Guide de mise en route

AWS Management Console

Version 1.0

AWS Management Console: Guide de mise en route

Table of Contents

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

AWS Management ConsoleIl 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

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 ConsoleIl 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 le 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 pouvez utiliser le menu des 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 Favoris pour afficher votre liste de favoris.
4. (Facultatif) Choisissez Tous les services pour afficher la liste alphabétique de tous les AWS services.
5. (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 le 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 incluent :

- Services
- Fonctionnalités
- Documents
- Blogs
- Articles de connaissances
- Événements
- Didacticiels
- 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 `/Resources` au début de votre requête dans la barre de recherche et choisissez /Resources dans le menu déroulant. Entrez ensuite le reste de votre requête.

Rubriques

Recherche de AWS produits dans le 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 EC2 console Amazon, entrez ec2 et appuyez sur 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 le 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 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 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 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 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 applicables aux 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.

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 Consoleou pour certains services, tels que AWS Identity and Access Management. 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 (telles que les EC2 instances Amazon) 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 depuis 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

La barre rapide des favoris apparaît lorsqu'au moins un AWS service ou une application est ajouté 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. Vous pouvez ainsi 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 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.

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 applications dans le widget Favoris.

Pour plus d'informations sur les widgets, consultezthe 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 Consoleen 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

- Rooter les utilisateurs dans AWS Management Console

- Les utilisateurs d'IAM dans AWS Management Console
- Les utilisateurs de l'IAM Identity Center dans AWS Management Console
- Les identités fédérées dans le AWS Management Console

Rooter 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'AWS Identity and Access Management 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 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

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 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.

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.

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.

> **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

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.

> **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 multisession, l'URL de la console contient un sous-domaine (par exemple,`https://000000000000-aaaaaaaa.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 multisession en choisissant Activer la multisession dans le menu du compte ou en choisissant Activer la AWS Management Console multisession 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.

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

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. 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 Envoyer.

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

Dans quoi se trouve 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

- 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.
- 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,

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
- 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)
- Moyen-Orient (Bahreïn)
- 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

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 AWS CloudFormation associez une pile, cochez la case en bas de page.

> **Note**
>
> L'ajout d'une AWS 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 AWS 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 afficher vos applications dans toutes les régions ou dans des régions spécifiques, ainsi que leurs informations pertinentes sous forme de carte ou de tableau.

Pour afficher des applications

1. Dans la barre latérale gauche, choisissez myApplications.
2. Dans Régions, sélectionnez Région actuelle ou Régions prises en charge.

3. Pour trouver une application spécifique, entrez son nom, ses mots-clés ou sa description dans la barre de recherche.
4. (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.

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 EC2 instance Amazon, 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

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 associée à cette paire clé-valeur de balise existe déjà pour cette application. Une application peut prendre en charge plusieurs synchronisations de balises, mais chaque synchronisation de balises doit avoir une paire clé-valeur de balise différente. Après avoir spécifié une autre paire clé-valeur de balise, réessayez la tâche de synchronisation de 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. Sélectionnez Remove (Supprimer).
8. Confirmez que vous souhaitez supprimer la ressource en choisissant Supprimer des ressources.

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 de l' Amazon CloudWatch utilisation du processeur des EC2 instances Amazon et des invocations Lambda.

Configuration du widget de calcul

Pour renseigner les données dans le widget Compute, configurez au moins une EC2 instance Amazon 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.

Configuration du widget AWS de sécurité

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

AWS Security Hub 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 en OpsItems fonction des règles et des 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 automatique de correctifs pour les EC2 instances Amazon de votre application en configurant AWS Systems Manager Patch Manager. 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 CloudWatch les tarifs Amazon et le blog sur les opérations et migrations AWS dans le cloud, respectivement.

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

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 sélection de 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)
- Moyen-Orient (Bahreïn)

- 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

- AWS Compute Optimizer
- 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
- Vue EC2 globale d'Amazon
- EC2 Image Builder
- Amazon EC2 Instance Connect
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- AWS Elastic Disaster Recovery
- 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
- AWS Identity and Access Management
- 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 Private Certificate Authority
- Tableau de bord de santé publique

- Amazon Rekognition
- Amazon Relational Database Service
- AWS Resource Access Manager
- AWS Resource Groups 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
- 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 de compte sur 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, voirRésolution 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, et`docs.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

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 accèderont 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 :

- Connectez-vous

  - *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*
  - 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)
  - *.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 votreDNS, 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
- *.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 AWSAWS 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 autorise l'utilisation d'Amazon EC2 et CloudWatch des 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 EC2 console Amazon, ces politiques relatives aux points de terminaison VPC ne seront pas évaluées par rapport aux actions entreprises par EC2 Amazon 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.

```
{
```

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

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.

```
{
  "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 pourcom.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 d'`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

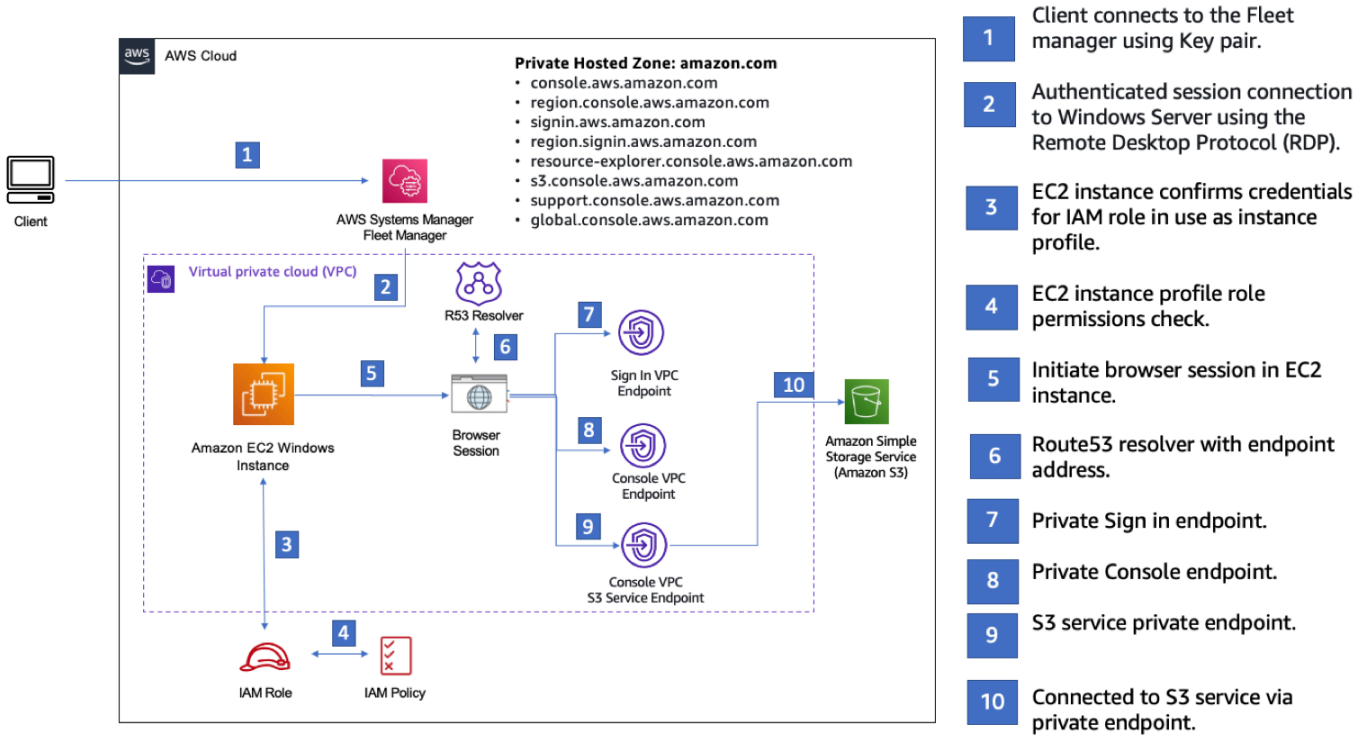
- Configuration des tests avec Amazon EC2
- Configuration des tests avec Amazon WorkSpaces
- Configuration test du VPC avec des politiques IAM

Configuration des tests avec Amazon EC2

Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud Amazon Web Services. Vous pouvez utiliser Amazon EC2 pour lancer autant ou aussi peu de serveurs virtuels que nécessaire, configurer la sécurité et le réseau, et gérer le stockage. Dans cette configuration, nous utilisons Fleet Manager, une fonctionnalité de AWS Systems Manager, pour nous connecter à une instance Amazon EC2 Windows 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 EC2 instance Amazon. Ce didacticiel AWS CloudFormation permet 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'utiliser Amazon EC2 pour accéder à une configuration d'accès AWS Management Console privé. Il montre comment un utilisateur est connecté à Amazon S3 à l'aide d'un point de terminaison privé.



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

AWS Management Console EC2 AWS CloudFormation Modèle Amazon 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 AWS CloudFormation.
2. Sélectionnez Créer la pile.
3. Choisissez Avec de nouvelles ressources (standard). Téléchargez le fichier AWS 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 EC2 clés Amazon existantes dans votre compte. Si vous ne possédez pas de paire de EC2 clés Amazon existante, vous devez en créer une avant de passer à l'étape suivante. Pour plus d'informations, consultez la section Créer une paire de clés à l'aide d'Amazon EC2 dans le guide de EC2 l'utilisateur Amazon.

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' EC2 instance Amazon

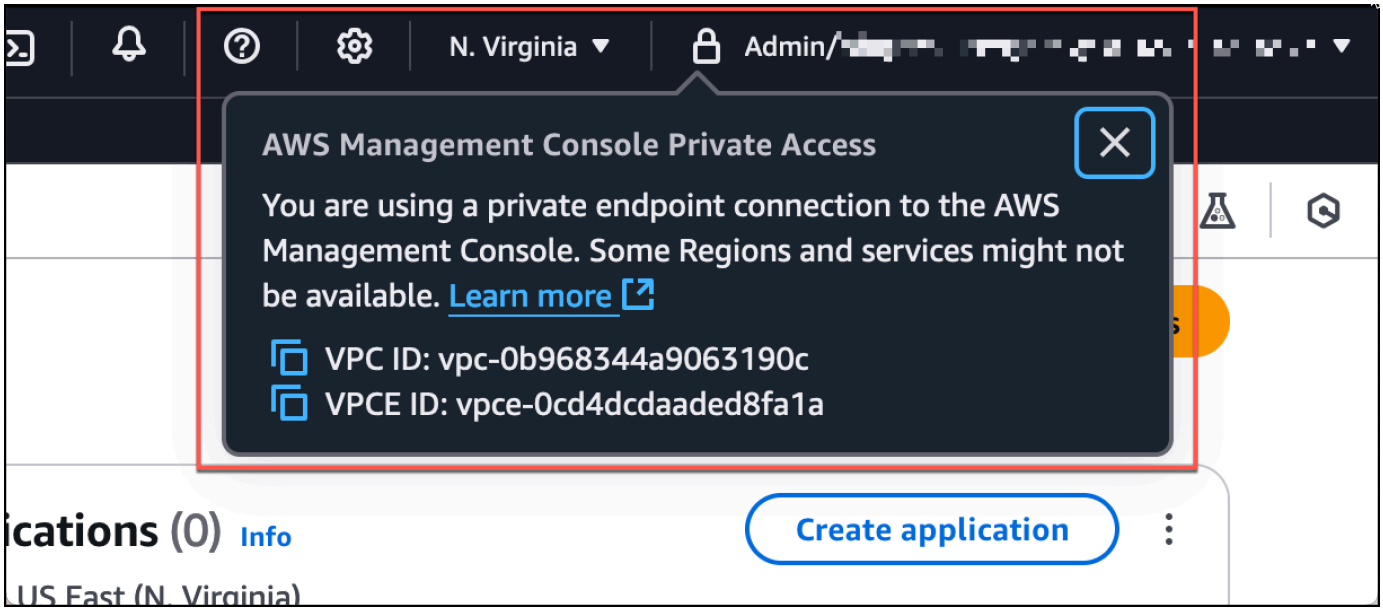
1. Connectez-vous au compte de gestion de votre organisation et ouvrez la EC2 console Amazon.
2. Dans le panneau de navigation, choisissez Instances.
3. Sur la page Instances, sélectionnez l'instance de test Console VPCE créée par le AWS CloudFormation modèle. Choisissez ensuite Connect (Connecter).

> **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' EC2 instance Amazon et accéder au bureau Windows via l'interface Web, utilisez la clé privée associée à la paire de EC2 clés Amazon que vous avez utilisée lors de la création du AWS CloudFormation modèle.
7. À partir de l'instance Amazon EC2 Windows, AWS Management Console ouvrez-la dans le navigateur.
8. 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

1. Connectez-vous au compte de gestion de votre organisation et ouvrez la console Amazon S3.
2. 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.



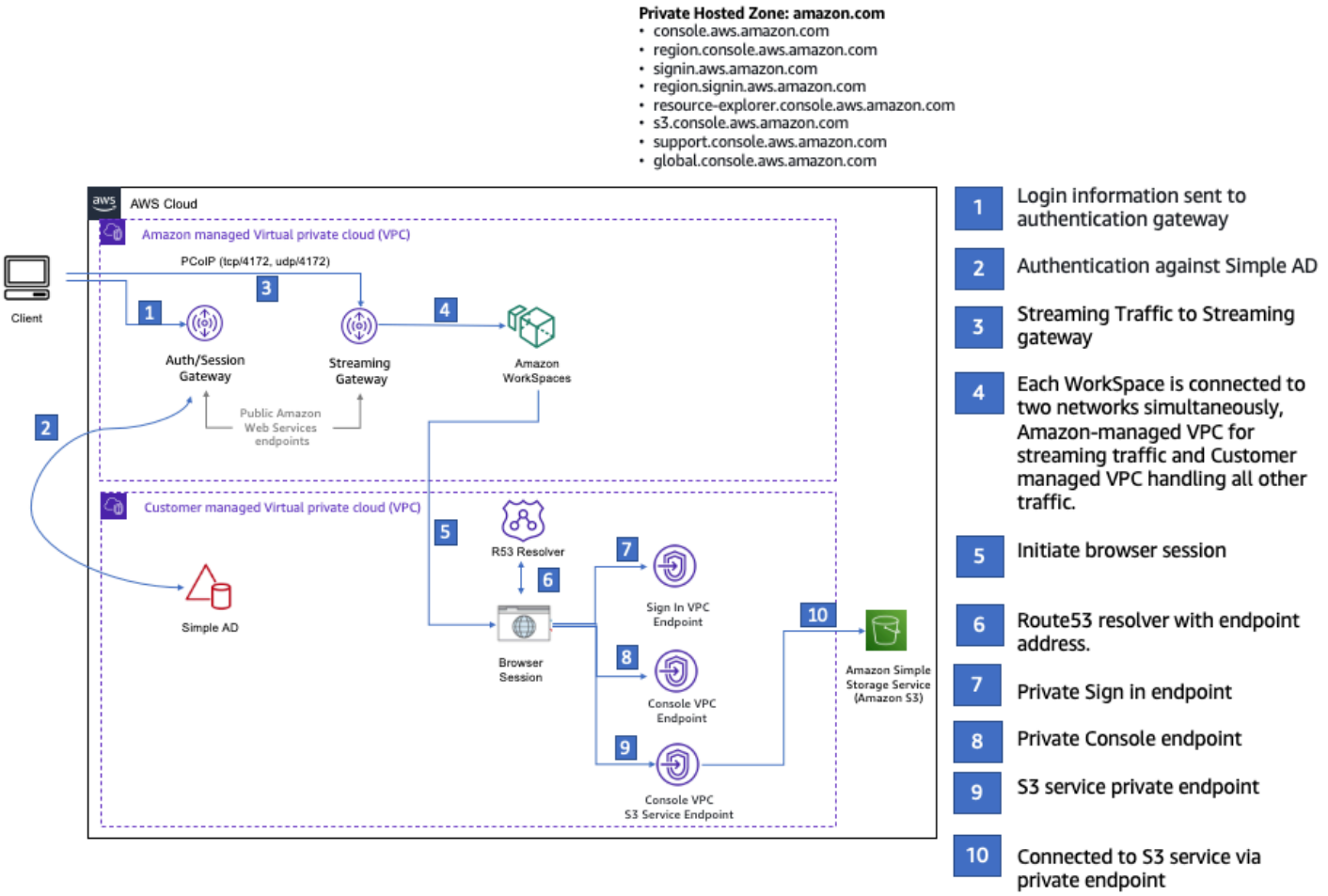
Configuration des tests avec Amazon WorkSpaces

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.



Copiez le AWS 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 ConsoleAWS 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
```

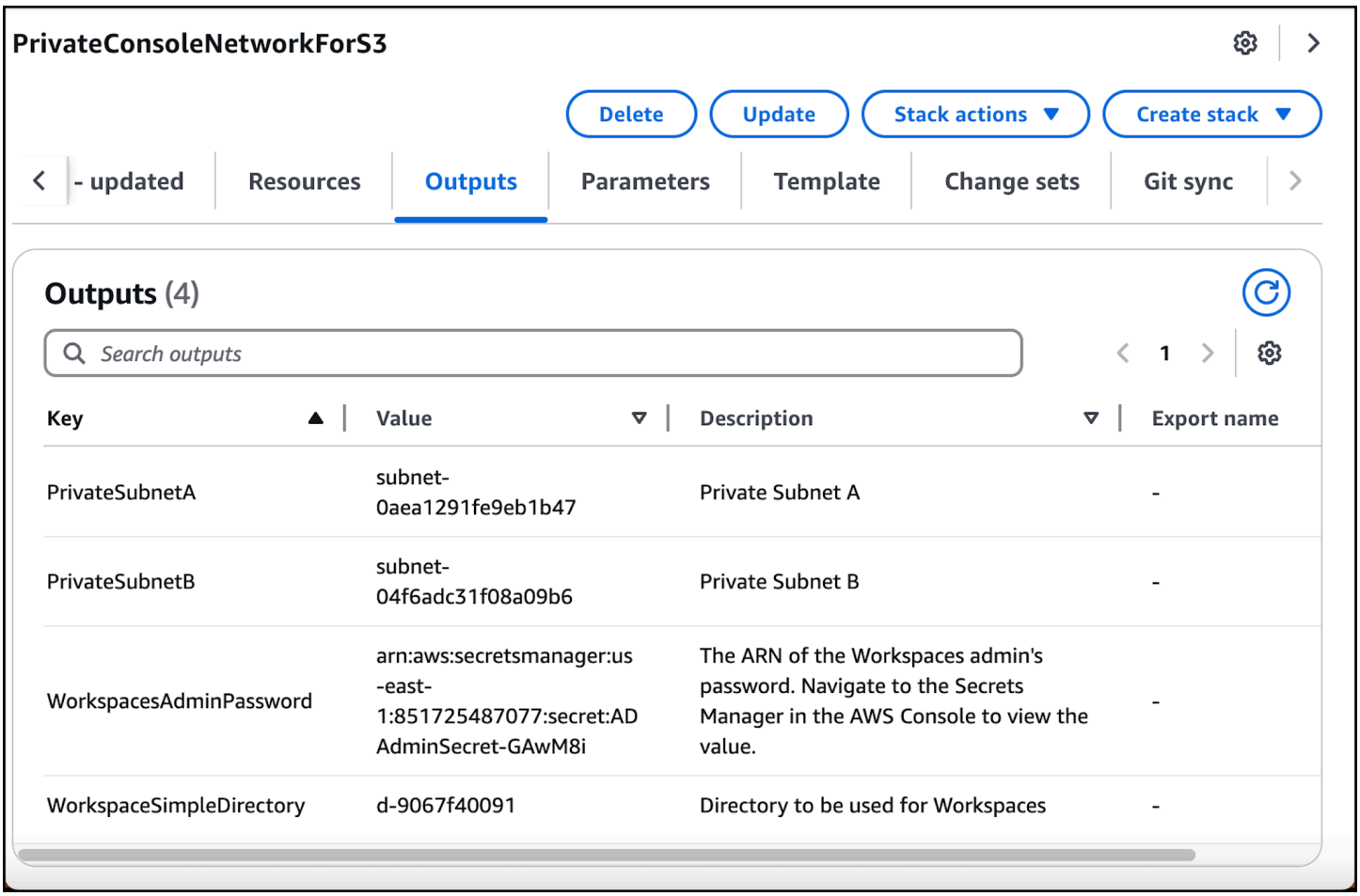
> **Note**
>
> Cette configuration test est conçue pour être exécutée dans la région USA Est (Virginie du Nord) (us-east-1).

Pour configurer un réseau

1. Connectez-vous au compte de gestion de votre organisation et ouvrez la console AWS CloudFormation.
2. Sélectionnez Créer la pile.
3. Choisissez Avec de nouvelles ressources (standard). Téléchargez le fichier AWS 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.

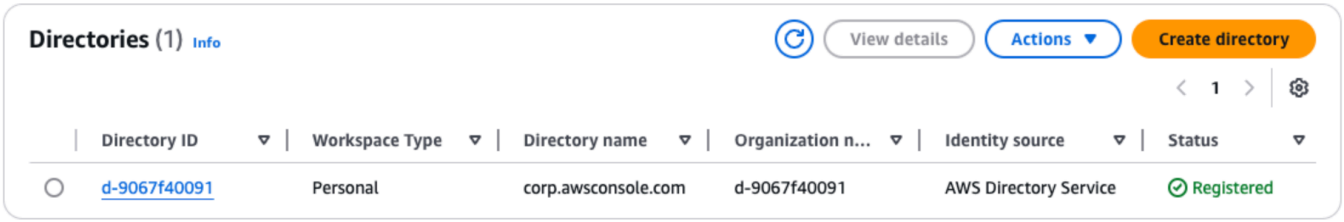
La capture d'écran suivante montre l'onglet Sorties qui affiche les valeurs des sous-réseaux privés et de l'annuaire Workspace Simple Directory.



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 (Annuaires).
3. Sur la page Annuaires, vérifiez que le statut de l'annuaire est Actif. La capture d'écran suivante montre une page Annuaires 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 AWS 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 adresse 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

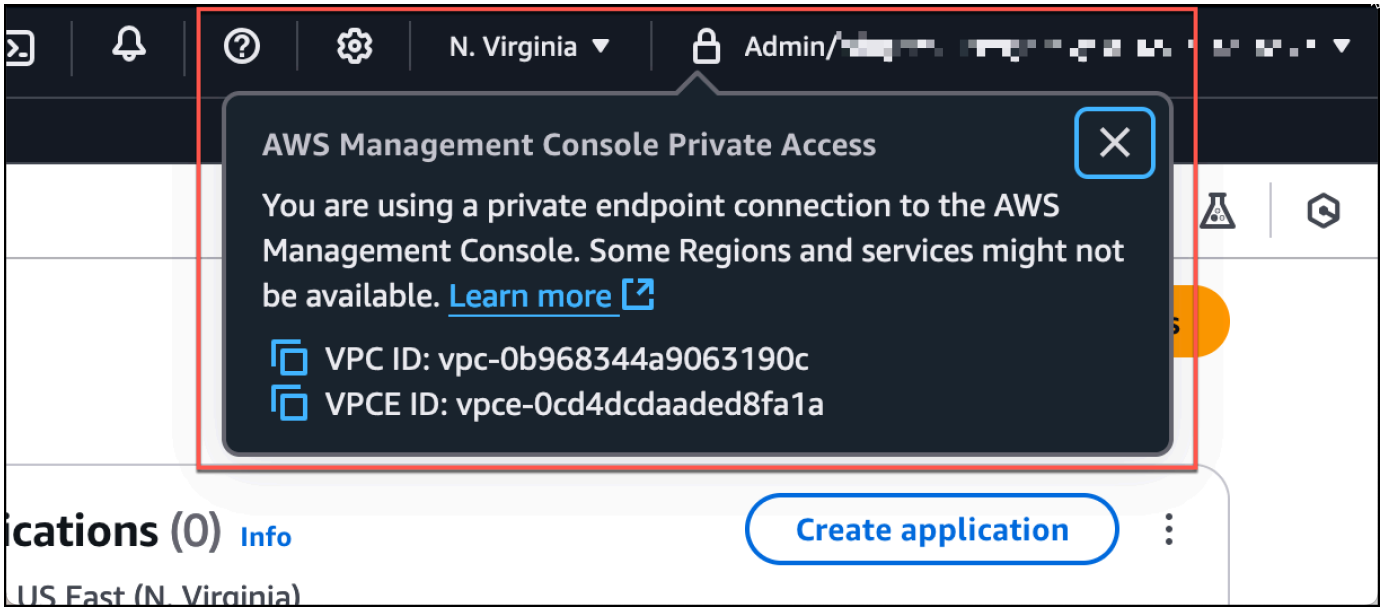
1. Ouvrez l'e-mail que vous avez reçu à l'étape 14 de la procédure précédente.
2. Dans l'e-mail, choisissez le lien unique fourni pour configurer votre profil et télécharger le WorkSpaces client.
3. Définissez votre mot de passe.
4. Téléchargez le client de votre choix.
5. Installez et lancez le client. 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 via AWS Management Console Private Access.
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 le VPC que vous avez configuré avec Amazon EC2 ou en WorkSpaces 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.

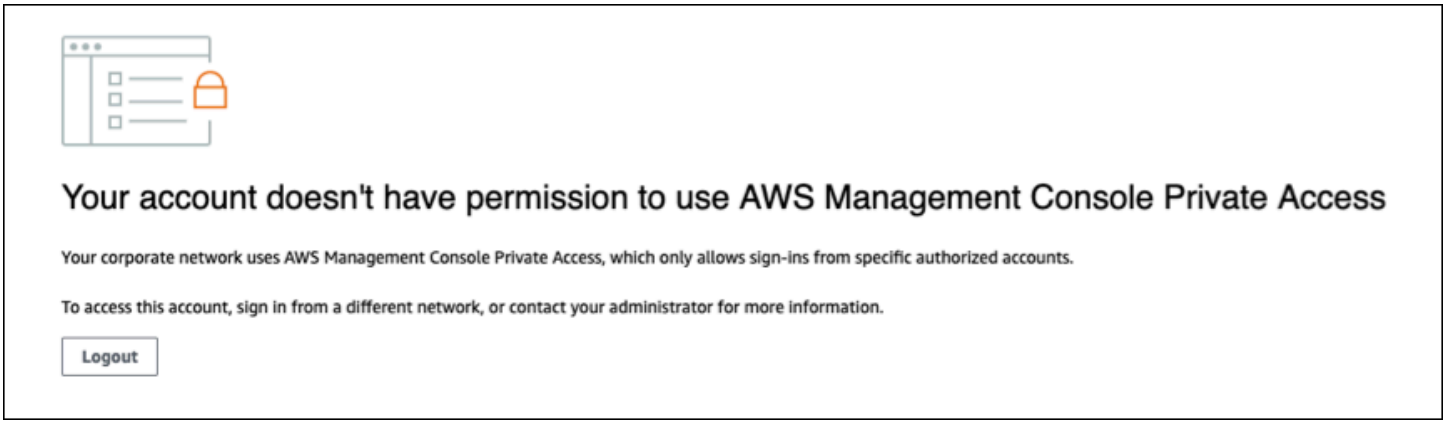
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "S3:*",
            "Resource": "*",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "aws:SourceVpc": "sourceVPC"
                },
                "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.

```
{
    "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.

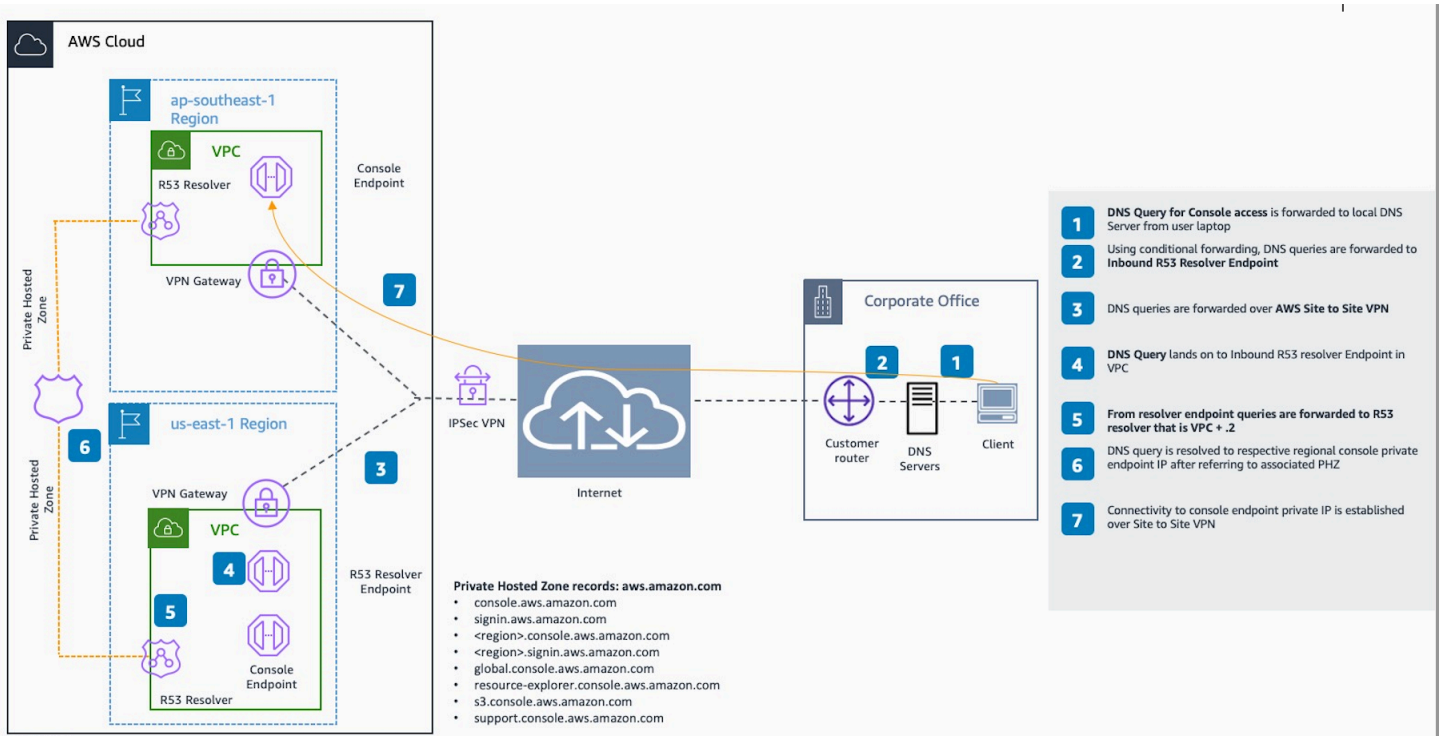


Architecture de référence

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.

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

Paragraphes, 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 :

```
 

 
```

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).
```

Listes

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.

- 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.

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 AWS Health Dashboard.

Je veux modifier la langue de la AWS Management Console mais je ne trouve pas le menu de sélection de la langue au bas de la 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.

Modification	Description	Date
Page ajoutée	Nouvelle page ajoutée pour expliquer la fonctionnalité multisession. 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 informati ons, 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
Obtenez de l'aide	Une nouvelle page a été ajoutée pour décrire comment obtenir de l'aide. Pour de plus amples informations, veuillez consulter ???.	18 juin 2024

Modification	Description	Date
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
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

Modification	Description	Date
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 Managemen t Console. Pour de plus amples informations, veuillez consulter la section Modificat ion de la langue de la AWS Management Console.	1 avril 2021
Lancement CloudShell	Ouvrez AWS CloudShell depuis AWS Managemen t 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.