, cochez la case dans la zone d'alerte.
7. Choisissez Intégrer l'application.

Affichage des applications dans MyApplications

Vous pouvez consulter vos candidatures à partir de MyApplications ou du menu Services. Si vous consultez vos candidatures depuis MyApplications, vous pouvez les consulter sous forme de carte Régions AWS ou de tableau sous forme de carte ou de tableau, dans leur ensemble ou dans des informations spécifiques Régions AWS .

Note

Vous pouvez également consulter les applications ajoutées à vos favoris dans le menu des favoris. Pour de plus amples informations, veuillez consulter [Favoris dans le AWS Management Console](#).

myApplications

Pour consulter les candidatures dans MyApplications

1. Ouvrez la [AWS Management Console](#).
2. Dans la barre latérale gauche, choisissez myApplications.
3. Dans Régions, sélectionnez Région actuelle ou Régions prises en charge.
4. Pour trouver une application spécifique, entrez son nom, ses mots-clés ou sa description dans la barre de recherche.
5. (Facultatif) Votre affichage par défaut est sous forme de carte. Pour personnaliser votre page d'application :

- a. Sélectionnez l'icône d'engrenage.
- b. (Facultatif) Sélectionnez la taille de votre page.
- c. (Facultatif) Choisissez l'affichage sous forme de carte ou de tableau.
- d. (Facultatif) Sélectionnez la taille de votre page.
- e. (Facultatif) Si vous utilisez la vue tabulaire, sélectionnez les propriétés de cette vue tabulaire.
- f. (Facultatif) Indiquez quelles propriétés de l'application sont visibles et l'ordre dans lequel elles apparaissent.
- g. Choisissez Confirmer.

Services menu

Pour consulter les applications depuis le menu Services

1. Ouvrez la [AWS Management Console](#).
2. Dans la barre de navigation, choisissez Services ().
3. Choisissez Toutes les applications.
4. Sélectionnez une application.
5. (Facultatif) Sélectionnez une [vue](#).
6. (Facultatif) Sélectionnez un filtre. Vous pouvez filtrer vos ressources par propriétés ou par balises. Pour plus d'informations, consultez [la section Référence de syntaxe des requêtes de recherche pour Resource Explorer](#) dans le guide de Explorateur de ressources AWS l'utilisateur.
7. (Facultatif) Sélectionnez une ressource pour l'afficher dans la console de service correspondante.

Tip

Vous pouvez continuer à parcourir les ressources là où vous vous êtes arrêté en sélectionnant Services (). Les filtres de recherche que vous avez appliqués seront également conservés.

Modification d'applications dans MyApplications

La modification de votre application s'ouvre AppRegistry pour que vous puissiez mettre à jour sa description. Vous pouvez également l'utiliser AppRegistry pour modifier les balises et les groupes d'attributs de votre application.

Pour modifier une application

1. Ouvrez la [AWS Management Console](#).
2. Dans la barre latérale gauche de la console, choisissez myApplications.
3. Sélectionnez l'application que vous souhaitez modifier.
4. Sur le tableau de bord MyApplication, choisissez Actions, puis sélectionnez Modifier l'application.
5. Dans Modifier l'application, apportez les modifications souhaitées à la description, aux balises et aux groupes d'attributs de votre application.

Note

Pour plus d'informations sur la gestion des balises et des groupes d'attributs, consultez les [sections Gestion des balises](#) et [Modification des groupes d'attributs](#) dans le guide de l'AWS Service Catalog AppRegistry administrateur.

6. Choisissez Mettre à jour.

Supprimer des applications dans MyApplications

Vous pouvez supprimer des applications lorsqu'elles ne sont plus requises. Avant de supprimer une application, assurez-vous de supprimer tous les partages de ressources et groupes d'attributs associés qui n'ont pas été créés par un AWS service.

Note

La suppression d'une application n'a aucune incidence sur vos ressources. Les ressources étiquetées avec le tag AWS d'application resteront étiquetées.

Pour supprimer une application

1. Ouvrez la [AWS Management Console](#).

2. Dans la barre latérale gauche de la console, choisissez myApplications.
3. Sélectionnez l'application que vous souhaitez supprimer.
4. Sur le tableau de bord myApplications, choisissez Actions.
5. Choisissez Supprimer l'application.
6. Confirmez votre suppression, puis choisissez Supprimer.

Création d'extraits de code dans MyApplications

myApplications crée des extraits de code pour toutes vos applications. Vous pouvez utiliser des extraits de code pour ajouter automatiquement des ressources nouvellement créées à une application à l'aide des outils d'infrastructure en tant que code (IaC). Toutes les ressources ajoutées sont étiquetées avec le tag d' AWS application pour les associer à votre application.

Pour créer un extrait de code pour votre application

1. Ouvrez la [AWS Management Console](#).
2. Dans la barre latérale gauche de la console, choisissez myApplications.
3. Recherchez et sélectionnez une application.
4. Choisissez Actions.
5. Choisissez Obtenir un extrait de code.
6. Sélectionnez un type d'extrait de code.
7. Choisissez Copier pour copier le code dans votre presse-papiers.
8. Collez votre code dans votre outil IaC.

Ressources disponibles dans MyApplications

Dans AWS, une ressource est une entité avec laquelle vous pouvez travailler. Les exemples incluent une instance Amazon EC2, une AWS CloudFormation pile ou un compartiment Amazon S3. Vous pouvez gérer vos ressources dans MyApplications en les ajoutant ou en les supprimant des applications.

Rubriques

- [Ajouter des ressources dans MyApplications](#)
- [Supprimer des ressources dans MyApplications](#)

- [Afficher les ressources dans MyApplications](#)

Ajouter des ressources dans MyApplications

L'ajout de ressources à vos applications vous permet de les regrouper et de gérer leur sécurité, leurs performances et leur conformité. Vous pouvez ajouter des ressources aux applications existantes en les recherchant et en les sélectionnant ou en utilisant des balises existantes et en effectuant une synchronisation des balises.

Search and select resources

Pour rechercher et sélectionner des ressources

1. Ouvrez la [AWS Management Console](#).
2. Dans la barre latérale gauche de la console, choisissez myApplications.
3. Recherchez et sélectionnez une application.
4. Choisissez Gérer les ressources.
5. Choisissez Ajouter des ressources.
6. (Facultatif) Choisissez une [vue](#).
7. Recherchez vos ressources. Vous pouvez effectuer une recherche par mot-clé, nom ou type, ou choisir un type de ressource.

Note

Si vous ne trouvez pas la ressource que vous recherchez, effectuez un dépannage avec Explorateur de ressources AWS. Pour plus d'informations, consultez [Résolution des problèmes de recherche de Resource Explorer](#) dans le Guide de l'utilisateur de Resource Explorer.

8. Cochez la case à côté des ressources que vous souhaitez ajouter.
9. Choisissez Ajouter.

Automatically add resources using tags

Lorsque vous créez une application, vous pouvez intégrer des ressources en bloc en spécifiant une paire clé-valeur de balise existante. Avec cette méthode, applique AWS automatiquement la `awsApplication` balise à toutes les ressources et crée une synchronisation des balises pour les

ressources de l'application par défaut. Lorsque la synchronisation des balises est activée, toutes les ressources étiquetées avec la paire clé-valeur de balise spécifiée sont automatiquement ajoutées à l'application.

Pour ajouter des ressources à l'aide de balises existantes

1. Ouvrez la [AWS Management Console](#).
2. Dans la barre latérale gauche de la console, choisissez myApplications.
3. Choisissez Gérer les ressources.
4. Choisissez Create tag-sync.
5. Sélectionnez une clé de balise et une valeur existantes :
 - a. Sélectionnez le rôle utilisé pour étiqueter les ressources. Pour plus d'informations, consultez la section [Autorisations requises pour les tâches de synchronisation des balises](#) dans le Guide de l' AppRegistry administrateur du AWS Service Catalog.
 - b. Sélectionnez une clé Tag.
 - c. Sélectionnez une valeur de tag.
 - d. Lisez et acceptez le Je reconnais que les événements du cycle de vie du groupe seront activés pour créer un avis de synchronisation des balises. GLE permet AWS de remarquer les modifications apportées aux ressources étiquetées avec votre paire clé-valeur.
6. Choisissez Créer une synchronisation de balises.

Résolution des erreurs de synchronisation des balises dans MyApplications

Cette section décrit les erreurs courantes de synchronisation des balises et explique comment les résoudre. Après avoir tenté de résoudre l'erreur, vous pouvez réessayer la tâche de synchronisation des balises qui a échoué.

- **Autorisations insuffisantes** : vous ne disposez pas des autorisations minimales requises pour démarrer, mettre à jour ou annuler la synchronisation des balises. Consultez les [autorisations requises pour la synchronisation des balises](#) pour plus d'informations. Après avoir vérifié que le rôle que vous spécifiez pour exécuter la synchronisation des balises dispose des autorisations minimales requises, réessayez la tâche de synchronisation des balises qui a échoué.
- **Existe déjà** : une tâche avec cette paire clé-valeur de balise existe déjà pour cette application. Une application peut prendre en charge plusieurs synchronisations de balises, mais chacune doit avoir

une paire clé-valeur de balise différente. Après avoir spécifié une autre paire clé-valeur de balise, réessayez la tâche de synchronisation des balises qui a échoué.

- Limite maximale atteinte : vous avez atteint le maximum de 100 tâches de synchronisation de balises par compte, toutes applications confondues.

Supprimer des ressources dans MyApplications

Vous pouvez supprimer des ressources pour les dissocier de votre application.

Pour supprimer des ressources

1. Ouvrez la [AWS Management Console](#).
2. Dans la barre latérale gauche de la console, choisissez myApplications.
3. Recherchez et sélectionnez une application.
4. Choisissez Gérer les ressources.
5. (Facultatif) Choisissez une [vue](#).
6. Recherchez vos ressources. Vous pouvez effectuer une recherche par mot-clé, nom ou type, ou choisir un type de ressource.

Note

Si vous ne trouvez pas la ressource que vous recherchez, effectuez un dépannage avec Explorateur de ressources AWS. Pour plus d'informations, consultez [Résolution des problèmes de recherche de Resource Explorer](#) dans le Guide de l'utilisateur de Resource Explorer.

7. Cliquez sur Supprimer.
8. Confirmez que vous souhaitez supprimer la ressource en choisissant Supprimer des ressources.

Afficher les ressources dans MyApplications

Vous pouvez consulter les ressources de votre application dans MyApplications et dans le menu Services.

myApplications

Pour consulter vos ressources dans MyApplications

1. Ouvrez la [AWS Management Console](#).
2. Développez la barre latérale gauche et choisissez MyApplications.
3. Sélectionnez une application.
4. Dans le widget Ressources, consultez vos ressources.

Services menu

Pour consulter les applications depuis le menu Services

1. Ouvrez la [AWS Management Console](#).
2. Dans la barre de navigation, choisissez Services ().
3. Choisissez Toutes les applications.
4. Sélectionnez une application.
5. (Facultatif) Sélectionnez une [vue](#).
6. (Facultatif) Sélectionnez un filtre. Vous pouvez filtrer vos ressources par propriétés ou par balises. Pour plus d'informations, consultez [la section Référence de syntaxe des requêtes de recherche pour Resource Explorer](#) dans le guide de Explorateur de ressources AWS l'utilisateur.
7. (Facultatif) Sélectionnez une ressource pour l'afficher dans la console de service correspondante.

Tip

Vous pouvez continuer à parcourir les ressources là où vous vous êtes arrêté en sélectionnant Services (). Les filtres de recherche que vous avez appliqués seront également conservés.

Tableau de bord MyApplications dans AWS Console Home

Chaque application que vous créez ou intégrez possède son propre tableau de bord myApplications. Le tableau de bord MyApplications contient des widgets relatifs aux coûts, à la sécurité et au

fonctionnement qui permettent de recueillir des informations provenant de plusieurs AWS services. Chaque widget peut également être ajouté aux favoris, réorganisé, supprimé ou redimensionné. Pour de plus amples informations, veuillez consulter [Utilisation de widgets dans AWS Console Home](#).

Rubriques

- [Widget de configuration du tableau de bord des applications](#)
- [Widget récapitulatif des applications](#)
- [Widget de calcul](#)
- [Widget de coûts et d'utilisation](#)
- [AWS Widget de sécurité](#)
- [AWS Widget de résilience](#)
- [Widget de ressources](#)
- [DevOps widget](#)
- [Widget de surveillance et d'opérations](#)
- [Widget de balises](#)

Widget de configuration du tableau de bord des applications

Ce widget contient une liste d'activités de démarrage suggérées que vous pouvez utiliser Services AWS pour vous aider à configurer la gestion des ressources de l'application.

Widget récapitulatif des applications

Ce widget affiche le nom, la description et la [balise d'application AWS](#) de votre application. Vous pouvez accéder à la balise d'application dans l'infrastructure en tant que code (IaC) et la copier pour baliser manuellement les ressources.

Widget de calcul

Ce widget affiche les informations et les métriques relatives aux ressources de calcul que vous ajoutez à votre application. Cela inclut le nombre total d'alarmes et le nombre total de types de ressources de calcul. Le widget affiche également des graphiques de tendance relatifs aux indicateurs de performance des ressources issus Amazon CloudWatch de l'utilisation du processeur des instances Amazon EC2 et des appels Lambda.

Configuration du widget de calcul

Pour renseigner les données dans le widget de calcul, configurez au moins une instance Amazon EC2 ou une fonction Lambda pour votre application. Pour plus d'informations, consultez la [Documentation Amazon Elastic Compute Cloud](#) et [Démarrage avec Lambda](#) dans le Guide du développeur AWS Lambda .

Widget de coûts et d'utilisation

Ce widget affiche les données de AWS coût et d'utilisation des ressources de votre application. Vous pouvez utiliser ces données pour comparer les coûts mensuels et consulter la répartition des coûts par Service AWS. Ce widget résume uniquement les coûts des ressources étiquetées avec le tag d' AWS application, à l'exclusion des taxes, des frais et des autres coûts partagés qui ne sont pas directement associés à une ressource. Les coûts indiqués ne sont pas combinés et mis à jour au moins une fois toutes les 24 heures. FOr Pour plus d'informations, consultez la section [Analyse de vos coûts Explorateur de ressources AWS](#) dans le Guide de AWS Cost Management l'utilisateur.

Configuration du widget de coûts et d'utilisation

Pour configurer le widget Coût et utilisation, activez-le AWS Cost Explorer Service pour votre application et votre compte. Ce service est offert sans frais supplémentaires et il n'y a pas de frais d'installation ni d'engagement initial. Pour plus d'informations, consultez [Activation de Cost Explorer](#) in the Guide de l'utilisateur AWS Cost Management .

AWS Widget de sécurité

Ce widget affiche les résultats de AWS sécurité de Security pour votre application. AWS La sécurité fournit une vue complète des résultats de sécurité pour votre application dans AWS. Vous pouvez accéder aux derniers résultats prioritaires par niveau de gravité, surveiller leur niveau de sécurité, accéder aux derniers résultats critiques ou de gravité élevée et obtenir des informations pour les prochaines étapes. Pour de plus amples informations, veuillez consulter [AWS Security Hub CSPM](#).

Configuration du widget AWS de sécurité

Pour configurer le widget AWS de sécurité, configurez-le AWS Security Hub CSPM pour votre application et votre compte. Pour plus d'informations, voir [Qu'est-ce que c'est AWS Security Hub CSPM ?](#) dans le guide de AWS Security Hub CSPM l'utilisateur. Pour plus d'informations, consultez [Essai gratuit, utilisation et tarification d'AWS Security Hub CSPM](#) dans le Guide de l'utilisateur AWS Security Hub CSPM .

AWS Security Hub CSPM vous oblige à configurer l'enregistrement de AWS configuration. Ce service fournit une vue détaillée des ressources associées à votre AWS compte. Pour plus d'informations, consultez [AWS Systems Manager](#) dans le Guide de l'utilisateur AWS Systems Manager .

AWS Widget de résilience

Ce widget affiche les détails de AWS résilience de Resilience Hub pour vos applications. Après avoir lancé une évaluation, AWS Resiliency Hub analyse le niveau de résilience de vos applications en évaluant leurs ressources par rapport à une politique de résilience prédéfinie. Vous pouvez accéder à des indicateurs tels que le score de résilience, les violations des politiques, les dérives des politiques, les dérives des ressources et l'historique de votre score de résilience. Vos demandes sont évaluées quotidiennement pour un meilleur suivi, mais vous pouvez le désactiver à tout moment. Pour de plus amples informations, veuillez consulter [AWS Resilience Hub](#). Pour en savoir plus sur la tarification, consultez [Tarification AWS Resilience Hub](#).

Configuration du widget AWS Resiliency

Pour configurer le widget AWS Resiliency, ajoutez une application. Pour plus d'informations, voir [Qu'est-ce que c'est AWS Resilience Hub ?](#) dans le guide de AWS Resilience Hub l'utilisateur.

Widget de ressources

Ce widget utilise l'explorateur de AWS ressources pour afficher les ressources que vous avez ajoutées à votre application dans une vue. Vous pouvez également utiliser ce widget pour rechercher ou filtrer vos ressources à l'aide de métadonnées de ressources telles que les noms, les balises et IDs. Pour plus d'informations, consultez [AWS Resource Explorer](#).

Configuration du widget Ressources

Pour configurer le widget de ressources, intégrez Resource Explorer. Pour plus d'informations, voir [Commencer à utiliser l'explorateur de ressources](#) dans le guide de l'utilisateur de l'explorateur de AWS ressources.

DevOps widget

Ce widget affiche des informations opérationnelles afin que vous puissiez évaluer la conformité et prendre des mesures pour votre application. Ces informations incluent :

- Gestion de parc

- Gestion des états
- Gestion des correctifs
- Configuration et OpsItems gestion

Configuration du DevOps widget

Pour configurer le DevOps widget, activez-le AWS Systems Manager OpsCenter pour votre application et votre compte. Pour plus d'informations, consultez [Getting started with Systems Manager Explorer et OpsCenter](#) dans le Guide de AWS Systems Manager l'utilisateur. L'activation OpsCenter AWS Systems Manager Explorer permet de configurer AWS Config et Amazon CloudWatch de créer automatiquement leurs événements OpsItems en fonction des règles et événements couramment utilisés. Pour plus d'informations, voir [Configuration OpsCenter](#) dans le guide de AWS Systems Manager l'utilisateur.

Vous pouvez configurer vos instances afin que les agents Systems Manager exécutent et appliquent des autorisations pour activer l'analyse des correctifs. Pour plus d'informations, consultez [AWS Systems Manager Quick Setup](#) dans le Guide de l'utilisateur AWS Systems Manager .

Vous pouvez également configurer l'application de correctifs automatisés pour les instances Amazon EC2 en AWS Systems Manager configurant le gestionnaire de correctifs. Pour plus d'informations, consultez [Utilisation des stratégies de correctifs Quick Setup](#) dans le Guide de l'utilisateur AWS Systems Manager .

Pour en savoir plus sur la tarification, consultez [Tarification AWS Systems Manager](#).

Widget de surveillance et d'opérations

Ce widget affiche :

- Alarmes et alertes pour les ressources associées à votre application
- Objectifs de niveau de service des applications (SLOs) et métriques
- Métriques des signaux AWS d'application disponibles

Configuration du widget de surveillance et d'opérations

Pour configurer le widget Surveillance et opérations, créez des CloudWatch alarmes et des canaris dans votre AWS compte. Pour plus d'informations, consultez les sections [Utilisation des CloudWatch alarmes Amazon](#) et [Création d'un canari](#) dans le guide de CloudWatch l'utilisateur Amazon. Pour

connaître les tarifs CloudWatch d'alarme et ceux de Synthetic Canary, consultez respectivement [CloudWatch les tarifs Amazon](#) et le [blog sur les opérations et migrations dans le AWS cloud](#).

Pour plus d'informations sur les signaux CloudWatch d'application, consultez la section [Activer les signaux CloudWatch d'application Amazon](#) dans le guide de CloudWatch l'utilisateur Amazon.

Widget de balises

Ce widget affiche toutes les balises associées à votre application. Vous pouvez utiliser ce widget pour suivre et gérer les métadonnées des applications (gravité, environnement, centre de coûts). Pour plus d'informations, voir [Que sont les tags ?](#) dans le AWS livre blanc sur les meilleures pratiques pour le balisage AWS des ressources.

Discuter avec le développeur Amazon Q dans AWS Console Home

Amazon Q Developer est un assistant conversationnel basé sur l'intelligence artificielle générative (IA) qui peut vous aider à comprendre, créer, étendre et exploiter AWS des applications. Vous pouvez poser à Amazon Q toutes les questions concernant AWS notamment AWS l'architecture, vos AWS ressources, les meilleures pratiques, la documentation, etc. Vous pouvez également créer des dossiers d'assistance et bénéficier de l'assistance d'un agent en direct. Pour plus d'informations, consultez [Qu'est-ce qu'Amazon Q ?](#) dans le guide de l'utilisateur Amazon Q Developer.

Commencez avec Amazon Q

Vous pouvez commencer à discuter avec Amazon Q sur les sites Web de AWS documentation AWS Management Console, les AWS sites Web ou l'Application Mobile AWS Console en choisissant l'icône hexagonale Amazon Q. Pour plus d'informations, consultez la section [Commencer avec Amazon Q Developer](#) dans le guide de l'utilisateur Amazon Q Developer.

Exemples de questions

Voici quelques exemples de questions que vous pouvez poser à Amazon Q :

- How do I get billing support?
- How do I create an EC2 instance?
- How do I troubleshoot a "Failed to load" error?
- How do I close an AWS account?
- Can you connect me with a person?

AWS Management Console Accès privé

AWS Management Console L'accès privé est une fonctionnalité de sécurité avancée permettant de contrôler l'accès au AWS Management Console. L'accès privé à la console est utile lorsque vous souhaitez empêcher les utilisateurs de se connecter Comptes AWS de manière inattendue depuis votre réseau. Grâce à cette fonctionnalité, vous pouvez limiter l'accès AWS Management Console à un ensemble spécifique de données connues Comptes AWS lorsque le trafic provient de votre réseau. L'accès privé à la console est également utile lorsque vous souhaitez vous assurer que tous les appels provenant Services AWS du AWS Management Console to proviennent de votre réseau et de comptes autorisés.

Rubriques

- [Consoles Régions AWS de service et fonctionnalités d'accès privé prises en charge](#)
- [Vue d'ensemble des contrôles de sécurité des accès AWS Management Console privés](#)
- [Points de terminaison de VPC et configuration DNS requis](#)
- [Mise en œuvre de politiques de contrôle des services et de politiques de points de terminaison de VPC](#)
- [Mise en œuvre de politiques basées sur l'identité et d'autres types de politiques](#)
- [Essayez l'accès AWS Management Console privé](#)
- [Architecture de référence](#)

Consoles Régions AWS de service et fonctionnalités d'accès privé prises en charge

AWS Management Console L'accès privé ne prend en charge qu'un sous-ensemble de régions et de AWS services. Les consoles de service non prises en charge sont inactives dans AWS Management Console. En outre, certaines AWS Management Console fonctionnalités peuvent être désactivées lors de l'utilisation de l'accès AWS Management Console privé, par exemple la [région par défaut](#) dans les paramètres unifiés.

Les régions et consoles de service suivantes sont prises en charge.

Régions prises en charge

- USA Est (Ohio)

- USA Est (Virginie du Nord)
- USA Ouest (Californie du Nord)
- US West (Oregon)
- Asie-Pacifique (Hyderabad)
- Asie-Pacifique (Mumbai)
- Asie-Pacifique (Séoul)
- Asie-Pacifique (Osaka)
- Asie-Pacifique (Singapour)
- Asie-Pacifique (Sydney)
- Asie-Pacifique (Malaisie)
- Asie-Pacifique (Thaïlande)
- Asie-Pacifique (Tokyo)
- Canada (Centre)
- Europe (Francfort)
- Europe (Irlande)
- Europe (Londres)
- Europe (Paris)
- Europe (Stockholm)
- Amérique du Sud (São Paulo)
- Afrique (Le Cap)
- Asie-Pacifique (Hong Kong)
- Asie-Pacifique (Jakarta)
- Asie-Pacifique (Melbourne)
- Canada-Ouest (Calgary)
- Mexique (Centre)
- Europe (Milan)
- Europe (Espagne)
- Europe (Zurich)

- Middle East (Bahrain)
- Moyen-Orient (EAU)
- Israël (Tel Aviv)

Consoles de service prises en charge

- Amazon API Gateway
- AWS App Mesh
- AWS Application Migration Service
- AWS Artifact
- Amazon Athena
- AWS Audit Manager
- AWS Auto Scaling
- AWS Batch
- AWS Billing Conductor
- AWS Billing and Cost Management
- AWS Budgets
- AWS Certificate Manager
- AWS Cloud Map
- AWS CloudFormation
- Amazon CloudFront
- AWS CloudTrail
- Amazon CloudWatch
- AWS CodeArtifact
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- Amazon CodeGuru
- AWS CodePipeline
- Amazon Comprehend

- Amazon Comprehend Medical
- Optimiseur de calcul AWS
- AWS Console Home
- AWS Control Tower
- Amazon DataZone
- AWS Database Migration Service
- AWS DataSync
- AWS DeepRacer
- AWS Direct Connect
- AWS Directory Service
- Amazon DocumentDB
- Amazon DynamoDB
- Amazon EC2
- Amazon EC2 Global View (Amazon EC2 Global View)
- EC2 Image Builder
- Amazon EC2 Instance Connect
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- Reprise après sinistre AWS Elastic
- Amazon Elastic File System
- Amazon Elastic Kubernetes Service
- Elastic Load Balancing
- Amazon ElastiCache
- Amazon EMR
- Amazon EventBridge
- AWS Firewall Manager
- GameLift Serveurs Amazon
- AWS Glue

- AWS Global Accelerator
- AWS Glue DataBrew
- AWS Ground Station
- Amazon GuardDuty
- AWS IAM Identity Center
- Gestion des identités et des accès AWS
- AWS Identity and Access Management Access Analyzer
- Amazon Inspector
- Amazon Kendra
- AWS Key Management Service
- Amazon Kinesis
- Service géré Amazon pour Apache Flink
- Amazon Data Firehose
- Amazon Kinesis Data Streams
- Amazon Kinesis Video Streams
- AWS Lambda
- Amazon Lex
- AWS License Manager
- Amazon Managed Grafana
- Amazon Macie
- Amazon Managed Streaming for Apache Kafka
- Amazon Managed Workflows for Apache Airflow (MWAA)
- Recommandations stratégiques d'AWS Migration Hub
- Amazon MQ
- Analyseur d'accès réseau
- AWS Network Firewall
- AWS Network Manager
- Amazon OpenSearch Service

- AWS Organizations
- AWS Autorité de certification privée
- Tableau de bord de santé publique
- Amazon Rekognition
- Amazon Relational Database Service
- AWS Resource Access Manager
- Groupes de ressources AWS et éditeur de balises
- Amazon Route 53 Resolver
- Amazon Route 53 Resolver Pare-feu DNS
- Amazon S3 sur Outposts
- Amazon SageMaker
- Amazon SageMaker Runtime
- Données synthétiques Amazon SageMaker AI
- AWS Secrets Manager
- AWS Service Catalog
- AWS Security Hub CSPM
- Service Quotas
- AWS Signer
- Amazon Simple Email Service
- Amazon SNS
- Amazon Simple Queue Service
- Amazon Simple Storage Service (Amazon S3)
- AWS SQL Workbench
- AWS Step Functions
- AWS Storage Gateway
- Support
- AWS Systems Manager
- Amazon Timestream

- AWS Transfer Family
- AWS Trusted Advisor
- Paramètres unifiés
- Amazon VPC IP Address Manager (IPAM)
- Amazon Virtual Private Cloud
- Client Amazon WorkSpaces Thin

Vue d'ensemble des contrôles de sécurité des accès AWS Management Console privés

Restrictions relatives aux comptes AWS Management Console depuis votre réseau

AWS Management Console L'accès privé est utile dans les scénarios où vous souhaitez limiter l'accès AWS Management Console depuis votre réseau à un ensemble spécifique connu Comptes AWS dans votre organisation. Vous pouvez ainsi empêcher les utilisateurs de se connecter à des Comptes AWS inattendus depuis votre réseau. Vous pouvez implémenter ces contrôles à l'aide de la politique de point de terminaison de VPC d' AWS Management Console . Pour de plus amples informations, veuillez consulter [Mise en œuvre de politiques de contrôle des services et de politiques de points de terminaison de VPC](#).

Connectivité entre votre réseau et Internet

La connectivité Internet depuis votre réseau est toujours requise pour accéder aux ressources utilisées par le AWS Management Console, telles que le contenu statique (CSSJavaScript, images), et toutes les ressources Services AWS non activées par [AWS PrivateLink](#). Pour obtenir la liste des domaines de premier niveau utilisés par le AWS Management Console, voir [Résolution des problèmes](#).

Note

Actuellement, AWS Management Console Private Access ne prend pas en charge les points de terminaison tels que `status.aws.amazon.com`, `health.aws.amazon.com`, `etdocs.aws.amazon.com`. Vous devez acheminer ces domaines vers l'Internet public.

Points de terminaison de VPC et configuration DNS requis

AWS Management Console L'accès privé nécessite les deux points de terminaison VPC suivants par région. Remplacez *region* par les informations de votre région.

1. com.amazonaws. *region*.console pour AWS Management Console
2. com.amazonaws. *region*.signin pour Connexion à AWS

Note

Veillez à toujours allouer une connectivité d'infrastructure et de réseau à la région USA Est (Virginie du Nord) (us-east-1), quelles que soient les autres régions que vous utilisez avec la AWS Management Console. Vous pouvez utiliser AWS Transit Gateway pour configurer la connectivité entre USA Est (Virginie du Nord) et toutes les autres régions. Pour en savoir plus, consultez [Mise en route avec les passerelles de transit](#) dans le Guide des passerelles de transit Amazon VPC. Vous pouvez également utiliser l'appairage Amazon VPC. Pour en savoir plus, consultez [Qu'est-ce que l'appairage de VPC ?](#) dans le Guide d'appairage Amazon VPC. Pour comparer ces options, consultez les options de [connectivité Amazon VPC-to-Amazon VPC dans le livre blanc sur les options](#) de connectivité Amazon Virtual Private Cloud.

Rubriques

- [DNSconfiguration pour AWS Management Console et Connexion à AWS](#)
- [Points de terminaison VPC et DNS configuration des services dans le AWS AWS Management Console](#)

DNSconfiguration pour AWS Management Console et Connexion à AWS

Pour touter votre trafic réseau vers les points de terminaison de VPC respectifs, configurez les enregistrements DNS dans le réseau à partir desquels vos utilisateurs accéderont à AWS Management Console. Ces enregistrements DNS dirigeront le trafic du navigateur de vos utilisateurs vers les points de terminaison de VPC que vous avez créés.

Vous pouvez créer une zone hébergée unique. Cependant, les points de terminaison tels que `health.aws.amazon.com` et `docs.aws.amazon.com` ne seront pas accessibles, car ils ne

disposent pas de points de terminaison de VPC. Vous devez acheminer ces domaines vers l'Internet public. Nous vous recommandons de créer deux zones hébergées privées par région, une pour `signin.aws.amazon.com` et une autre pour `console.aws.amazon.com` avec les enregistrements CNAME suivants :

- S'inscrire
 - `region.signin.aws.amazon.com` pointant vers le point de terminaison Connexion à AWS VPC dans la zone de connexion où se trouve la région souhaitée DNS `region`
 - `signin.aws.amazon.com` pointant vers le point de terminaison AWS VPC de connexion dans l'est des États-Unis (Virginie du Nord) (`us-east-1`)
- Console
 - `region.console.aws.amazon.com` pointant vers le point de terminaison AWS Management Console VPC dans la zone de console où se trouve la région souhaitée DNS `region`
 - `*.region.console.aws.amazon.com` pointant vers le point de terminaison AWS Management Console VPC dans la zone de console où se trouve la région souhaitée DNS `region`
 - `*.region.console.aws.amazon.com` pointant vers le point de terminaison AWS Management Console VPC dans la zone console DNS
 - Enregistrements CNAME sans région pour la région USA Est (Virginie du Nord) uniquement. Vous devez toujours configurer la région USA Est (Virginie du Nord).
 - `signin.aws.amazon.com` pointant vers un point de terminaison Connexion à AWS VPC dans l'est des États-Unis (Virginie du Nord) (`us-east-1`)
 - `*.console.aws.amazon.com` pointant vers un point de terminaison AWS Management Console VPC dans l'est des États-Unis (Virginie du Nord) (`us-east-1`)

Pour obtenir des instructions sur la création d'un enregistrement CNAME, consultez [Utilisation des enregistrements](#) dans le Guide du développeur Amazon Route 53.

Certaines AWS consoles, notamment Amazon S3, utilisent des modèles différents pour leurs DNS noms. En voici deux exemples :

- `support.console.aws.amazon.com`
- `s3.console.aws.amazon.com`

Pour pouvoir diriger ce trafic vers votre point de terminaison AWS Management Console VPC, vous devez ajouter ces noms individuellement. Pour une expérience totalement privée, nous vous recommandons de configurer le routage pour tous les points de terminaison. Toutefois, cela n'est pas obligatoire pour utiliser l'accès AWS Management Console privé.

Les json fichiers suivants contiennent la liste complète des points de Service AWS terminaison et de console à configurer par région. Utilisez le champ `PrivateIpv4DnsNames` situé sous le point de terminaison `com.amazonaws.region.console` pour les noms DNS.

- <https://configuration.private-access.console.amazonaws.com/us-east-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/us-east-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/us-west-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-northeast-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-northeast-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-southeast-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-southeast-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-south-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-south-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ca-central-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/eu-central-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/eu-west-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/eu-west-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/il-central-1.config.json>

Note

Cette liste est mise à jour tous les mois lorsque nous ajoutons des points de terminaison supplémentaires à la portée de l'accès privé AWS Management Console . Pour maintenir vos zones hébergées privées à jour, extrayez régulièrement la liste de fichiers précédente.

Si vous utilisez Route 53 pour configurer votre DNS, accédez à <https://console.aws.amazon.com/route53/v2/hostedzones#> pour vérifier la configuration. DNS Pour chaque zone hébergée privée dans Route 53, vérifiez que les ensembles d'enregistrements suivants sont présents.

- `console.aws.amazon.com`
- `signin.aws.amazon.com`
- `*.region.console.aws.amazon.com`
- `region.console.aws.amazon.com`

- *. *region*.console.aws.amazon.com
- signin.aws.amazon.com
- *region*.signin.aws.amazon.com
- Enregistrements supplémentaires présents dans les fichiers JSON précédemment répertoriés

Points de terminaison VPC et DNS configuration des services dans le AWS AWS Management Console

Les AWS Management Console appels Services AWS via une combinaison de demandes directes du navigateur et de demandes transmises par des serveurs Web. Pour diriger ce trafic vers votre point de terminaison AWS Management Console VPC, vous devez ajouter le point de terminaison VPC et le configurer DNS pour chaque service dépendant. AWS

Les json fichiers suivants répertorient les fichiers AWS PrivateLink pris en charge Services AWS que vous pouvez utiliser. Si un service ne s'intègre pas à ces fichiers AWS PrivateLink, il n'est pas inclus dans ces fichiers.

- <https://configuration.private-access.console.amazonaws.com/us-east-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/us-east-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/us-west-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-northeast-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-northeast-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-southeast-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-southeast-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-south-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/ap-south-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/ca-central-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/eu-central-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/eu-west-1.config.json>
- <https://configuration.private-access.console.amazonaws.com/eu-west-2.config.json>
- <https://configuration.private-access.console.amazonaws.com/il-central-1.config.json>

Utilisez le champ `ServiceName` pour le point de terminaison de VPC du service correspondant à ajouter à votre VPC.

Note

Nous mettons à jour cette liste chaque mois à mesure que nous ajoutons la prise en charge de l'accès AWS Management Console privé à un plus grand nombre de consoles de service. Pour rester à jour, extrayez régulièrement la liste de fichiers précédente et mettez à jour vos points de terminaison de VPC.

Mise en œuvre de politiques de contrôle des services et de politiques de points de terminaison de VPC

Vous pouvez utiliser les politiques de contrôle des services (SCPs) et les politiques de point de terminaison VPC pour l'accès AWS Management Console privé afin de limiter le nombre de comptes autorisés à utiliser le formulaire au sein AWS Management Console de votre VPC et de ses réseaux locaux connectés.

Rubriques

- [Utilisation de l'accès AWS Management Console privé avec des politiques AWS Organizations de contrôle des services](#)
- [Autoriser AWS Management Console l'utilisation pour les comptes et organisations attendus uniquement \(identités fiables\)](#)

Utilisation de l'accès AWS Management Console privé avec des politiques AWS Organizations de contrôle des services

Si votre AWS organisation utilise une politique de contrôle des services (SCP) qui autorise des services spécifiques, vous devez ajouter des actions `signin:*` aux actions autorisées. Cette autorisation est nécessaire car la connexion AWS Management Console au point de terminaison VPC via un accès privé exécute une autorisation IAM que le SCP bloque sans autorisation. À titre d'exemple, la politique de contrôle des services suivante permet d'utiliser Amazon EC2 et les CloudWatch services dans l'organisation, y compris lorsqu'ils sont accessibles via un point de terminaison d'accès AWS Management Console privé.

```
{
  "Effect": "Allow",
  "Action": [
    "signin:*",
    "ec2:*",
    "cloudwatch:*",
    ... Other services allowed
  ],
  "Resource": "*"
}
```

Pour plus d'informations SCPs, voir [Politiques de contrôle des services \(SCPs\)](#) dans le Guide de AWS Organizations l'utilisateur.

Autoriser AWS Management Console l'utilisation pour les comptes et organisations attendus uniquement (identités fiables)

AWS Management Console et Connexion à AWS soutenez une politique de point de terminaison VPC qui contrôle spécifiquement l'identité du compte connecté.

Contrairement aux autres politiques de point de terminaison de VPC, cette politique est évaluée avant l'authentification. Par conséquent, il contrôle spécifiquement la connexion et l'utilisation de la session authentifiée uniquement, et non les actions AWS spécifiques au service effectuées par la session. Par exemple, lorsque la session accède à une console de AWS service, telle que la console Amazon EC2, ces politiques de point de terminaison VPC ne seront pas évaluées par rapport aux actions Amazon EC2 entreprises pour afficher cette page. Vous pouvez plutôt utiliser les politiques IAM associées au principal IAM connecté pour contrôler son autorisation d'effectuer des actions de service. AWS

Note

Les politiques de point de terminaison VPC et les points de terminaison AWS Management Console SignIn VPC ne prennent en charge qu'un sous-ensemble limité de formulations de politiques. `Principal` et `Resource` doivent chacun être définis sur `*` et `Action` doit avoir la valeur `*` ou `signin:*`. Vous contrôlez l'accès aux points de terminaison de VPC à l'aide des clés de condition `aws:PrincipalOrgId` et `aws:PrincipalAccount`.

Les politiques suivantes sont recommandées pour les points de terminaison de la console et du SignIn VPC.

Cette politique de point de terminaison VPC autorise la connexion Comptes AWS à l' AWS organisation spécifiée et bloque la connexion à tout autre compte.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgId": "o-xxxxxxxxxxxxx"
        }
      }
    }
  ]
}
```

Cette politique de point de terminaison VPC limite la connexion à une liste de comptes spécifiques Comptes AWS et bloque la connexion à tout autre compte.

JSON

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

```
    "aws:PrincipalAccount": [ "111122223333", "222233334444" ]
  }
}
]
```

Les politiques qui limitent Comptes AWS ou limitent une organisation sur les points de terminaison VPC AWS Management Console et de connexion sont évaluées au moment de la connexion et sont périodiquement réévaluées pour les sessions existantes.

Mise en œuvre de politiques basées sur l'identité et d'autres types de politiques

Vous gérez l'accès en AWS créant des politiques et en les associant à des identités IAM (utilisateurs, groupes d'utilisateurs ou rôles) ou à des AWS ressources. Cette page décrit le fonctionnement des politiques lorsqu'elles sont utilisées conjointement avec l'accès AWS Management Console privé.

Clés contextuelles de condition AWS globale prises en charge

AWS Management Console L'accès privé ne prend pas en charge `aws:SourceVpce` les clés contextuelles de condition `aws:VpcSourceIp` AWS globale. Lorsque vous utilisez la AWS Management Console en accès privé, vous pouvez utiliser à la place la condition IAM `aws:SourceVpc` dans vos politiques.

Comment fonctionne AWS Management Console Private Access avec AWS : SourceVpc

Cette section décrit les différents chemins réseau que les demandes générées par vous AWS Management Console peuvent emprunter Services AWS. En général, les consoles de AWS service sont mises en œuvre avec un mélange de requêtes directes du navigateur et de demandes transmises par proxy aux serveurs AWS Management Console Web. Services AWS Ces implémentations sont susceptibles d'être modifiées sans préavis. Si vos exigences en matière de sécurité incluent l'accès à Services AWS l'utilisation de points de terminaison VPC, nous vous recommandons de configurer des points de terminaison VPC pour tous les services que vous avez l'intention d'utiliser depuis un VPC, que ce soit directement ou via un accès privé. AWS Management

Console En outre, vous devez utiliser la condition `aws:SourceVpc` IAM dans vos politiques plutôt que des `aws:SourceVpce` valeurs spécifiques avec la fonctionnalité AWS Management Console d'accès privé. Cette section fournit des détails sur le fonctionnement des différents chemins réseau.

Une fois qu'un utilisateur s'est connecté au AWS Management Console, il envoie des demandes Services AWS via une combinaison de demandes directes du navigateur et de demandes transmises par des serveurs AWS Management Console Web à AWS des serveurs. Par exemple, les demandes de données CloudWatch graphiques sont effectuées directement depuis le navigateur. Alors que certaines demandes de console de AWS service, telles qu'Amazon S3, sont transmises par proxy à Amazon S3 par le serveur Web.

Pour les requêtes directes du navigateur, l'utilisation de l'accès AWS Management Console privé ne change rien. Comme auparavant, la demande atteint le service via le chemin réseau que le VPC a configuré pour atteindre `monitoring.region.amazonaws.com`. Si le VPC est configuré avec un point de terminaison VPC pour `com.amazonaws.region.monitoring`, la demande atteindra CloudWatch ce point de terminaison VPC. CloudWatch S'il n'existe aucun point de terminaison VPC pour CloudWatch, la demande CloudWatch atteindra son point de terminaison public, via une passerelle Internet sur le VPC. Les demandes qui arrivent via CloudWatch le point de terminaison du CloudWatch VPC seront soumises aux conditions IAM `aws:SourceVpc` et seront `aws:SourceVpce` définies sur leurs valeurs respectives. Ceux qui accèdent CloudWatch via son point de terminaison public auront `aws:SourceIp` défini l'adresse IP source de la demande. Pour plus d'informations sur ces clés de condition IAM, consultez [Clés de condition globales](#) dans le Guide de l'utilisateur IAM.

Pour les demandes transmises par le serveur AWS Management Console Web, telles que la demande faite par la console Amazon S3 pour répertorier vos buckets lorsque vous visitez la console Amazon S3, le chemin réseau est différent. Ces demandes ne sont pas initiées depuis votre VPC et n'utilisent donc pas le point de terminaison de VPC que vous avez peut-être configuré sur votre VPC pour ce service. Même si vous disposez d'un point de terminaison de VPC pour Amazon S3 dans ce cas, la demande de votre session à Amazon S3 pour répertorier les compartiments n'utilise pas le point de terminaison de VPC Amazon S3. Toutefois, lorsque vous utilisez AWS Management Console Private Access avec des services pris en charge, ces demandes (par exemple, adressées à Amazon S3) incluent la clé de `aws:SourceVpc` condition dans leur contexte de demande. La clé de `aws:SourceVpc` condition sera définie sur l'ID VPC sur lequel vos points de terminaison AWS Management Console d'accès privé pour la connexion et la console sont déployés. Ainsi, si vous utilisez des restrictions `aws:SourceVpc` dans vos politiques basées sur l'identité, vous devez ajouter l'ID du VPC qui héberge les points de terminaison de connexion et de console de l'accès privé AWS Management Console . La `aws:SourceVpce` condition sera définie sur le point de terminaison IDs VPC de connexion ou de console correspondant.

Note

Si vos utilisateurs ont besoin d'accéder à des consoles de service qui ne sont pas prises en charge par la AWS Management Console en accès privé, vous devez inclure la liste de vos adresses réseau publiques attendues (comme la plage de votre réseau sur site) en utilisant la clé de condition `aws:SourceIP` dans les politiques basées sur l'identité des utilisateurs.

Comment les différents chemins réseau sont reflétés dans CloudTrail

Les différents chemins réseau utilisés par les demandes que vous avez générées AWS Management Console sont reflétés dans l'historique de vos CloudTrail événements.

Pour les requêtes directes du navigateur, l'utilisation de l'accès AWS Management Console privé ne change rien. CloudTrail les événements incluront des détails sur la connexion, tels que l'ID de point de terminaison VPC utilisé pour effectuer l'appel d'API de service.

Pour les demandes transmises par le serveur AWS Management Console Web, les CloudTrail événements n'incluront aucun détail relatif au VPC. Toutefois, les demandes initiales requises pour établir la session du navigateur, telles Connexion à AWS que le type `AwsConsoleSignIn` événement, incluront l'ID du point de terminaison du Connexion à AWS VPC dans les détails de l'événement.

Essayez l'accès AWS Management Console privé

Cette section explique comment configurer et tester l'accès AWS Management Console privé dans un nouveau compte.

AWS Management Console L'accès privé est une fonctionnalité de sécurité avancée qui nécessite des connaissances préalables en matière de mise en réseau et de configuration VPCs. Cette rubrique décrit comment tester l'accès privé AWS Management Console sans une infrastructure à grande échelle.

Rubriques

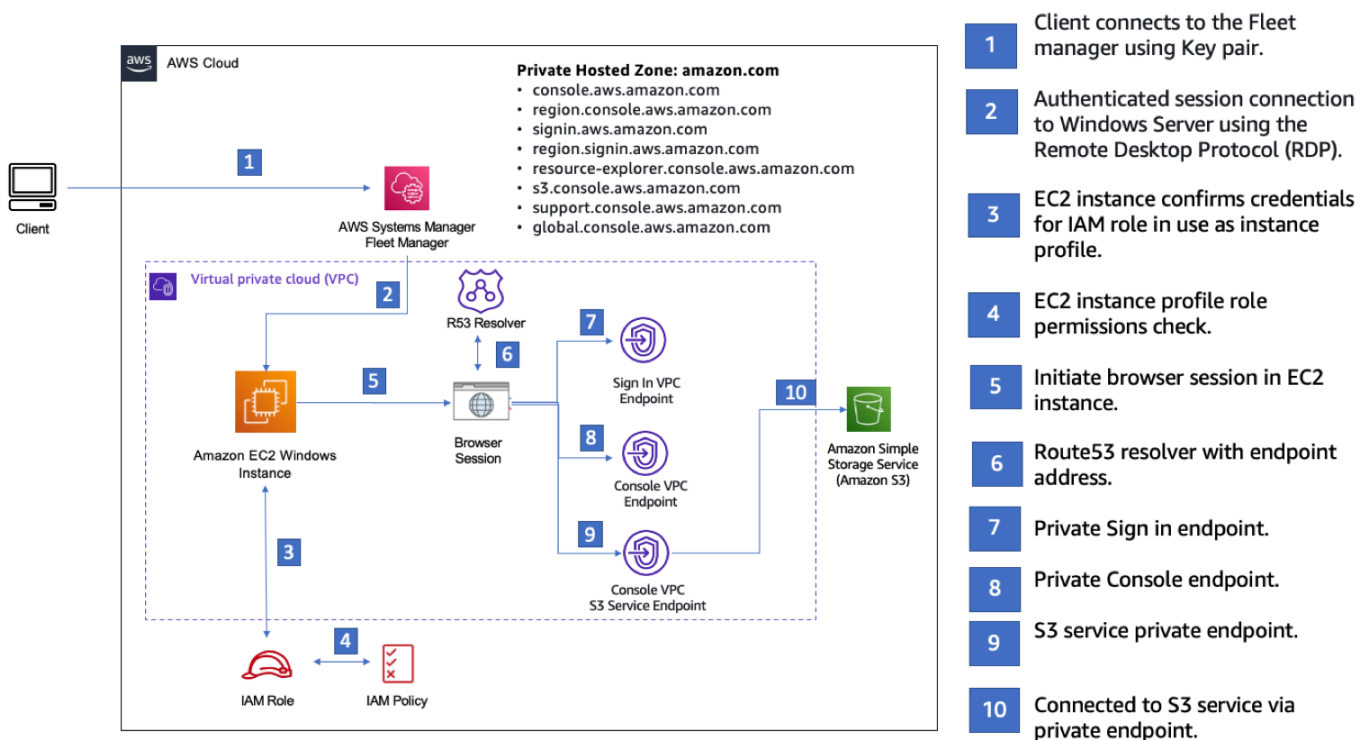
- [Configuration test avec Amazon EC2](#)
- [Configuration des tests avec Amazon WorkSpaces](#)
- [Configuration test du VPC avec des politiques IAM](#)

Configuration test avec Amazon EC2

[Amazon Elastic Compute Cloud](#) (Amazon EC2) offre une capacité de calcul évolutive dans le cloud Amazon Web Services. Vous pouvez utiliser Amazon EC2 pour lancer autant de serveurs virtuels que nécessaire, configurer la sécurité et les réseaux, et gérer le stockage. Dans cette configuration, nous utilisons la fonctionnalité [Fleet Manager](#) d'AWS Systems Manager pour nous connecter à une instance Windows Amazon EC2 à l'aide du protocole RDP (Remote Desktop Protocol).

Ce guide présente un environnement de test pour configurer et tester une connexion d'accès AWS Management Console privé à Amazon Simple Storage Service à partir d'une instance Amazon EC2. Ce didacticiel permet CloudFormation de créer et de configurer la configuration réseau à utiliser par Amazon EC2 pour visualiser cette fonctionnalité.

Le schéma suivant décrit le flux de travail permettant d'accéder à une installation de la AWS Management Console en accès privé à l'aide d'Amazon EC2. Il montre comment un utilisateur est connecté à Amazon S3 à l'aide d'un point de terminaison privé.



Copiez le CloudFormation modèle suivant et enregistrez-le dans un fichier que vous utiliserez à l'étape 3 de la procédure Pour configurer un réseau.

Note

Ce CloudFormation modèle utilise des configurations qui ne sont actuellement pas prises en charge dans la région d'Israël (Tel Aviv).

AWS Management Console Modèle Amazon CloudFormation EC2 d'environnement d'accès privé

Description: |

AWS Management Console Private Access.

Parameters:

VpcCIDR:

Type: String

Default: 172.16.0.0/16

Description: CIDR range for VPC

Ec2KeyPair:

Type: AWS::EC2::KeyPair::KeyName

Description: The EC2 KeyPair to use to connect to the Windows instance

PublicSubnet1CIDR:

Type: String

Default: 172.16.1.0/24

Description: CIDR range for Public Subnet A

PublicSubnet2CIDR:

Type: String

Default: 172.16.0.0/24

Description: CIDR range for Public Subnet B

PublicSubnet3CIDR:

Type: String

Default: 172.16.2.0/24

Description: CIDR range for Public Subnet C

PrivateSubnet1CIDR:

Type: String

Default: 172.16.4.0/24

Description: CIDR range for Private Subnet A

PrivateSubnet2CIDR:

Type: String

Default: 172.16.5.0/24

```
Description: CIDR range for Private Subnet B
```

```
PrivateSubnet3CIDR:
```

```
  Type: String
```

```
  Default: 172.16.3.0/24
```

```
  Description: CIDR range for Private Subnet C
```

```
LatestWindowsAmiId:
```

```
  Type: 'AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>'
```

```
  Default: '/aws/service/ami-windows-latest/Windows_Server-2022-English-Full-Base'
```

```
InstanceTypeParameter:
```

```
  Type: String
```

```
  Default: 't3.medium'
```

```
Resources:
```

```
#####  
# VPC AND SUBNETS  
#####
```

```
AppVPC:
```

```
  Type: 'AWS::EC2::VPC'
```

```
  Properties:
```

```
    CidrBlock: !Ref VpcCIDR
```

```
    InstanceTenancy: default
```

```
    EnableDnsSupport: true
```

```
    EnableDnsHostnames: true
```

```
PublicSubnetA:
```

```
  Type: 'AWS::EC2::Subnet'
```

```
  Properties:
```

```
    VpcId: !Ref AppVPC
```

```
    CidrBlock: !Ref PublicSubnet1CIDR
```

```
    MapPublicIpOnLaunch: true
```

```
    AvailabilityZone:
```

```
      Fn::Select:
```

```
        - 0
```

```
        - Fn::GetAZs: ""
```

```
PublicSubnetB:
```

```
  Type: 'AWS::EC2::Subnet'
```

```
  Properties:
```

```
VpcId: !Ref AppVPC
CidrBlock: !Ref PublicSubnet2CIDR
MapPublicIpOnLaunch: true
AvailabilityZone:
  Fn::Select:
    - 1
    - Fn::GetAZs: ""
```

```
PublicSubnetC:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PublicSubnet3CIDR
    MapPublicIpOnLaunch: true
    AvailabilityZone:
      Fn::Select:
        - 2
        - Fn::GetAZs: ""
```

```
PrivateSubnetA:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PrivateSubnet1CIDR
    AvailabilityZone:
      Fn::Select:
        - 0
        - Fn::GetAZs: ""
```

```
PrivateSubnetB:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PrivateSubnet2CIDR
    AvailabilityZone:
      Fn::Select:
        - 1
        - Fn::GetAZs: ""
```

```
PrivateSubnetC:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PrivateSubnet3CIDR
```

```
AvailabilityZone:
  Fn::Select:
    - 2
    - Fn::GetAZs: ""
```

```
InternetGateway:
  Type: AWS::EC2::InternetGateway
```

```
InternetGatewayAttachment:
  Type: AWS::EC2::VPCGatewayAttachment
  Properties:
    InternetGatewayId: !Ref InternetGateway
    VpcId: !Ref AppVPC
```

```
NatGatewayEIP:
  Type: AWS::EC2::EIP
  DependsOn: InternetGatewayAttachment
```

```
NatGateway:
  Type: AWS::EC2::NatGateway
  Properties:
    AllocationId: !GetAtt NatGatewayEIP.AllocationId
    SubnetId: !Ref PublicSubnetA
```

```
#####
# Route Tables
#####
```

```
PrivateRouteTable:
  Type: 'AWS::EC2::RouteTable'
  Properties:
    VpcId: !Ref AppVPC
```

```
DefaultPrivateRoute:
  Type: AWS::EC2::Route
  Properties:
    RouteTableId: !Ref PrivateRouteTable
    DestinationCidrBlock: 0.0.0.0/0
    NatGatewayId: !Ref NatGateway
```

```
PrivateSubnetRouteTableAssociation1:
  Type: 'AWS::EC2::SubnetRouteTableAssociation'
  Properties:
    RouteTableId: !Ref PrivateRouteTable
```

```
SubnetId: !Ref PrivateSubnetA
```

```
PrivateSubnetRouteTableAssociation2:
```

```
Type: 'AWS::EC2::SubnetRouteTableAssociation'
```

```
Properties:
```

```
RouteTableId: !Ref PrivateRouteTable
```

```
SubnetId: !Ref PrivateSubnetB
```

```
PrivateSubnetRouteTableAssociation3:
```

```
Type: 'AWS::EC2::SubnetRouteTableAssociation'
```

```
Properties:
```

```
RouteTableId: !Ref PrivateRouteTable
```

```
SubnetId: !Ref PrivateSubnetC
```

```
PublicRouteTable:
```

```
Type: AWS::EC2::RouteTable
```

```
Properties:
```

```
VpcId: !Ref AppVPC
```

```
DefaultPublicRoute:
```

```
Type: AWS::EC2::Route
```

```
DependsOn: InternetGatewayAttachment
```

```
Properties:
```

```
RouteTableId: !Ref PublicRouteTable
```

```
DestinationCidrBlock: 0.0.0.0/0
```

```
GatewayId: !Ref InternetGateway
```

```
PublicSubnetARouteTableAssociation1:
```

```
Type: AWS::EC2::SubnetRouteTableAssociation
```

```
Properties:
```

```
RouteTableId: !Ref PublicRouteTable
```

```
SubnetId: !Ref PublicSubnetA
```

```
PublicSubnetBRouteTableAssociation2:
```

```
Type: AWS::EC2::SubnetRouteTableAssociation
```

```
Properties:
```

```
RouteTableId: !Ref PublicRouteTable
```

```
SubnetId: !Ref PublicSubnetB
```

```
PublicSubnetBRouteTableAssociation3:
```

```
Type: AWS::EC2::SubnetRouteTableAssociation
```

```
Properties:
```

```
RouteTableId: !Ref PublicRouteTable
```

```
SubnetId: !Ref PublicSubnetC
```

```
#####  
# SECURITY GROUPS  
#####  
  
VPCEndpointSecurityGroup:  
  Type: 'AWS::EC2::SecurityGroup'  
  Properties:  
    GroupDescription: Allow TLS for VPC Endpoint  
    VpcId: !Ref AppVPC  
    SecurityGroupIngress:  
      - IpProtocol: tcp  
        FromPort: 443  
        ToPort: 443  
        CidrIp: !GetAtt AppVPC.CidrBlock  
  
EC2SecurityGroup:  
  Type: 'AWS::EC2::SecurityGroup'  
  Properties:  
    GroupDescription: Default EC2 Instance SG  
    VpcId: !Ref AppVPC  
  
#####  
# VPC ENDPOINTS  
#####  
  
VPCEndpointGatewayS3:  
  Type: 'AWS::EC2::VPCEndpoint'  
  Properties:  
    ServiceName: !Sub 'com.amazonaws.${AWS::Region}.s3'  
    VpcEndpointType: Gateway  
    VpcId: !Ref AppVPC  
    RouteTableIds:  
      - !Ref PrivateRouteTable  
  
VPCEndpointInterfaceSSM:  
  Type: 'AWS::EC2::VPCEndpoint'  
  Properties:  
    VpcEndpointType: Interface  
    PrivateDnsEnabled: false  
    SubnetIds:  
      - !Ref PrivateSubnetA  
      - !Ref PrivateSubnetB
```

```
SecurityGroupIds:
  - !Ref VPCEndpointSecurityGroup
ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ssm'
VpcId: !Ref AppVPC
```

```
VPCEndpointInterfaceEc2messages:
  Type: 'AWS::EC2::VPCEndpoint'
  Properties:
    VpcEndpointType: Interface
    PrivateDnsEnabled: false
    SubnetIds:
      - !Ref PrivateSubnetA
      - !Ref PrivateSubnetB
      - !Ref PrivateSubnetC
    SecurityGroupIds:
      - !Ref VPCEndpointSecurityGroup
    ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ec2messages'
    VpcId: !Ref AppVPC
```

```
VPCEndpointInterfaceSsmmessages:
  Type: 'AWS::EC2::VPCEndpoint'
  Properties:
    VpcEndpointType: Interface
    PrivateDnsEnabled: false
    SubnetIds:
      - !Ref PrivateSubnetA
      - !Ref PrivateSubnetB
      - !Ref PrivateSubnetC
    SecurityGroupIds:
      - !Ref VPCEndpointSecurityGroup
    ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ssmmessages'
    VpcId: !Ref AppVPC
```

```
VPCEndpointInterfaceSignin:
  Type: 'AWS::EC2::VPCEndpoint'
  Properties:
    VpcEndpointType: Interface
    PrivateDnsEnabled: false
    SubnetIds:
      - !Ref PrivateSubnetA
      - !Ref PrivateSubnetB
      - !Ref PrivateSubnetC
    SecurityGroupIds:
      - !Ref VPCEndpointSecurityGroup
```

```

ServiceName: !Sub 'com.amazonaws.${AWS::Region}.signin'
VpcId: !Ref AppVPC

```

```

VPCEndpointInterfaceConsole:

```

```

  Type: 'AWS::EC2::VPCEndpoint'

```

```

  Properties:

```

```

    VpcEndpointType: Interface

```

```

    PrivateDnsEnabled: false

```

```

    SubnetIds:

```

```

      - !Ref PrivateSubnetA

```

```

      - !Ref PrivateSubnetB

```

```

      - !Ref PrivateSubnetC

```

```

    SecurityGroupIds:

```

```

      - !Ref VPCEndpointSecurityGroup

```

```

  ServiceName: !Sub 'com.amazonaws.${AWS::Region}.console'

```

```

  VpcId: !Ref AppVPC

```

```

#####

```

```

# ROUTE53 RESOURCES

```

```

#####

```

```

ConsoleHostedZone:

```

```

  Type: "AWS::Route53::HostedZone"

```

```

  Properties:

```

```

    HostedZoneConfig:

```

```

      Comment: 'Console VPC Endpoint Hosted Zone'

```

```

      Name: 'console.aws.amazon.com'

```

```

    VPCs:

```

```

      -

```

```

        VPCId: !Ref AppVPC

```

```

        VPCRegion: !Ref "AWS::Region"

```

```

ConsoleRecordGlobal:

```

```

  Type: AWS::Route53::RecordSet

```

```

  Properties:

```

```

    HostedZoneId: !Ref 'ConsoleHostedZone'

```

```

    Name: 'console.aws.amazon.com'

```

```

    AliasTarget:

```

```

      DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt

```

```

VPCEndpointInterfaceConsole.DnsEntries]]]

```

```

      HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt

```

```

VPCEndpointInterfaceConsole.DnsEntries]]]

```

```

    Type: A

```

```
GlobalConsoleRecord:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref 'ConsoleHostedZone'
    Name: 'global.console.aws.amazon.com'
    AliasTarget:
      DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
    Type: A

ConsoleS3ProxyRecordGlobal:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref 'ConsoleHostedZone'
    Name: 's3.console.aws.amazon.com'
    AliasTarget:
      DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
    Type: A

ConsoleSupportProxyRecordGlobal:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref 'ConsoleHostedZone'
    Name: "support.console.aws.amazon.com"
    AliasTarget:
      DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
    Type: A

ExplorerProxyRecordGlobal:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref 'ConsoleHostedZone'
    Name: "resource-explorer.console.aws.amazon.com"
    AliasTarget:
      DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
```

```
    HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
```

```
    Type: A
```

```
WidgetProxyRecord:
```

```
    Type: AWS::Route53::RecordSet
```

```
    Properties:
```

```
        HostedZoneId: !Ref 'ConsoleHostedZone'
```

```
        Name: "*.widget.console.aws.amazon.com"
```

```
        AliasTarget:
```

```
            DNSName: !Select ["1", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],,],]
```

```
            HostedZoneId: !Select ["0", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],,],]
```

```
            Type: A
```

```
ConsoleRecordRegional:
```

```
    Type: AWS::Route53::RecordSet
```

```
    Properties:
```

```
        HostedZoneId: !Ref 'ConsoleHostedZone'
```

```
        Name: !Sub "${AWS::Region}.console.aws.amazon.com"
```

```
        AliasTarget:
```

```
            DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
```

```
            HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
```

```
            Type: A
```

```
ConsoleRecordRegionalMultiSession:
```

```
    Type: AWS::Route53::RecordSet
```

```
    Properties:
```

```
        HostedZoneId: !Ref 'ConsoleHostedZone'
```

```
        Name: !Sub "*.${AWS::Region}.console.aws.amazon.com"
```

```
        AliasTarget:
```

```
            DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
```

```
            HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
```

```
            Type: A
```

```
SigninHostedZone:
```

```
    Type: "AWS::Route53::HostedZone"
```

```
    Properties:
```

```
        HostedZoneConfig:
```

```

    Comment: 'Signin VPC Endpoint Hosted Zone'
    Name: 'signin.aws.amazon.com'
    VPCs:
      -
        VPCId: !Ref AppVPC
        VPCRegion: !Ref "AWS::Region"

```

SigninRecordGlobal:

```

    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: 'signin.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

```

SigninRecordRegional:

```

    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: !Sub "${AWS::Region}.signin.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

```

```

#####
# EC2 INSTANCE
#####

```

Ec2InstanceRole:

```

    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          -
            Effect: Allow
            Principal:

```

```
    Service:
      - ec2.amazonaws.com
    Action:
      - sts:AssumeRole
    Path: /
    ManagedPolicyArns:
      - arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore

Ec2InstanceProfile:
  Type: AWS::IAM::InstanceProfile
  Properties:
    Path: /
    Roles:
      - !Ref Ec2InstanceRole

EC2WinInstance:
  Type: 'AWS::EC2::Instance'
  Properties:
    ImageId: !Ref LatestWindowsAmiId
    IamInstanceProfile: !Ref Ec2InstanceProfile
    KeyName: !Ref Ec2KeyPair
    InstanceType:
      Ref: InstanceTypeParameter
    SubnetId: !Ref PrivateSubnetA
    SecurityGroupIds:
      - Ref: EC2SecurityGroup
    BlockDeviceMappings:
      - DeviceName: /dev/sda1
        Ebs:
          VolumeSize: 50
    Tags:
      - Key: "Name"
        Value: "Console VPCE test instance"
```


Pour configurer un réseau

1. Connectez-vous au compte de gestion de votre organisation et ouvrez la [console CloudFormation](#).
2. Sélectionnez Créer la pile.
3. Choisissez Avec de nouvelles ressources (standard). Téléchargez le fichier CloudFormation modèle que vous avez créé précédemment, puis choisissez Next.

4. Entrez un nom pour la pile, tel que **PrivateConsoleNetworkForS3**, puis choisissez Suivant.
5. Pour VPC et sous-réseaux, entrez vos plages CIDR d'adresses IP préférées ou utilisez les valeurs par défaut fournies. Si vous utilisez les valeurs par défaut, vérifiez qu'elles ne se chevauchent pas avec les ressources VPC existantes dans votre. Compte AWS
6. Pour le KeyPair paramètre Ec2, sélectionnez-en une parmi les paires de clés Amazon EC2 existantes dans votre compte. Si vous ne disposez pas d'une paire de clés Amazon EC2 existante, vous devez en créer une avant de passer à l'étape suivante. Pour plus d'informations, consultez la section [Création d'une paire de clés à l'aide d'Amazon EC2](#) dans le guide de l'utilisateur Amazon EC2.
7. Sélectionnez Créer la pile.
8. Une fois la pile créée, choisissez l'onglet Ressources pour afficher les ressources qui ont été créées.

Pour vous connecter à l'instance Amazon EC2

1. Connectez-vous au compte de gestion de votre organisation et ouvrez la [console Amazon EC2](#).
2. Dans le panneau de navigation, choisissez Instances.
3. Sur la page Instances, sélectionnez l'instance de test Console VPCE créée par le CloudFormation modèle. Choisissez ensuite Connect (Connecter).

 Note

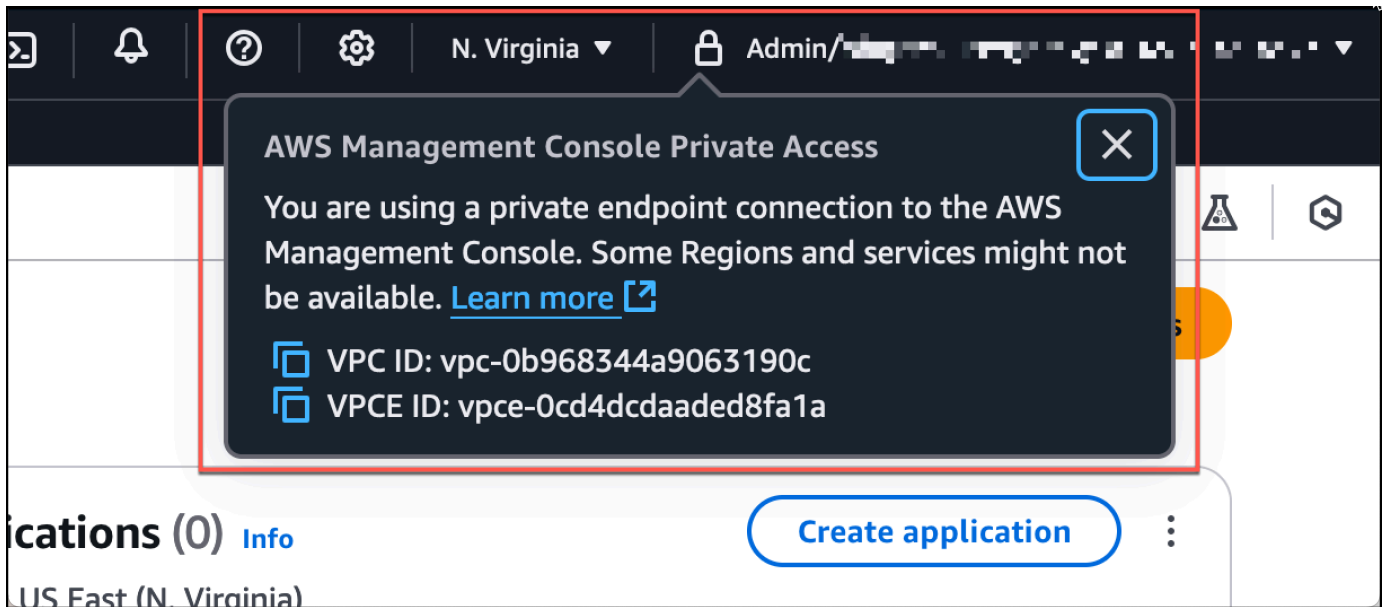
Cet exemple utilise Fleet Manager, une fonctionnalité de AWS Systems Manager Explorer, pour se connecter à votre serveur Windows. Plusieurs minutes peuvent être nécessaires pour démarrer la connexion.

4. Sur la page Se connecter à l'instance, choisissez Client RDP, puis Connexion à l'aide du gestionnaire de parc.
5. Choisissez Bureau à distance Fleet Manager.
6. Pour obtenir le mot de passe administratif de l'instance Amazon EC2 et accéder au bureau Windows via l'interface Web, utilisez la clé privée associée à la paire de clés Amazon EC2 que vous avez utilisée lors CloudFormation de la création du modèle.
7. À partir de l'instance Windows Amazon EC2, ouvrez-la AWS Management Console dans le navigateur.

- Après vous être connecté avec vos AWS informations d'identification, ouvrez la [console Amazon S3](#) et vérifiez que vous êtes connecté via AWS Management Console Private Access.

Pour tester la configuration de l'accès AWS Management Console privé

- Connectez-vous au compte de gestion de votre organisation et ouvrez la [console Amazon S3](#).
- Choisissez l'icône de verrouillage dans la barre de navigation pour afficher le point de terminaison de VPC en cours d'utilisation. La capture d'écran suivante montre l'emplacement de l'icône de verrouillage privé et les informations sur le VPC.



Configuration des tests avec Amazon WorkSpaces

Amazon vous WorkSpaces permet de fournir des ordinateurs de bureau Windows, Amazon Linux ou Ubuntu Linux virtuels basés sur le cloud pour vos utilisateurs, connus sous WorkSpaces le nom de. Vous pouvez rapidement ajouter ou supprimer des utilisateurs à mesure que vos besoins évoluent. Les utilisateurs peuvent accéder à leurs bureaux virtuels à partir de plusieurs appareils ou navigateurs web. Pour en savoir plus WorkSpaces, consultez le [guide d' WorkSpaces administration Amazon](#).

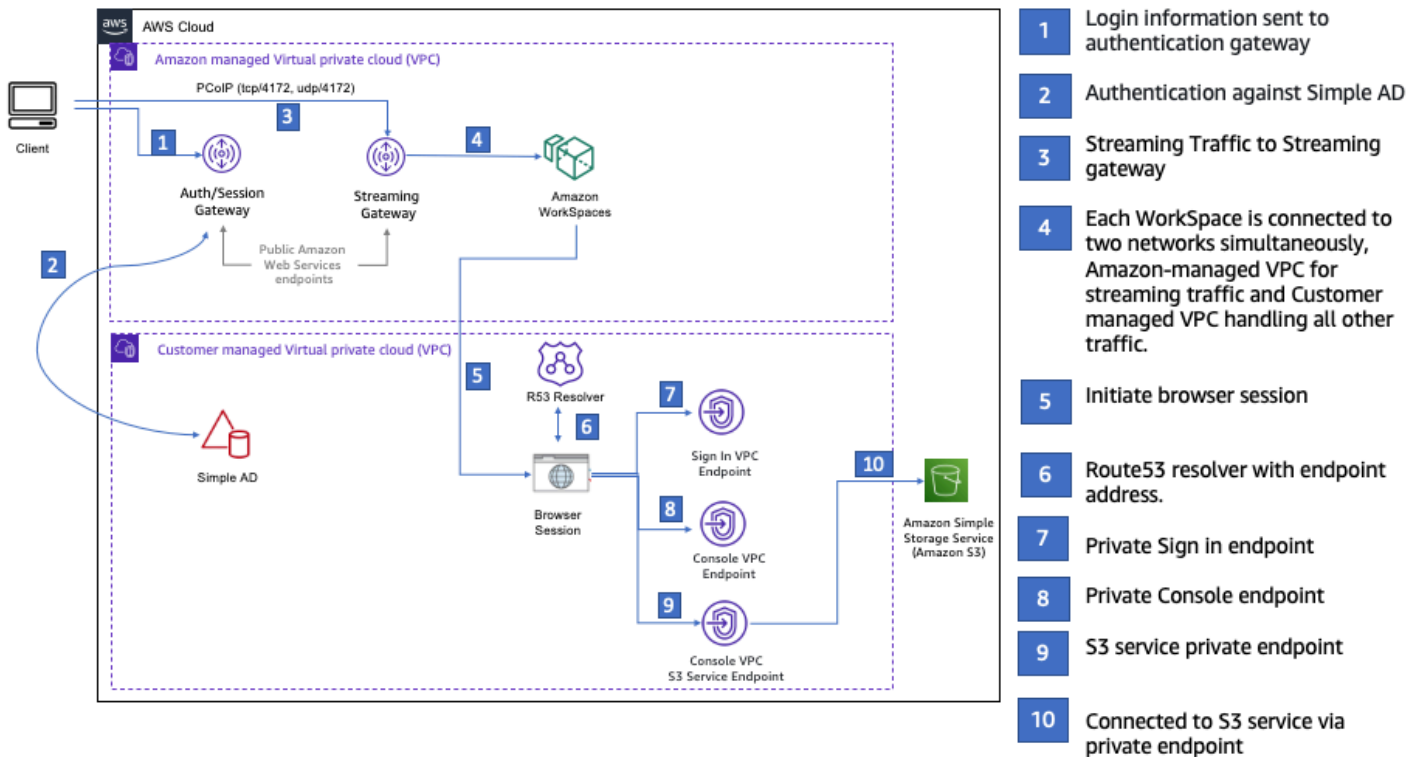
L'exemple de cette section décrit un environnement de test dans lequel un environnement utilisateur utilise un navigateur Web exécuté sur un WorkSpace pour se connecter à AWS Management Console Private Access. L'utilisateur accède ensuite à la console Amazon Simple Storage Service. Cela WorkSpace vise à simuler l'expérience d'un utilisateur professionnel utilisant un ordinateur

portable sur un réseau connecté à un VPC, y accédant AWS Management Console depuis son navigateur.

Ce didacticiel permet AWS CloudFormation de créer et de configurer la configuration du réseau et un répertoire Active Directory simple à utiliser, WorkSpaces ainsi que des instructions étape par étape pour configurer un à WorkSpace l'aide du AWS Management Console.

Le schéma suivant décrit le flux de travail permettant d'utiliser un WorkSpace pour tester une configuration d'accès AWS Management Console privé. Il montre la relation entre un client WorkSpace, un VPC géré par Amazon et un VPC géré par le client.

- Private Hosted Zone: amazon.com**
- console.aws.amazon.com
 - region.console.aws.amazon.com
 - signin.aws.amazon.com
 - region.signin.aws.amazon.com
 - resource-explorer.console.aws.amazon.com
 - s3.console.aws.amazon.com
 - support.console.aws.amazon.com
 - global.console.aws.amazon.com



Copiez le CloudFormation modèle suivant et enregistrez-le dans un fichier que vous utiliserez à l'étape 3 de la procédure de configuration d'un réseau.

AWS Management Console CloudFormation Modèle d'environnement d'accès privé

Description: |

AWS Management Console Private Access.

Parameters:

VpcCIDR:

Type: String

Default: 172.16.0.0/16

Description: CIDR range for VPC

PublicSubnet1CIDR:

Type: String

Default: 172.16.1.0/24

Description: CIDR range for Public Subnet A

PublicSubnet2CIDR:

Type: String

Default: 172.16.0.0/24

Description: CIDR range for Public Subnet B

PrivateSubnet1CIDR:

Type: String

Default: 172.16.4.0/24

Description: CIDR range for Private Subnet A

PrivateSubnet2CIDR:

Type: String

Default: 172.16.5.0/24

Description: CIDR range for Private Subnet B

DSAdminPasswordResourceName:

Type: String

Default: ADAdminSecret

Description: Password for directory services admin

Amazon WorkSpaces is available in a subset of the Availability Zones for each supported Region.

<https://docs.aws.amazon.com/workspaces/latest/adminguide/azs-workspaces.html>

Mappings:

RegionMap:

us-east-1:

az1: use1-az2

az2: use1-az4

az3: use1-az6

us-west-2:

az1: usw2-az1

```
    az2: usw2-az2
    az3: usw2-az3
ap-south-1:
    az1: aps1-az1
    az2: aps1-az2
    az3: aps1-az3
ap-northeast-2:
    az1: apne2-az1
    az2: apne2-az3
ap-southeast-1:
    az1: apse1-az1
    az2: apse1-az2
ap-southeast-2:
    az1: apse2-az1
    az2: apse2-az3
ap-northeast-1:
    az1: apne1-az1
    az2: apne1-az4
ca-central-1:
    az1: cac1-az1
    az2: cac1-az2
eu-central-1:
    az1: euc1-az2
    az2: euc1-az3
eu-west-1:
    az1: euw1-az1
    az2: euw1-az2
eu-west-2:
    az1: euw2-az2
    az2: euw2-az3
sa-east-1:
    az1: sae1-az1
    az2: sae1-az3
```

Resources:

```
iamLambdaExecutionRole:
  Type: AWS::IAM::Role
  Properties:
    AssumeRolePolicyDocument:
      Version: 2012-10-17
      Statement:
        - Effect: Allow
          Principal:
```

```
    Service:
      - lambda.amazonaws.com
    Action:
      - 'sts:AssumeRole'
  ManagedPolicyArns:
    - arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole
  Policies:
    - PolicyName: describe-ec2-az
      PolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Action:
              - 'ec2:DescribeAvailabilityZones'
            Resource: '*'
  MaxSessionDuration: 3600
  Path: /service-role/

fnZoneIdtoZoneName:
  Type: AWS::Lambda::Function
  Properties:
    Runtime: python3.8
    Handler: index.lambda_handler
    Code:
      ZipFile: |
        import boto3
        import cfnresponse

        def zoneId_to_zoneName(event, context):
            responseData = {}
            ec2 = boto3.client('ec2')
            describe_az = ec2.describe_availability_zones()
            for az in describe_az['AvailabilityZones']:
                if event['ResourceProperties']['ZoneId'] == az['ZoneId']:
                    responseData['ZoneName'] = az['ZoneName']
                    cfnresponse.send(event, context, cfnresponse.SUCCESS,
responseData, str(az['ZoneId']))

            def no_op(event, context):
                print(event)
                responseData = {}
                cfnresponse.send(event, context, cfnresponse.SUCCESS, responseData,
str(event['RequestId']))
```

```
    def lambda_handler(event, context):
        if event['RequestType'] == ('Create' or 'Update'):
            zoneId_to_zoneName(event, context)
        else:
            no_op(event, context)
    Role: !GetAtt iamLambdaExecutionRole.Arn

getAZ1:
  Type: "Custom::zone-id-zone-name"
  Properties:
    ServiceToken: !GetAtt fnZoneIdtoZoneName.Arn
    ZoneId: !FindInMap [ RegionMap, !Ref 'AWS::Region', az1 ]
getAZ2:
  Type: "Custom::zone-id-zone-name"
  Properties:
    ServiceToken: !GetAtt fnZoneIdtoZoneName.Arn
    ZoneId: !FindInMap [ RegionMap, !Ref 'AWS::Region', az2 ]

#####
# VPC AND SUBNETS
#####

AppVPC:
  Type: 'AWS::EC2::VPC'
  Properties:
    CidrBlock: !Ref VpcCIDR
    InstanceTenancy: default
    EnableDnsSupport: true
    EnableDnsHostnames: true

PublicSubnetA:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PublicSubnet1CIDR
    MapPublicIpOnLaunch: true
    AvailabilityZone: !GetAtt getAZ1.ZoneName

PublicSubnetB:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PublicSubnet2CIDR
    MapPublicIpOnLaunch: true
```

```
AvailabilityZone: !GetAtt getAZ2.ZoneName
```

```
PrivateSubnetA:
```

```
Type: 'AWS::EC2::Subnet'
```

```
Properties:
```

```
VpcId: !Ref AppVPC
```

```
CidrBlock: !Ref PrivateSubnet1CIDR
```

```
AvailabilityZone: !GetAtt getAZ1.ZoneName
```

```
PrivateSubnetB:
```

```
Type: 'AWS::EC2::Subnet'
```

```
Properties:
```

```
VpcId: !Ref AppVPC
```

```
CidrBlock: !Ref PrivateSubnet2CIDR
```

```
AvailabilityZone: !GetAtt getAZ2.ZoneName
```

```
InternetGateway:
```

```
Type: AWS::EC2::InternetGateway
```

```
InternetGatewayAttachment:
```

```
Type: AWS::EC2::VPCGatewayAttachment
```

```
Properties:
```

```
InternetGatewayId: !Ref InternetGateway
```

```
VpcId: !Ref AppVPC
```

```
NatGatewayEIP:
```

```
Type: AWS::EC2::EIP
```

```
DependsOn: InternetGatewayAttachment
```

```
NatGateway:
```

```
Type: AWS::EC2::NatGateway
```

```
Properties:
```

```
AllocationId: !GetAtt NatGatewayEIP.AllocationId
```

```
SubnetId: !Ref PublicSubnetA
```

```
#####
```

```
# Route Tables
```

```
#####
```

```
PrivateRouteTable:
```

```
Type: 'AWS::EC2::RouteTable'
```

```
Properties:
```

```
VpcId: !Ref AppVPC
```

```
DefaultPrivateRoute:
  Type: AWS::EC2::Route
  Properties:
    RouteTableId: !Ref PrivateRouteTable
    DestinationCidrBlock: 0.0.0.0/0
    NatGatewayId: !Ref NatGateway

PrivateSubnetRouteTableAssociation1:
  Type: 'AWS::EC2::SubnetRouteTableAssociation'
  Properties:
    RouteTableId: !Ref PrivateRouteTable
    SubnetId: !Ref PrivateSubnetA

PrivateSubnetRouteTableAssociation2:
  Type: 'AWS::EC2::SubnetRouteTableAssociation'
  Properties:
    RouteTableId: !Ref PrivateRouteTable
    SubnetId: !Ref PrivateSubnetB

PublicRouteTable:
  Type: AWS::EC2::RouteTable
  Properties:
    VpcId: !Ref AppVPC

DefaultPublicRoute:
  Type: AWS::EC2::Route
  DependsOn: InternetGatewayAttachment
  Properties:
    RouteTableId: !Ref PublicRouteTable
    DestinationCidrBlock: 0.0.0.0/0
    GatewayId: !Ref InternetGateway

PublicSubnetARouteTableAssociation1:
  Type: AWS::EC2::SubnetRouteTableAssociation
  Properties:
    RouteTableId: !Ref PublicRouteTable
    SubnetId: !Ref PublicSubnetA

PublicSubnetBRouteTableAssociation2:
  Type: AWS::EC2::SubnetRouteTableAssociation
  Properties:
    RouteTableId: !Ref PublicRouteTable
    SubnetId: !Ref PublicSubnetB
```

```
#####  
# SECURITY GROUPS  
#####  
  
VPCEndpointSecurityGroup:  
  Type: 'AWS::EC2::SecurityGroup'  
  Properties:  
    GroupDescription: Allow TLS for VPC Endpoint  
    VpcId: !Ref AppVPC  
    SecurityGroupIngress:  
      - IpProtocol: tcp  
        FromPort: 443  
        ToPort: 443  
        CidrIp: !GetAtt AppVPC.CidrBlock  
  
#####  
# VPC ENDPOINTS  
#####  
  
VPCEndpointGatewayS3:  
  Type: 'AWS::EC2::VPCEndpoint'  
  Properties:  
    ServiceName: !Sub 'com.amazonaws.${AWS::Region}.s3'  
    VpcEndpointType: Gateway  
    VpcId: !Ref AppVPC  
    RouteTableIds:  
      - !Ref PrivateRouteTable  
  
VPCEndpointInterfaceSignin:  
  Type: 'AWS::EC2::VPCEndpoint'  
  Properties:  
    VpcEndpointType: Interface  
    PrivateDnsEnabled: false  
    SubnetIds:  
      - !Ref PrivateSubnetA  
      - !Ref PrivateSubnetB  
    SecurityGroupIds:  
      - !Ref VPCEndpointSecurityGroup  
    ServiceName: !Sub 'com.amazonaws.${AWS::Region}.signin'  
    VpcId: !Ref AppVPC  
  
VPCEndpointInterfaceConsole:  
  Type: 'AWS::EC2::VPCEndpoint'
```

Properties:

```
VpcEndpointType: Interface
PrivateDnsEnabled: false
SubnetIds:
  - !Ref PrivateSubnetA
  - !Ref PrivateSubnetB
SecurityGroupIds:
  - !Ref VPCEndpointSecurityGroup
ServiceName: !Sub 'com.amazonaws.${AWS::Region}.console'
VpcId: !Ref AppVPC
```

```
#####
```

```
# ROUTE53 RESOURCES
```

```
#####
```

ConsoleHostedZone:

```
Type: "AWS::Route53::HostedZone"
Properties:
  HostedZoneConfig:
    Comment: 'Console VPC Endpoint Hosted Zone'
    Name: 'console.aws.amazon.com'
  VPCs:
    -
      VPCId: !Ref AppVPC
      VPCRegion: !Ref "AWS::Region"
```

ConsoleRecordGlobal:

```
Type: AWS::Route53::RecordSet
Properties:
  HostedZoneId: !Ref 'ConsoleHostedZone'
  Name: 'console.aws.amazon.com'
  AliasTarget:
    DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
    HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
  Type: A
```

GlobalConsoleRecord:

```
Type: AWS::Route53::RecordSet
Properties:
  HostedZoneId: !Ref 'ConsoleHostedZone'
  Name: 'global.console.aws.amazon.com'
  AliasTarget:
```

```
    DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
    HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
    Type: A

ConsoleS3ProxyRecordGlobal:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref 'ConsoleHostedZone'
    Name: 's3.console.aws.amazon.com'
    AliasTarget:
      DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

ConsoleSupportProxyRecordGlobal:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref 'ConsoleHostedZone'
    Name: "support.console.aws.amazon.com"
    AliasTarget:
      DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

ExplorerProxyRecordGlobal:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref 'ConsoleHostedZone'
    Name: "resource-explorer.console.aws.amazon.com"
    AliasTarget:
      DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

WidgetProxyRecord:
  Type: AWS::Route53::RecordSet
```

```

Properties:
  HostedZoneId: !Ref "ConsoleHostedZone"
  Name: "*.widget.console.aws.amazon.com"
  AliasTarget:
    DNSName: !Select ["1", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],,],]
    HostedZoneId: !Select ["0", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],,],]
  Type: A

ConsoleRecordRegional:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref 'ConsoleHostedZone'
    Name: !Sub "${AWS::Region}.console.aws.amazon.com"
    AliasTarget:
      DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
    Type: A

ConsoleRecordRegionalMultiSession:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref 'ConsoleHostedZone'
    Name: !Sub ".*${AWS::Region}.console.aws.amazon.com"
    AliasTarget:
      DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
    Type: A

SigninHostedZone:
  Type: "AWS::Route53::HostedZone"
  Properties:
    HostedZoneConfig:
      Comment: 'Signin VPC Endpoint Hosted Zone'
      Name: 'signin.aws.amazon.com'
    VPCs:
      -
        VPCId: !Ref AppVPC
        VPCRegion: !Ref "AWS::Region"

```

```

SigninRecordGlobal:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref 'SigninHostedZone'
    Name: 'signin.aws.amazon.com'
    AliasTarget:
      DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
      HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
    Type: A

SigninRecordRegional:
  Type: AWS::Route53::RecordSet
  Properties:
    HostedZoneId: !Ref 'SigninHostedZone'
    Name: !Sub "${AWS::Region}.signin.aws.amazon.com"
    AliasTarget:
      DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
      HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceSignin.DnsEntries]]]
    Type: A

#####
# WORKSPACE RESOURCES
#####
ADAdminSecret:
  Type: AWS::SecretsManager::Secret
  Properties:
    Name: !Ref DSAdminPasswordResourceName
    Description: "Password for directory services admin"
    GenerateSecretString:
      SecretStringTemplate: '{"username": "Admin"}'
      GenerateStringKey: password
      PasswordLength: 30
      ExcludeCharacters: '"@/\

WorkspaceSimpleDirectory:
  Type: AWS::DirectoryService::SimpleAD
  DependsOn: AppVPC
  Properties:
    Name: "corp.awsconsole.com"

```

```
    Password: '{{resolve:secretsmanager:ADAdminSecret:SecretString:password}}'  
    Size: "Small"  
    VpcSettings:  
      SubnetIds:  
        - Ref: PrivateSubnetA  
        - Ref: PrivateSubnetB  
  
    VpcId:  
      Ref: AppVPC
```

Outputs:**PrivateSubnetA:**

```
Description: Private Subnet A  
Value: !Ref PrivateSubnetA
```

PrivateSubnetB:


```
Description: Private Subnet B  
Value: !Ref PrivateSubnetB
```

WorkspaceSimpleDirectory:

```
Description: Directory to be used for Workspaces  
Value: !Ref WorkspaceSimpleDirectory
```

WorkspacesAdminPassword:

```
Description : "The ARN of the Workspaces admin's password.  Navigate to the Secrets  
Manager in the AWS Console to view the value."  
Value: !Ref ADAdminSecret
```

 Note

Cette configuration test est conçue pour être exécutée dans la région USA Est (Virginie du Nord) (us-east-1).

Pour configurer un réseau

1. Connectez-vous au compte de gestion de votre organisation et ouvrez la [console CloudFormation](#).
2. Sélectionnez Créer la pile.

3. Choisissez Avec de nouvelles ressources (standard). Téléchargez le fichier CloudFormation modèle que vous avez créé précédemment, puis choisissez Next.
4. Entrez un nom pour la pile, tel que **PrivateConsoleNetworkForS3**, puis choisissez Suivant.
5. Pour VPC et sous-réseaux, entrez vos plages CIDR d'adresses IP préférées ou utilisez les valeurs par défaut fournies. Si vous utilisez les valeurs par défaut, vérifiez qu'elles ne se chevauchent pas avec les ressources VPC existantes dans votre. Compte AWS
6. Sélectionnez Créer la pile.
7. Une fois la pile créée, choisissez l'onglet Ressources pour afficher les ressources qui ont été créées.
8. Choisissez l'onglet Sorties pour afficher les valeurs des sous-réseaux privés et de l'annuaire Workspace Simple Directory. Prenez note de ces valeurs, car vous les utiliserez à la quatrième étape de la prochaine procédure de création et de configuration d'un WorkSpace.

La capture d'écran suivante montre l'onglet Sorties qui affiche les valeurs des sous-réseaux privés et de l'annuaire Workspace Simple Directory.

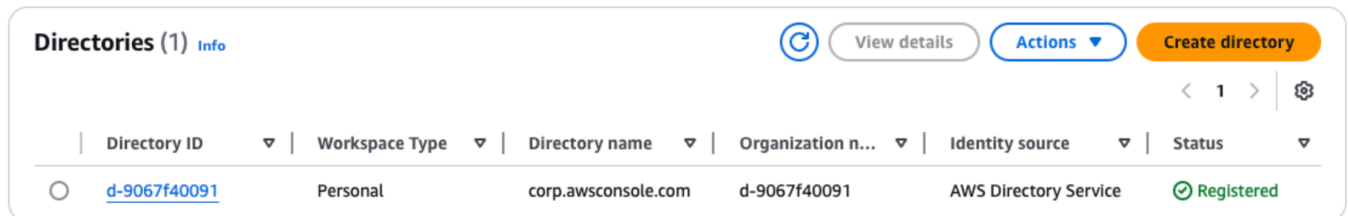
The screenshot shows the AWS Management Console interface for a stack named "PrivateConsoleNetworkForS3". The "Outputs" tab is selected, displaying a table of four outputs. The table has columns for Key, Value, Description, and Export name. The outputs are:

Key	Value	Description	Export name
PrivateSubnetA	subnet-0aea1291fe9eb1b47	Private Subnet A	-
PrivateSubnetB	subnet-04f6adc31f08a09b6	Private Subnet B	-
WorkspacesAdminPassword	arn:aws:secretsmanager:us-east-1:851725487077:secret:ADAdminSecret-GAwM8i	The ARN of the Workspaces admin's password. Navigate to the Secrets Manager in the AWS Console to view the value.	-
WorkspaceSimpleDirectory	d-9067f40091	Directory to be used for Workspaces	-

Maintenant que vous avez créé votre réseau, suivez les procédures suivantes pour créer et accéder à un WorkSpace.

Pour créer un WorkSpace

1. Ouvrez la [WorkSpaces console](#).
2. Dans le volet de navigation, choisissez Directories (Annuaire).
3. Sur la page Annuaire, vérifiez que le statut de l'annuaire est Actif. La capture d'écran suivante montre une page Annuaire avec un annuaire actif.



4. Pour utiliser un répertoire dans WorkSpaces, vous devez l'enregistrer. Dans le volet de navigation, choisissez WorkSpaces, puis choisissez Create WorkSpaces.
5. Pour Sélectionner un annuaire, choisissez l'annuaire créé par CloudFormation dans la procédure précédente. Dans le menu Actions, choisissez Enregistrer.
6. Pour la sélection des sous-réseaux, sélectionnez les deux sous-réseaux privés indiqués à l'étape 9 de la procédure précédente.
7. Sélectionnez Activer les autorisations en libre-service, puis choisissez Enregistrer.
8. Une fois le répertoire enregistré, continuez à créer le WorkSpace. Sélectionnez l'annuaire enregistré, puis choisissez Suivant.
9. Sur la page Créer des utilisateurs, choisissez Créer un utilisateur supplémentaire. Entrez votre nom et votre e-mail pour vous permettre d'utiliser le WorkSpace. Vérifiez que l'adresse e-mail est valide car les informations de WorkSpace connexion sont envoyées à cette adresse e-mail.
10. Choisissez Suivant.
11. Sur la page Identifier les utilisateurs, sélectionnez l'utilisateur que vous avez créé à l'étape 9, puis choisissez Suivant.
12. Sur la page Sélectionner un bundle, choisissez Standard avec Amazon Linux 2, puis choisissez Suivant.
13. Utilisez les paramètres par défaut pour le mode d'exécution et la personnalisation utilisateur, puis sélectionnez Créer des instances WorkSpaces. Le Pending statut WorkSpace commence et passe à Available environ 20 minutes.

14. Lorsque le sera WorkSpace disponible, vous recevrez un e-mail contenant les instructions pour y accéder à l'adresse e-mail que vous avez fournie à l'étape 9.


Une fois connecté à votre WorkSpace, vous pouvez vérifier que vous y accédez à l'aide de votre accès AWS Management Console privé.

Pour accéder à un WorkSpace

1. Ouvrez l'e-mail que vous avez reçu à l'étape 14 de la procédure précédente.
2. Dans l'e-mail, choisissez le lien unique fourni pour configurer votre profil et télécharger le WorkSpaces client.
3. Définissez votre mot de passe.
4. Téléchargez le client de votre choix.
5. Installez et lancez le client. Entrez le code d'enregistrement fourni dans votre e-mail, puis choisissez Enregistrer.
6. Connectez-vous à Amazon à WorkSpaces l'aide des informations d'identification que vous avez créées à l'étape 3.

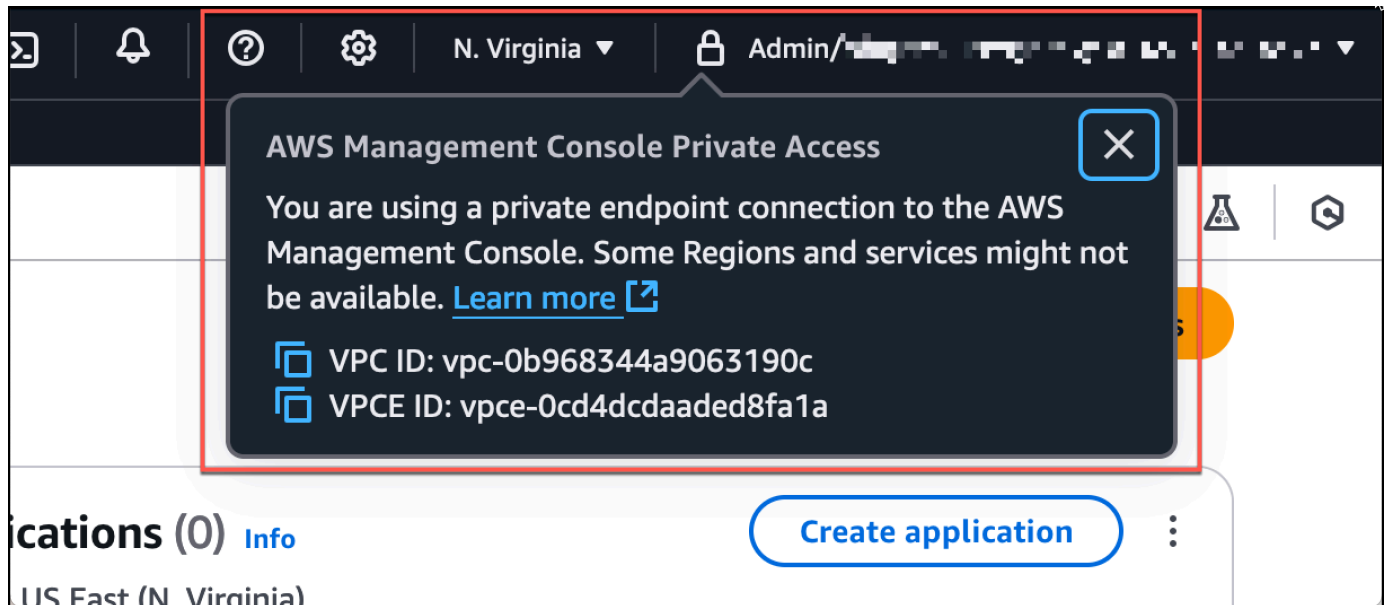
Pour tester la configuration de l'accès AWS Management Console privé

1. À partir de votre WorkSpace, ouvrez votre navigateur. Accédez ensuite à la [AWS Management Console](#) et connectez-vous à l'aide de vos informations d'identification.

 Note

Si vous utilisez Firefox comme navigateur, vérifiez que l'option Activer le DNS sur HTTPS est désactivée dans les paramètres de votre navigateur.

2. Ouvrez la [console Amazon S3](#) où vous pouvez vérifier que vous êtes connecté à l'aide d' AWS Management Console un accès privé.
3. Choisissez l'icône de verrouillage sur la barre de navigation pour afficher le VPC et le point de terminaison d'un VPC en cours d'utilisation. La capture d'écran suivante montre l'emplacement de l'icône de verrouillage privé et les informations sur le VPC.



Configuration test du VPC avec des politiques IAM

Vous pouvez tester davantage votre VPC que vous avez configuré avec Amazon EC2 WorkSpaces ou en déployant des politiques IAM qui limitent l'accès.

La politique suivante refuse l'accès à Amazon S3, sauf si ce dernier utilise le VPC que vous avez spécifié.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "S3:*",
      "Resource": "*",
      "Condition": {
        "StringNotEqualsIfExists": {
          "aws:SourceVpc": "vpc-12345678"
        },
        "Bool": {
          "aws:ViaAwsService": "false"
        }
      }
    }
  ]
}
```

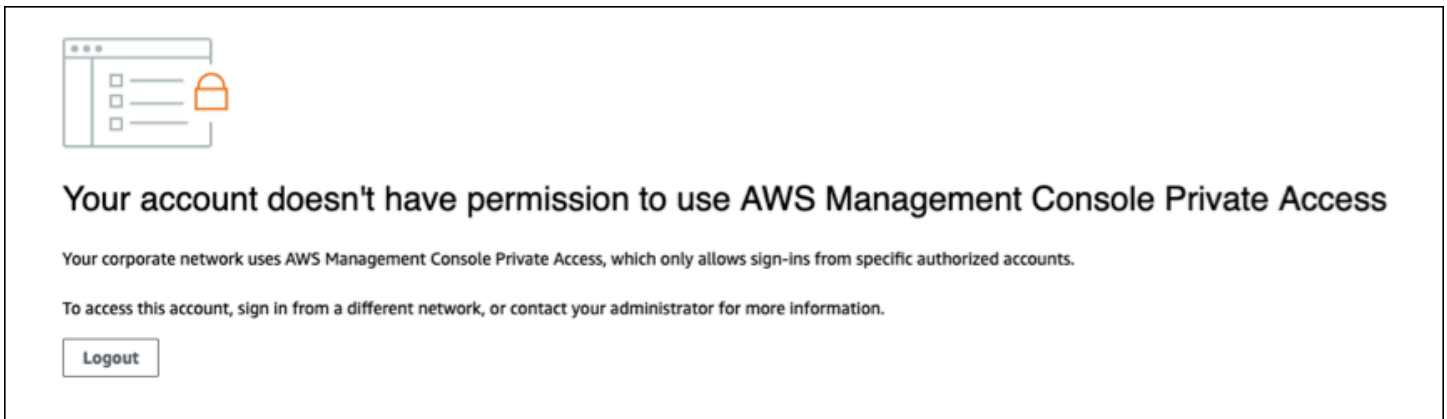
```
    }
  ]
}
```

La politique suivante limite la connexion aux éléments sélectionnés à l'aide Compte AWS IDs d'une politique d'accès AWS Management Console privé pour le point de terminaison de connexion.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalAccount": [
            "AWSAccountID"
          ]
        }
      }
    }
  ]
}
```

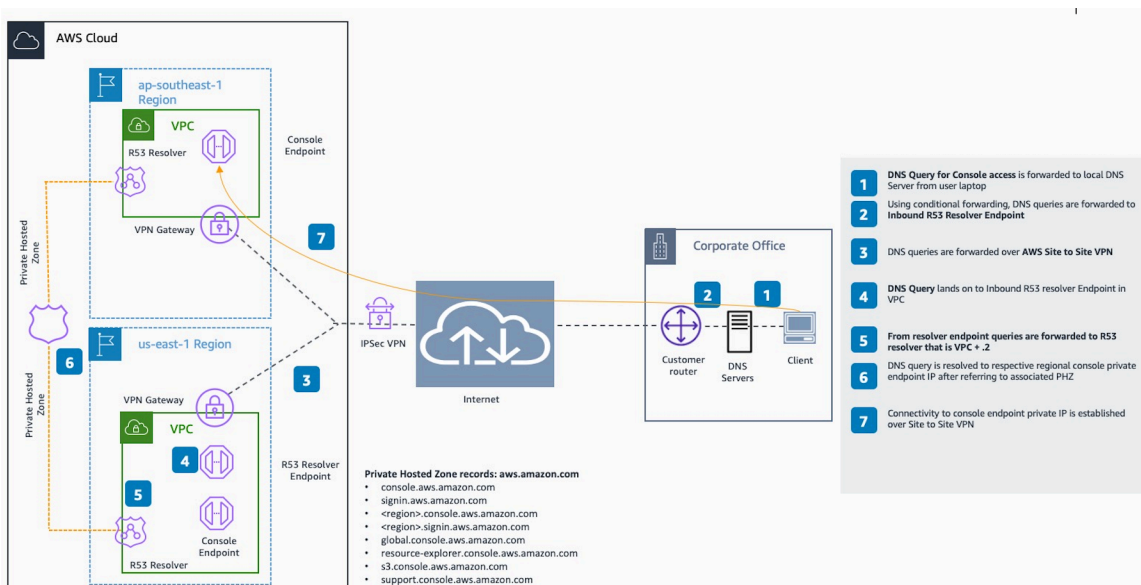
Si vous vous connectez avec une identité qui n'appartient pas à votre compte, la page d'erreur suivante s'affiche.



Architecture de référence

Pour vous connecter en privé à AWS Management Console Private Access depuis un réseau local, vous pouvez utiliser l'option de connexion AWS Site-to-Site VPN à AWS Virtual Private Gateway (VGW). AWS Site-to-Site VPN permet d'accéder à votre réseau distant depuis votre VPC en créant une connexion et en configurant le routage pour faire passer le trafic via la connexion. Pour plus d'informations, consultez la section [Qu'est-ce qu'un VPN de AWS site à site dans le guide de l'utilisateur du AWS Site-to-Site VPN](#). AWS La passerelle privée virtuelle (VGW) est un service régional à haute disponibilité qui fait office de passerelle entre un VPC et le réseau sur site.

AWS Site-to-Site VPN vers AWS Virtual Private Gateway (VGW)



Un élément essentiel de cette conception d'architecture de référence est, en particulier Amazon Route 53 Resolver, le résolveur entrant. Lorsque vous le configurez dans le VPC où les points de terminaison d'accès AWS Management Console privé sont créés, les points de terminaison du

résolveur (interfaces réseau) sont créés dans les sous-réseaux spécifiés. Leurs adresses IP peuvent ensuite être référencées dans des redirecteurs conditionnels sur les serveurs DNS sur site, afin de permettre des requêtes d'enregistrements dans une zone hébergée privée. Lorsque les clients locaux se connectent au AWS Management Console, ils sont routés vers le terminal privé des points de terminaison AWS Management Console d'accès privé. IPs

Avant de configurer la connexion au point de terminaison d'accès AWS Management Console privé, suivez les étapes préalables de configuration des points de terminaison d'accès AWS Management Console privé dans toutes les régions où vous souhaitez accéder AWS Management Console, ainsi que dans la région de l'est des États-Unis (Virginie du Nord), et de configuration de la zone hébergée privée.

AWS Personnalisation de l'expérience utilisateur (UXC)

AWS La personnalisation de l'expérience utilisateur (UXC) est un utilitaire qui permet aux administrateurs de compte de personnaliser l'apparence visuelle du compte AWS Management Console et de gérer ces paramètres au niveau du compte.

Avec UXC, vous pouvez personnaliser les paramètres suivants :

- **Couleur du compte** : vous pouvez définir une couleur pour vos comptes afin de les distinguer visuellement. Par exemple, vous pouvez utiliser le vert pour les comptes de développement, le jaune pour les comptes de test et le rouge pour les comptes de production.
- **Visibilité des services** : vous pouvez contrôler les AWS services qui apparaissent dans la navigation de la console. La visibilité des services simplifie AWS Management Console le fait de n'afficher que les AWS services pertinents pour votre compte.
- **Visibilité des régions** : vous pouvez contrôler AWS les régions qui apparaissent dans le sélecteur de régions. La visibilité des régions simplifie AWS Management Console le fait de n'afficher que les régions pertinentes pour votre compte.

Si vous n'avez pas configuré de paramètre, le comportement par défaut s'applique : tous les services et régions sont visibles, et aucune couleur de compte n'est définie. Vous pouvez rétablir la couleur par défaut du compte en définissant la valeur sur "none". Vous pouvez rétablir les valeurs par défaut des services visibles et des régions en définissant leurs valeurs sur null.

Note

Les `visibleRegions` paramètres `visibleServices` et contrôlent uniquement l'apparence des services et des régions dans le AWS Management Console. Ils ne limitent pas l'accès par le biais de AWS Command Line Interface SDKs, ou autre APIs.

Rubriques

- [Commencer à personnaliser AWS l'expérience utilisateur](#)
- [Enregistrement des appels d'API de personnalisation de l'expérience AWS utilisateur à l'aide AWS CloudTrail](#)
- [Sécurité dans la personnalisation de l'expérience AWS utilisateur](#)

Commencer à personnaliser AWS l'expérience utilisateur

Avec UXC, les administrateurs de compte peuvent configurer des personnalisations de compte pour le. AWS Management Console

Conditions préalables

Avant de commencer, vous avez besoin de ce qui suit :

- Un AWS compte
- Autorisations Gestion des identités et des accès AWS (IAM) appropriées pour UXC. Pour plus d'informations, consultez [Comment fonctionne la personnalisation de AWS l'expérience utilisateur avec IAM](#) et [les politiques AWS gérées pour le AWS Management Console](#).

Accès aux paramètres UXC dans le AWS Management Console

Pour accéder à la couleur du compte dans le AWS Management Console, voir [Accès aux informations du compte dans le AWS Management Console](#). Pour accéder à la visibilité des services et à la visibilité des régions dans le AWS Management Console, voir [Configuration à l' AWS Management Console aide de paramètres unifiés](#).

Pour définir la couleur d'un compte dans la console

1. Connectez-vous à la [AWS Management Console](#).
2. Sur la barre de navigation, choisissez le nom de votre compte.
3. Choisissez Account.
4. Dans les paramètres d'affichage du compte, choisissez une couleur.
5. Choisissez Mettre à jour.

Pour définir des régions visibles dans la console

1. Connectez-vous à la [AWS Management Console](#).
2. Ouvrez les [paramètres unifiés](#).
3. Choisissez Modifier dans la section Régions visibles.
4. Définissez vos régions visibles sur Toutes les régions disponibles ou sélectionnez les régions et configurez votre liste.

5. Sélectionnez Enregistrer les modifications.

Pour définir des services visibles dans la console

1. Connectez-vous à la [AWS Management Console](#).
2. Ouvrez les [paramètres unifiés](#).
3. Choisissez Modifier dans la section Services visibles.
4. Définissez vos services visibles sur Tous les services ou Sélectionnez les services et configurez votre liste.
5. Sélectionnez Enregistrer les modifications.

Accès aux paramètres UXC par programmation

Vous pouvez également gérer les paramètres de personnalisation des comptes par programmation ou sous forme d'infrastructure sous forme de code. Pour plus d'informations, consultez la [référence de l'API de personnalisation de l'expérience AWS utilisateur](#) et la référence du [AWS::UXC::AccountCustomization](#) CloudFormation modèle.

Enregistrement des appels d'API de personnalisation de l'expérience AWS utilisateur à l'aide AWS CloudTrail

AWS La personnalisation de l'expérience utilisateur est intégrée à [AWS CloudTrail](#) un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un Service AWS. CloudTrail capture tous les appels d'API pour UXC sous forme d'événements. Les appels capturés incluent des appels provenant de la console UXC et des appels de code vers les opérations de l'API UXC. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à UXC, l'adresse IP à partir de laquelle la demande a été faite, la date à laquelle elle a été faite et des détails supplémentaires.

CloudTrail est actif dans votre compte Compte AWS lorsque vous créez le compte et vous avez automatiquement accès à l'historique des CloudTrail événements. L'historique des CloudTrail événements fournit un enregistrement consultable, consultable, téléchargeable et immuable des 90 derniers jours des événements de gestion enregistrés dans un. Région AWS Pour plus d'informations, consultez la section [Utilisation de l'historique des CloudTrail événements](#) dans le guide de AWS CloudTrail l'utilisateur. La consultation de CloudTrail l'historique des événements est gratuite.

Pour un enregistrement continu des événements de vos 90 Compte AWS derniers jours, créez un magasin de données sur les événements de Trail ou [CloudTrailLake](#).

Événements de gestion UXC dans CloudTrail

[Les événements de gestion](#) fournissent des informations sur les opérations de gestion effectuées sur les ressources de votre Compte AWS. Ils sont également connus sous le nom opérations de plan de contrôle. Par défaut, CloudTrail enregistre les événements de gestion.

AWS La personnalisation de l'expérience utilisateur enregistre toutes les opérations du plan de contrôle UXC en tant qu'événements de gestion. Pour obtenir la liste des opérations du plan de contrôle de personnalisation de AWS l'expérience utilisateur auxquelles UXC se connecte CloudTrail, consultez la [référence de l'API de personnalisation de AWS l'expérience utilisateur](#).

Exemples d'événements UXC

Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'opération d'API demandée, la date et l'heure de l'opération, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics. Les événements n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre un CloudTrail événement illustrant l'opération.

```
{
  "eventVersion" : "1.09",
  "userIdentity" : {
    "type" : "AssumedRole",
    "principalId" : "AIDACKCEVSQ6C2EXAMPLE:jdoe",
    "arn" : "arn:aws:sts::111122223333:assumed-role/user/jdoe",
    "accountId" : "111122223333",
    "accessKeyId" : "AKIAIOSFODNN7EXAMPLE",
    "sessionContext" : {
      "sessionIssuer" : {
        "type" : "Role",
        "principalId" : "AIDACKCEVSQ6C2EXAMPLE",
        "arn" : "arn:aws:iam::111122223333:role/user",
        "accountId" : "111122223333",
        "userName" : "jdoe"
      },
      "webIdFederationData" : { },
      "attributes" : {
```

```
        "creationDate" : "2022-12-09T23:48:51Z",
        "mfaAuthenticated" : "false"
    }
},
"eventTime" : "2022-12-09T23:50:03Z",
"eventSource" : "uxc.amazonaws.com",
"eventName" : "GetAccountColor",
"awsRegion" : "us-east-2",
"sourceIPAddress" : "10.24.34.3",
"userAgent" : "PostmanRuntime/7.43.4",
"requestParameters" : null,
"responseElements" : null,
"requestID" : "543db7ab-b4b2-11e9-8925-d139e92a1fe8",
"eventID" : "5b2805a5-3e06-4437-a7a2-b5fdb5cbb4e2",
"readOnly" : true,
"eventType" : "AwsApiCall",
"managementEvent" : true,
"recipientAccountId" : "111122223333",
"eventCategory" : "Management"
}
```

Pour plus d'informations sur le contenu des CloudTrail enregistrements, voir [le contenu des CloudTrail enregistrements](#) dans le Guide de AWS CloudTrail l'utilisateur.

Sécurité dans la personnalisation de l'expérience AWS utilisateur

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 ceci 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 la personnalisation de AWS l'expérience utilisateur, 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 l'utilisation de l'UXC. Les rubriques suivantes expliquent comment configurer l'UXC pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources UXC.

Rubriques

- [Identity and Access Management pour la personnalisation de AWS l'expérience utilisateur](#)

Identity and Access Management pour la personnalisation de AWS l'expérience utilisateur

AWS La personnalisation de l'expérience utilisateur (UXC) utilise des politiques IAM pour gérer l'accès aux opérations d'API UXC.

Gestion des identités et des accès AWS (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 les ressources de personnalisation de l'expérience utilisateur. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- [Public ciblé](#)
- [Authentification par des identités](#)
- [Gestion de l'accès à l'aide de politiques](#)
- [Comment fonctionne la personnalisation de l'expérience AWS utilisateur avec IAM](#)
- [Exemples de politiques basées sur l'identité pour la personnalisation de AWS l'expérience utilisateur](#)

Public ciblé

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

- Utilisateur du service : demandez des autorisations à votre administrateur si vous ne pouvez pas accéder aux fonctionnalités (voir [Résolution des problèmes AWS d'expérience utilisateur Personnalisation de l'identité et de l'accès](#))
- Administrateur du service : déterminez l'accès des utilisateurs et soumettez les demandes d'autorisation (voir [Comment fonctionne la personnalisation de l'expérience AWS utilisateur avec IAM](#))
- Administrateur IAM : rédigez des politiques pour gérer l'accès (voir [Exemples de politiques basées sur l'identité pour la personnalisation de AWS l'expérience utilisateur](#))

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 en tant qu'utilisateur IAM ou en assumant un rôle IAM.

Utilisateur racine d'un compte AWS

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

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

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une seule identité de connexion appelée utilisateur Compte AWS root qui dispose d'un accès complet à toutes Services AWS les ressources. Il est vivement déconseillé d'utiliser l'utilisateur racine pour vos tâches quotidiennes. Pour les tâches qui requièrent des informations d'identification de l'utilisateur racine, consultez [Tâches qui requièrent les informations d'identification de l'utilisateur racine](#) dans le Guide de l'utilisateur IAM.

Utilisateurs et groupes IAM

Un [utilisateur IAM](#) est une identité qui dispose d'autorisations spécifiques pour une seule personne ou application. Nous vous recommandons d'utiliser ces informations d'identification temporaires au lieu des utilisateurs IAM avec des informations d'identification à long terme. Pour plus d'informations,

voir [Exiger des utilisateurs humains qu'ils utilisent la fédération avec un fournisseur d'identité pour accéder à AWS l'aide d'informations d'identification temporaires](#) dans le guide de l'utilisateur IAM.

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

Rôles IAM

Un [rôle IAM](#) est une identité dotée d'autorisations spécifiques qui fournit des informations d'identification temporaires. Vous pouvez assumer un rôle en [passant d'un rôle d'utilisateur à un rôle IAM \(console\)](#) ou en appelant une opération d' AWS API AWS CLI ou d'API. Pour plus d'informations, consultez [Méthodes pour endosser un rôle](#) dans le Guide de l'utilisateur IAM.

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

Gestion de l'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 définit les autorisations lorsqu'elles sont associées à une identité ou à une ressource. AWS évalue ces politiques lorsqu'un directeur fait une demande. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations les documents de politique JSON, consultez [Vue d'ensemble des politiques JSON](#) dans le Guide de l'utilisateur IAM.

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

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Un administrateur IAM crée des politiques IAM et les ajoute aux rôles, que les utilisateurs peuvent ensuite assumer. Les politiques IAM définissent les autorisations quelle que soit la méthode que vous utilisez pour exécuter l'opération.

Politiques basées sur l'identité

Les stratégies basées sur l'identité sont des documents de stratégie d'autorisations JSON que vous attachez à une identité (utilisateur, groupe ou rôle). Ces politiques contrôlent les actions que peuvent

exécuter ces identités, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez [Définition d'autorisations IAM personnalisées avec des politiques gérées par le client](#) dans le Guide de l'utilisateur IAM.

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

Politiques basées sur les ressources

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

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

Autres types de politique

AWS prend en charge des types de politiques supplémentaires qui peuvent définir les autorisations maximales accordées par les types de politiques les plus courants :

- Limites d'autorisations : une limite des autorisations définit le nombre maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM. Pour plus d'informations, consultez [Limites d'autorisations pour des entités IAM](#) dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCPs) — Spécifiez les autorisations maximales pour une organisation ou une unité organisationnelle dans AWS Organizations. Pour plus d'informations, consultez [Politiques de contrôle de service](#) dans le Guide de l'utilisateur AWS Organizations .
- Politiques de contrôle des ressources (RCPs) : définissez le maximum d'autorisations disponibles pour les ressources de vos comptes. Pour plus d'informations, voir [Politiques de contrôle des ressources \(RCPs\)](#) dans le guide de AWS Organizations l'utilisateur.
- Politiques de session : politiques avancées que vous passez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Pour plus d'informations, consultez [Politiques de session](#) dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour 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 fonctionne la personnalisation de l'expérience AWS utilisateur avec IAM

AWS La personnalisation de l'expérience utilisateur (UXC) fonctionne avec les politiques IAM pour gérer l'accès aux opérations de l'API UXC.

Avant d'utiliser IAM pour gérer l'accès à la personnalisation de AWS l'expérience utilisateur (personnalisation de l'expérience utilisateur), découvrez quelles fonctionnalités IAM peuvent être utilisées dans le cadre de la personnalisation de l'expérience utilisateur. Nous vous recommandons d'intégrer la personnalisation de l'expérience utilisateur par le biais d'une politique AWS gérée. Pour plus d'informations, consultez [les politiques AWS gérées pour le AWS Management Console](#).

Avant d'utiliser IAM pour gérer l'accès à la personnalisation de l'expérience utilisateur, découvrez quelles fonctionnalités IAM peuvent être utilisées dans le cadre de la personnalisation de l'expérience utilisateur.

Fonctionnalité IAM	Assistance à la personnalisation de l'expérience utilisateur
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Non
Clés de condition d'une politique	Non
Informations d'identification temporaires	Oui
Autorisations principales interservices	Non
Rôles liés à un service	Non

Fonctionnalité IAM	Assistance à la personnalisation de l'expérience utilisateur
Rôles du service	Non

Pour obtenir une vue d'ensemble de la façon dont la personnalisation de l'expérience utilisateur et 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.

Politiques basées sur l'identité pour la personnalisation de l'expérience utilisateur

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 [Définition d'autorisations IAM personnalisées avec des politiques gérées par le client](#) dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez [Références des éléments de politique JSON IAM](#) dans le Guide de l'utilisateur IAM.

Pour consulter des exemples de politiques basées sur l'identité de personnalisation de l'expérience utilisateur, consultez la section [Exemples de politiques basées sur l'identité pour AWS](#) la personnalisation de l'expérience utilisateur.

Actions politiques pour la personnalisation de l'expérience utilisateur

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

Pour voir toutes les actions de personnalisation de l'expérience utilisateur, reportez-vous à la [référence des API](#).

Dans le cadre de la personnalisation de l'expérience utilisateur, les actions de stratégie utilisent le `uxc` : préfixe situé avant l'action (par exemple `uxc:GetAccountCustomizations`).

Pour spécifier plusieurs actions dans une seule déclaration, séparez-les par des virgules :

```
"Action": [  
    "uxc:GetAccountCustomizations",  
    "uxc:ListServices"  
]
```

Pour consulter des exemples de politiques basées sur l'identité de personnalisation de l'expérience utilisateur, consultez la section [Exemples de politiques basées sur l'identité pour AWS](#) la personnalisation de l'expérience utilisateur.

Ressources relatives aux politiques pour la personnalisation de l'expérience utilisateur

La personnalisation de l'expérience utilisateur ne prend pas en charge les ressources relatives aux politiques.

Utilisation d'informations d'identification temporaires avec personnalisation de l'expérience utilisateur

Les informations d'identification temporaires fournissent un accès à court terme aux AWS ressources et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. 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](#) et [Services AWS compatibles avec IAM](#) dans le Guide de l'utilisateur IAM.

Résolution des problèmes AWS d'expérience utilisateur Personnalisation de l'identité et de l'accès

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lors de l'utilisation de la personnalisation de l'expérience utilisateur et de l'IAM.

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource `my-example-widget` fictive, mais ne dispose pas des autorisations `uxc:GetWidget` fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
  uxc: GetWidget on resource: my-example-widget because no identity-based policy allows
  the GetWidget action
```

Dans ce cas, la politique qui s'applique à l'utilisateur mateojackson doit être mise à jour pour autoriser l'accès à la ressource *my-example-widget* à l'aide de l'action uxc : *GetWidget*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Une fois les clés d'accès utilisateur IAM créées, vous pouvez afficher votre ID de clé d'accès à tout moment. Toutefois, vous ne pouvez pas revoir votre clé d'accès secrète. Si vous perdez votre clé d'accès secrète, vous devez créer une nouvelle paire de clés.

Les clés d'accès se composent de deux parties : un ID de clé d'accès (par exemple, AKIAIOSFODNN7EXAMPLE) et une clé d'accès secrète (par exemple, wJa1rXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY). À l'instar d'un nom d'utilisateur et un mot de passe, vous devez utiliser à la fois l'ID de clé d'accès et la clé d'accès secrète pour authentifier vos demandes. Gérez vos clés d'accès de manière aussi sécurisée que votre nom d'utilisateur et votre mot de passe.

Important

Ne communiquez pas vos clés d'accès à un tiers, même pour qu'il vous aide à [trouver votre ID utilisateur canonique](#). Ce faisant, vous pourriez donner à quelqu'un un accès permanent à votre Compte AWS.

Lorsque vous créez une paire de clé d'accès, enregistrez l'ID de clé d'accès et la clé d'accès secrète dans un emplacement sécurisé. La clé d'accès secrète est accessible uniquement au moment de sa création. Si vous perdez votre clé d'accès secrète, vous devez ajouter de nouvelles clés d'accès pour votre utilisateur IAM. Vous pouvez avoir un maximum de deux clés d'accès. Si vous en avez déjà deux, vous devez supprimer une paire de clés avant d'en créer une nouvelle. Pour afficher les instructions, consultez [Gestion des clés d'accès](#) dans le Guide de l'utilisateur IAM.

Pour permettre à d'autres utilisateurs d'accéder à la personnalisation de l'expérience utilisateur, vous devez accorder l'autorisation aux personnes ou aux applications qui ont besoin d'y accéder. Si vous utilisez AWS IAM Identity Center pour gérer des personnes et des applications, vous attribuez des ensembles d'autorisations aux utilisateurs ou aux groupes afin de définir leur niveau d'accès. Les

ensembles d'autorisations créent et attribuent automatiquement des politiques IAM aux rôles IAM associés à la personne ou à l'application. Pour plus d'informations, consultez la section [Ensembles d'autorisations](#) dans le guide de AWS IAM Identity Center l'utilisateur.

Si vous n'utilisez pas IAM Identity Center, vous devez créer des entités IAM (utilisateurs ou rôles) pour les personnes ou les applications qui ont besoin d'un accès. Vous devez ensuite associer une politique à l'entité qui lui accorde les autorisations appropriées dans le cadre de la personnalisation de l'expérience utilisateur. Une fois les autorisations accordées, fournissez les informations d'identification à l'utilisateur ou au développeur de l'application. Ils utiliseront ces informations d'identification pour y accéder AWS. Pour en savoir plus sur la création d'utilisateurs, de groupes, de politiques et d'autorisations [IAM, consultez la section Identités, politiques et autorisations IAM dans le guide de l'utilisateur IAM.](#)

Exemples de politiques basées sur l'identité pour la personnalisation de AWS l'expérience utilisateur

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à obtenir ou à modifier les ressources UXC. Pour autoriser les utilisateurs à effectuer des actions sur les ressources, un administrateur IAM peut créer des politiques IAM. Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez [Création de politiques IAM \(console\)](#) dans le Guide de l'utilisateur IAM.

Rubriques

- [Bonnes pratiques en matière de politiques](#)
- [Accès en lecture seule aux personnalisations des comptes UXC](#)
- [Accès complet aux personnalisations des comptes UXC](#)

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources de personnalisation de l'expérience utilisateur 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.

- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation d'IAM pour appliquer des autorisations, consultez [politiques et autorisations dans IAM](#) dans le Guide de l'utilisateur IAM.
- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que CloudFormation. Pour plus d'informations, consultez [Conditions pour éléments de politique JSON IAM](#) dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez [Validation de politiques avec IAM Access Analyzer](#) dans le Guide de l'utilisateur IAM.
- 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 la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez [Sécurisation de l'accès aux API avec MFA](#) dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez [Bonnes pratiques de sécurité dans IAM](#) dans le Guide de l'utilisateur IAM.

Accès en lecture seule aux personnalisations des comptes UXC

L'exemple suivant montre comment créer une politique qui autorise l'accès en lecture seule aux personnalisations de comptes UXC :

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

Accès complet aux personnalisations des comptes UXC

L'exemple suivant montre comment créer une politique qui autorise un accès complet aux personnalisations de comptes UXC :

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

AWS politiques gérées pour AWS Management Console

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 [Politiques gérées par AWS](#) dans le Guide de l'utilisateur IAM.

AWS politique gérée : AWSManagement ConsoleBasicUserAccess

Vous pouvez associer `AWSManagementConsoleBasicUserAccess` à vos utilisateurs, groupes et rôles.

Cette politique accorde les autorisations nécessaires aux utilisateurs non administrateurs du AWS Management Console. Cela inclut des fonctionnalités telles que la découverte des ressources, les notifications, l'accès au shell via un navigateur et une navigation personnalisée.

Détails de l'autorisation

Ces autorisations `AWSManagementConsoleBasicUserAccess` sont regroupées dans les ensembles d'autorisations suivants :

- `cloudshell`— Permet aux principaux un accès complet aux AWS CloudShell fonctionnalités, notamment à la création d'environnements, à la gestion des sessions et à l'exécution des commandes.
- `ec2`— Permet aux principaux de décrire les régions activées pour le compte dans [Unified Navigation](#).
- `notifications`— Permet aux directeurs d'obtenir des événements à partir de Notifications des utilisateurs AWS.
- `q`— Permet aux directeurs de discuter avec Amazon Q Developer.
- `resource-explorer-2`— Permet aux directeurs de rechercher et de découvrir des AWS ressources à l'aide de la [recherche unifiée](#).
- `uxc`— Permet aux administrateurs de lire les paramètres de personnalisation de l'expérience AWS utilisateur.
- `action-recommendations`— Permet aux directeurs de recevoir des recommandations d'actions contextuelles.
- `account`— Permet aux principaux de récupérer des informations sur le compte spécifié, notamment son nom de compte, son identifiant de compte, ainsi que la date et l'heure de création du compte.

Pour voir les autorisations de cette stratégie, consultez [AWSManagementConsoleBasicUserAccess](#) dans le AWS Guide de référence des stratégies gérées par.

AWS politique gérée : `AWSManagementConsoleAdministratorAccess`

Vous pouvez associer `AWSManagementConsoleAdministratorAccess` à vos utilisateurs, groupes et rôles.

Cette politique accorde un accès complet pour configurer et personnaliser le AWS Management Console. Il permet aux administrateurs de définir les couleurs des comptes, d'activer les notifications aux utilisateurs et de configurer la découverte des ressources. Il inclut également les autorisations issues de la politique `AWSManagementConsoleBasicUserAccess` gérée, qui sont essentielles pour les utilisateurs non administrateurs du AWS Management Console.

Détails de l'autorisation

Ces autorisations `AWSManagementConsoleAdministratorAccess` sont regroupées dans les ensembles d'autorisations suivants :

- `cloudshell`— Permet aux principaux un accès complet aux AWS CloudShell fonctionnalités, notamment à la création d'environnements, à la gestion des sessions et à l'exécution des commandes.
- `ec2`— Permet aux principaux de décrire les régions activées pour le compte dans [Unified Navigation](#).
- `notifications`— Permet aux principaux d'accéder aux configurations de notification, aux événements et au statut d'adhésion aux fonctionnalités et de les mettre à jour.
- `q`— Permet aux directeurs de discuter avec Amazon Q Developer pour bénéficier d'une assistance assistée par l'IA.
- `resource-explorer-2`— Permet aux directeurs de rechercher et de découvrir des AWS ressources à l'aide de la [recherche unifiée](#).
- `uxc`— Permet aux principaux un accès complet aux paramètres de personnalisation de AWS l'expérience utilisateur.
- `action-recommendations`— Permet aux directeurs de recevoir des recommandations d'actions contextuelles.
- `account`— Permet aux principaux de récupérer des informations sur le compte spécifié, notamment son nom de compte, son identifiant de compte, ainsi que la date et l'heure de création du compte.

Pour voir les autorisations de cette stratégie, consultez [AWSManagementConsoleAdministratorAccess](#) dans le AWS Guide de référence des stratégies gérées par.

AWS Management Console mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées AWS Management Console 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 Management Console document.

Modifier	Description	Date
AWSManagementConso leBasicUserAccess — Politique mise à jour	Ajouté <code>uxc:GetAccountCustomizations</code> et <code>uxc:ListServices</code> autorisations.	26 mars 2026
AWSManagementConso leAdministratorAccess — Politique mise à jour	Ajouté <code>uxc:GetAccountCustomizations</code> , <code>uxc:UpdateAccountCustomizations</code> , et <code>uxc:ListServices</code> autorisations.	26 mars 2026
AWSManagementConso leBasicUserAccess — Politique mise à jour	Politique mise à jour pour ajouter des autorisations permettant aux utilisateurs de consulter les informations du compte et de recevoir des recommandations d'action lorsqu'ils naviguent sur le AWS Management Console.	9 décembre 2025
AWSManagementConso leAdministratorAccess — Politique mise à jour	Politique mise à jour pour ajouter des autorisations permettant aux utilisateurs de consulter les informations du compte et de recevoir des	9 décembre 2025

Modifier	Description	Date
	recommandations d'action lorsqu'ils naviguent sur le AWS Management Console.	
AWSManagementConso leBasicUserAccess : nouvelle politique	Ajout d'une nouvelle politique AWS gérée qui accorde les autorisations nécessaires à la AWS Management Console navigation de base, à l'affichage des couleurs des comptes et à la découverte des ressources.	14 août 2025
AWSManagementConso leAdministratorAccess : nouvelle politique	Ajout d'une nouvelle politique AWS gérée qui fournit un accès complet pour configurer et personnaliser le AWS Management Console.	14 août 2025
AWS Management Console a commencé à suivre les modifications	AWS Management Console a commencé à suivre les modifications apportées AWS à ses politiques gérées.	14 août 2025

Utilisation de Markdown dans la console

Certains services du AWS Management Console, tels qu'Amazon CloudWatch, prennent en charge l'utilisation de [Markdown](#) dans certains domaines. Cette rubrique décrit les types de mise en forme Markdown pris en charge dans la console.

Table des matières

- [Paragraphe, espacement de ligne et lignes horizontales](#)
- [En-têtes](#)
- [Mise en forme d'un texte](#)
- [Liens](#)
- [Lists](#)
- [Tableaux et boutons \(CloudWatch tableaux de bord\)](#)

Paragraphe, espacement de ligne et lignes horizontales

Les paragraphes sont séparés par une ligne vide. Pour vous assurer que la ligne vide entre les paragraphes s'affiche lorsqu'elle est convertie en HTML, ajoutez une nouvelle ligne avec un espace non interrompu (), puis une ligne vide. Répétez cette paire de lignes pour insérer plusieurs lignes vides l'une après l'autre, comme dans l'exemple suivant :

```
&nbsp;
&nbsp;
```

Pour créer une règle horizontale séparant les paragraphes, ajoutez une ligne avec trois tirets d'affilée : ---

```
Previous paragraph.
---
Next paragraph.
```

Pour créer un bloc de texte avec une police à chasse fixe, ajoutez une ligne comportant trois guillemets obliques (``). Saisissez le texte à afficher dans le type de police à chasse fixe. Ensuite,

ajoutez une nouvelle ligne avec trois guillemets obliques. L'exemple suivant illustre le texte qui sera formaté en type de police à chasse fixe lorsqu'il est affiché :

```
...  
This appears in a text box with a background shading.  
The text is in monospace.  
...
```

En-têtes

Pour créer des en-têtes, utilisez le signe dièse (#). Un seul signe dièse et un espace indiquent un en-tête de niveau supérieur. Deux signes dièse créent un titre de deuxième niveau, et trois signes dièse créent un titre de troisième niveau. Les exemples suivants présentent un en-tête de premier niveau, de deuxième et de troisième niveaux :

```
# Top-level heading
```

```
## Second-level heading
```

```
### Third-level heading
```

Mise en forme d'un texte

Pour mettre en forme un texte en italique, encadrez-le avec un seul trait de soulignement (_) ou astérisque (*) de chaque côté.

```
*This text appears in italics.*
```

Pour mettre en forme un texte en gras, encadrez-le avec deux traits de soulignement ou deux astérisques de chaque côté.

```
**This text appears in bold.**
```

Pour mettre en forme un texte en barré, encadrez-le avec deux tildes (~) de chaque côté.

```
~~This text appears in strikethrough.~~
```

Liens

Pour ajouter un lien hypertexte, entrez le texte du lien entouré de crochets ([]), suivi de l'URL complète entre parenthèses (()), comme dans l'exemple suivant :

```
Choose [link_text](http://my.example.com).
```

Lists

Pour mettre en forme des lignes au sein d'une liste à puces, ajoutez-les sur des lignes distinctes commençant par un seul astérisque (*), puis un espace, comme dans l'exemple suivant :

```
Here is a bulleted list:  
* Ant  
* Bug  
* Caterpillar
```

Pour mettre en forme des lignes au sein d'une liste numérotée, ajoutez-les sur des lignes distinctes commençant par un numéro, un point (.) et un espace, comme dans l'exemple suivant :

```
Here is a numbered list:  
1. Do the first step  
2. Do the next step  
3. Do the final step
```

Tableaux et boutons (CloudWatch tableaux de bord)

CloudWatch les widgets de texte des tableaux de bord prennent en charge les tableaux et les boutons Markdown.

Pour créer un tableau, séparez les colonnes en utilisant des barres verticales (|) et les lignes à l'aide de nouvelles lignes. Pour faire de la première ligne une ligne d'en-tête, insérez une ligne entre la ligne d'en-tête et la première ligne de valeurs. Ajoutez ensuite au moins trois traits d'union (-) pour chaque colonne de la table. Séparez les colonnes avec des barres verticales. L'exemple suivant illustre Markdown pour une table comportant deux colonnes, une ligne d'en-tête et deux lignes de données :

```
Table | Header
```

```
----|-----  
Amazon Web Services | AWS  
1 | 2
```

Le texte Markdown de l'exemple précédent crée le tableau suivant :

Tableau	En-tête
Amazon Web Services	AWS
1	2

Dans un widget CloudWatch de texte de tableau de bord, vous pouvez également mettre en forme un lien hypertexte pour qu'il apparaisse sous forme de bouton. Pour créer un bouton, utilisez `[button:Button text]`, suivi de l'URL complète entre parenthèses (()), comme dans l'exemple suivant :

```
[button:Go to AWS](http://my.example.com)  
[button:primary:This button stands out even more](http://my.example.com)
```

Résolution des problèmes

Consultez cette section pour trouver des solutions aux problèmes courants liés au AWS Management Console.

Vous pouvez également diagnostiquer et résoudre les erreurs courantes de certains AWS services à l'aide d'Amazon Q Developer. Pour plus d'informations, consultez la section [Diagnostiquer les erreurs courantes dans la console avec Amazon Q Developer](#) dans le manuel Amazon Q Developer User Guide.

Rubriques

- [La page ne se charge pas correctement.](#)
- [Mon navigateur affiche un message d'erreur « accès refusé » lors de la connexion au AWS Management Console](#)
- [Mon navigateur affiche des erreurs de temporisation lors de la connexion au AWS Management Console](#)
- [Je souhaite changer la langue du AWS Management Console mais je ne trouve pas le menu de sélection de langue en bas de page](#)

La page ne se charge pas correctement.

- Si ce problème ne se produit qu'occasionnellement, vérifiez votre connexion Internet. Essayez de vous connecter via un autre réseau, avec ou sans VPN, ou essayez d'utiliser un autre navigateur Web.
- Si tous les utilisateurs concernés appartiennent à la même équipe, il peut s'agir d'un problème lié à l'extension de confidentialité du navigateur ou au pare-feu de sécurité. Les extensions de navigateur de confidentialité et les pare-feux de sécurité peuvent bloquer l'accès aux domaines utilisés par le AWS Management Console. Essayez de désactiver ces extensions ou de régler les paramètres du pare-feu. Pour vérifier les problèmes liés à votre connexion, ouvrez les outils de développement de votre navigateur ([Chrome](#), [Firefox](#)) et inspectez les erreurs dans l'onglet Console. Les AWS Management Console suffixes des domaines d'utilisation, y compris la liste suivante. Cette liste n'est pas exhaustive et peut évoluer avec le temps. Les suffixes de ces domaines ne sont pas utilisés exclusivement par AWS.
 - .a2z.com
 - amazon.com

- .amazonaws.com
- .aws
- .aws.com
- .aws.dev
- .awscloud.com
- .awsplayer.com
- .awsstatic.com
- .cloudfront.net
- .live-video.net

Warning

Depuis le 31 juillet 2022, Internet Explorer 11 AWS n'est plus compatible. Nous vous recommandons de l'utiliser AWS Management Console avec d'autres navigateurs compatibles. Pour en savoir plus, consultez le [blog d'actualités AWS](#).

Mon navigateur affiche un message d'erreur « accès refusé » lors de la connexion au AWS Management Console

Les modifications récentes apportées à la console peuvent affecter votre accès si toutes les conditions suivantes sont remplies :

- Vous accédez à AWS Management Console partir d'un réseau configuré pour atteindre les points de terminaison de AWS service via les points de terminaison VPC.
- Vous limitez l'accès aux AWS services en utilisant `aws:SourceIp` ou en utilisant une clé de condition `aws:SourceVpc` globale dans vos politiques IAM.

Nous vous recommandons de consulter les politiques IAM qui contiennent la clé de condition `aws:SourceVpc` globale `aws:SourceIp` ou. Appliquez les deux `aws:SourceIp`, `aws:SourceVpc` le cas échéant.

Certaines AWS Management Console fonctionnalités utilisent des domaines à double pile qui prennent en charge à la fois les IPv6 connexions IPv4 et les connexions. Si votre politique IAM

restreint l'accès uniquement à `aws : SourceIp` des blocs IPv4 CIDR, les demandes peuvent échouer lorsque votre système d'exploitation préfère les IPv6 connexions (ou vice versa). Pour éviter cela, incluez les deux blocs IPv4 et les blocs IPv6 CIDR dans votre `aws : SourceIp` état. Pour plus d'informations, consultez [aws : SourceIp](#) dans le guide de Gestion des identités et des accès AWS l'utilisateur.

Vous pouvez également intégrer la fonctionnalité d'accès AWS Management Console privé pour y accéder AWS Management Console via un point de terminaison VPC et utiliser `aws : SourceVpc` les conditions dans vos politiques. Pour plus d'informations, consultez les ressources suivantes :

- [AWS Management Console Accès privé](#)
- [the section called “Comment fonctionne AWS Management Console Private Access avec AWS : SourceVpc”](#)
- [the section called “Clés contextuelles de condition AWS globale prises en charge”](#)

Mon navigateur affiche des erreurs de temporisation lors de la connexion au AWS Management Console

En cas de panne de service par défaut Région AWS, votre navigateur peut afficher une erreur 504 Gateway Timeout lorsque vous essayez de vous connecter au AWS Management Console. Pour vous connecter au AWS Management Console depuis une autre région, spécifiez un point de terminaison régional alternatif dans l'URL. Par exemple, s'il y a une panne dans la région `us-west-1` (Caroline du Nord), utilisez le modèle suivant pour accéder à la région `us-west-2` (Oregon) :

```
https://region.console.aws.amazon.com
```

Pour plus d'informations, consultez [Points de terminaison de service AWS Management Console](#) dans le Références générales AWS.

Pour consulter le statut de tous Services AWS, y compris le AWS Management Console, voir [Tableau de bord AWS Health](#).

Je souhaite changer la langue du AWS Management Console mais je ne trouve pas le menu de sélection de langue en bas de page

Le menu de sélection de la langue a été déplacé vers la nouvelle page Paramètres unifiés. Pour modifier la langue de AWS Management Console, [accédez à la page des paramètres unifiés](#), puis choisissez la langue de la console.

Pour de plus amples informations, veuillez consulter la section [Modification de la langue de la AWS Management Console](#).

Historique du document

Le tableau suivant décrit les modifications importantes apportées au Manuel de mise en route de AWS Management Console depuis mars 2021.

Modifier	Description	Date
Politiques AWS gérées mises à jour	Mise à jour des AWSManagementConsoleBasicUserAccess politiques AWSManagementConsoleAdministratorAccess et avec les nouvelles autorisations UXC. Pour de plus amples informations, veuillez consulter ??? .	26 mars 2026
Page ajoutée	Nouvelle page ajoutée pour expliquer les actions recommandées. Pour de plus amples informations, veuillez consulter ??? .	15 octobre 2025
Nouvelles politiques AWS gérées	Ajout de deux nouvelles politiques pour définir les autorisations d'utilisation, de configuration et de personnalisation du AWS Management Console. <ul style="list-style-type: none">• AWSManagementConsoleBasicUserAccess• AWSManagementConsoleAdministratorAccess	14 août 2025
Personnalisations de l'expérience utilisateur (UXC)	Nouveau service disponible.	14 août 2025

Modifier	Description	Date
Page mise à jour	Vous pouvez désormais consulter vos candidatures dans MyApplications depuis le menu Services. Pour de plus amples informations, veuillez consulter ??? .	29 juillet 2025
Page ajoutée	Nouvelle page ajoutée pour expliquer la fonctionnalité multissession. Pour de plus amples informations, veuillez consulter ??? .	6 décembre 2024
Page mise à jour	Page de modification de votre mot de passe mise à jour. Pour de plus amples informations, veuillez consulter ??? .	18 juin 2024
Nouvelles pages ajoutées	De nouvelles pages ont été ajoutées pour décrire comment accéder au menu Services et aux notifications AWS d'événements. Pour plus d'informations, consultez ??? et ??? .	18 juin 2024
Page mise à jour	Qu'est-ce que le AWS Management Console ? page mise à jour. Pour de plus amples informations, veuillez consulter ??? .	18 juin 2024

Modifier	Description	Date
Accès au support	Une nouvelle page a été ajoutée pour décrire comment obtenir de l'aide. Pour de plus amples informations, veuillez consulter ??? .	18 juin 2024
Navigation unifiée et AWS Console Home	De nouvelles pages ont été ajoutées pour décrire le fonctionnement de la console. Pour plus d'informations, consultez ??? et ??? .	18 juin 2024
Discutez avec Amazon Q	Une nouvelle page de paramètres détaillant comment les utilisateurs peuvent poser AWS des questions à Amazon Q Developer. Pour plus d'informations, consultez Discuter avec Amazon Q Developer .	29 mai 2024
Mes candidatures	Une nouvelle page qui présente MyApplications. Pour plus d'informations, voir Sur quoi fonctionne MyApplications ? AWS .	29 novembre 2023

Modifier	Description	Date
Configuration des paramètres unifiés	Une nouvelle page de paramètres permettant de configurer les paramètres et les valeurs par défaut qui s'appliquent à l'utilisateur actuel, y compris la langue et la région. Pour plus d'informations, consultez Configuration des paramètres unifiés .	6 avril 2022
Nouvelle AWS Console Home interface utilisateur	Nouvelle AWS Console Home interface utilisateur, qui inclut des widgets pour afficher des informations d'utilisation importantes et des raccourcis vers les AWS services. Pour plus d'informations, consultez Utilisation des widgets .	25 février 2022
Modification de la langue de la console	Choisissez une autre langue pour la AWS Management Console. Pour de plus amples informations, veuillez consulter la section Modification de la langue de la AWS Management Console .	1 avril 2021
Lancement CloudShell	Ouvrez AWS CloudShell depuis AWS Management Console et exécutez les commandes AWS CLI. Pour plus d'informations, consultez la section Lancement AWS CloudShell .	22 mars 2021

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.