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 le AWS Management Console ?

AWS Management ConsoleIl s'agit d'une application Web qui comprend et fait référence à une vaste collection de consoles de service pour la gestion AWS des ressources. Lors de votre première connexion, vous accédez à la page d'accueil de la console. La page d'accueil permet d'accéder à chaque console de service, et offre un emplacement unique pour accéder aux informations dont vous avez besoin pour exécuter vos tâches associées à AWS . Il vous permet également de personnaliser l'expérience de la console d'accueil en ajoutant, en supprimant et en réorganisant des widgets tels que Recently visited, AWS Health, etc.

> **Note**
>
> L'option de sélection de la langue a été déplacée vers la nouvelle page Paramètres unifiés. Pour de plus amples informations, veuillez consulter la section Modification de la langue de la AWS Management Console.

Les consoles de service individuelles, d'autre part, offrent une vaste gamme d'outils pour le cloud computing, ainsi que des informations sur votre compte et sur votre facturation.

Utilisation de l'appareil de votre choix

La AWS Management Console a été conçue pour être utilisée sur tablette, ainsi que sur d'autres types d'appareils :

- 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.

AWS Management Console Il est également disponible sous forme d'application pour Android et iOS. Cette application fournit des tâches adaptées à une utilisation mobile et qui aident à améliorer l'expérience Web. Par exemple, vous pouvez facilement consulter et gérer vos instances Amazon EC2 existantes et vos CloudWatch alarmes Amazon depuis votre téléphone.

Vous pouvez télécharger l'application mobile AWS Console depuis Amazon Appstore, Google Play ou iTunes.

Configuration du AWS Management Console

Cette rubrique décrit comment configurer AWS Management Console et utiliser la page des paramètres unifiés pour définir les valeurs par défaut applicables à toutes les consoles de service. Il explique également les widgets, une fonctionnalité du tableau de bord de console d'accueil qui vous permet d'ajouter des composants personnalisés permettant de suivre les informations relatives à vos AWS services et ressources.

Rubriques

Utilisation des widgets

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.

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. Sélectionnez l'indicateur de glissement, représenté par six points verticaux en haut à gauche de la barre de titre du widget, puis faites-le glisser vers le tableau de bord Page d'accueil de la console.

Pour supprimer un widget

1. Sélectionnez les trois points de suspension verticaux en haut à droite de la barre de titre du widget.

2. Choisissez Remove widget (Supprimer le widget).

Pour réorganiser vos widgets

- Sélectionnez l'indicateur de glissement, représenté par six points verticaux en haut à gauche de la barre de titre du widget, puis faites glisser le widget vers un nouvel emplacement sur le tableau de bord Page d'accueil de la console.

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.

Configuration des paramètres unifiés

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. 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.

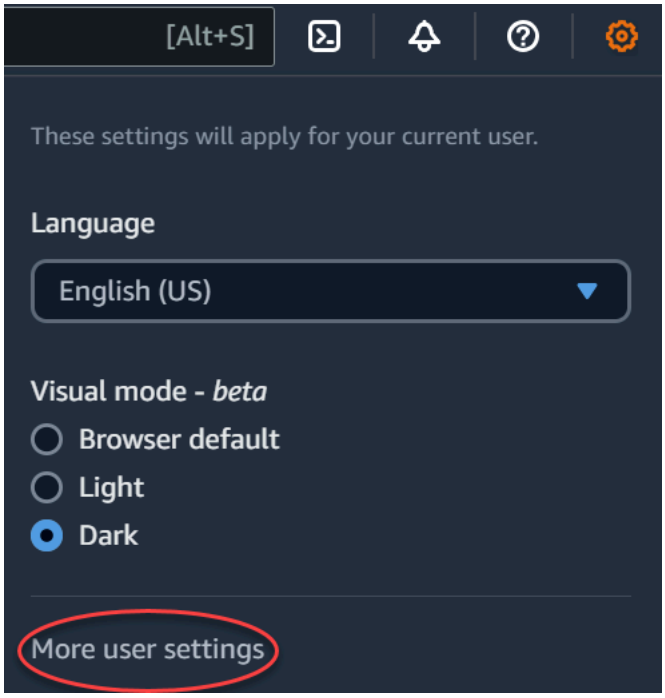
> **Important**
>
> Pour garantir la persistance de vos paramètres, de vos services favoris et des services récemment visités dans le monde entier, ces données sont stockées dans tous les pays Régions AWS, y compris dans les régions désactivées par défaut. Ces Régions sont Afrique (Le Cap), Asie-Pacifique (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.

Accès aux paramètres unifiés

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 Paramètres unifiés, choisissez Autres paramètres utilisateur.



Réinitialisation des paramètres unifiés

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

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

Pour réinitialiser tous les paramètres unifiés

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

Modification des paramètres unifiés

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 Plus de 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.

Modifier le mode visuel de 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.

Modification de la langue par défaut dans les paramètres unifiés

La procédure suivante explique comment modifier la langue par défaut à l'aide de 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.

Choisir une 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.

Pour choisir une région.

1. Connectez-vous à la AWS Management Console.
2. Choisissez un service pour accéder à la console correspondante.
3. Sur la barre de navigation, choisissez le nom de la région actuellement affichée. Choisissez ensuite la région que vous souhaitez utiliser.

Pour choisir une région par défaut

1. Dans la barre de navigation, cliquez sur l'icône Paramètres, puis choisissez Autres paramètres utilisateur pour accéder à la page Paramètres unifiés.
2. Choisissez Edit (Modifier) à côté de Localization and default Region (Localisation et région par défaut).
3. Sélectionnez votre région par défaut, puis cliquez sur Enregistrer les paramètres. Si vous ne sélectionnez pas de région par défaut, la dernière région que vous aurez visitée sera votre région par défaut.
4. (Facultatif) Choisissez Accéder à la nouvelle région par défaut pour accéder immédiatement à votre nouvelle région par défaut.

> **Note**
>
> Si vous avez créé AWS des ressources mais que vous ne les voyez pas dans la console, celle-ci affiche peut-être des ressources d'une autre région. Certaines ressources (par exemple, les instances Amazon EC2) sont spécifiques à la région dans laquelle elles ont été créées. Pour les afficher, utilisez le sélecteur Région pour choisir la région qui contient vos ressources.

Ajouter et supprimer des favoris

Pour accéder plus rapidement à vos services fréquemment utilisés, vous pouvez enregistrer leurs consoles de service dans une liste de Favoris.

Pour ajouter un service à la liste de Favoris

1. Connectez-vous à la AWS Management Console.

2. Cliquez sur le bouton Add widgets (Ajouter des widgets) dans le coin supérieur ou inférieur droit de la page.
3. Dans le menu Ajouter des widgets, sélectionnez les Favoris à ajouter à la console, puis choisissez Ajouter.

   Les favoris sont ajoutés au bas de la page d'accueil de votre console. Vous pouvez glisser-déposer les favoris en sélectionnant la barre de titre en haut du widget, puis faites glisser le widget vers un nouvel emplacement de la page.
4. Dans la barre de navigation, choisissez Services.
5. Dans la liste Récemment visité ou dans la liste Tous les services, arrêtez-vous sur le nom du service que vous souhaitez ajouter comme favori.
6. Cliquez sur l'étoile située à gauche du nom du service.
7. Répétez les deux étapes précédentes pour ajouter d'autres services à votre liste des Favoris.

Pour supprimer un service de la liste de Favoris

1. Dans la barre de navigation, choisissez Services.
2. Effectuez l'une des actions suivantes :

   - Dans la liste Favoris, survolez le nom d'un service. Ensuite, cliquez sur le x à droite du nom du service.
   - Dans la liste Visites récentes ou dans la liste Tous les services, désélectionnez l'étoile par le nom d'un service qui se trouve dans votre liste Favoris.

Modifier votre mot de passe

Si vous êtes titulaire d'un compte, vous pouvez modifier le mot de passe de votre AWS compte depuis le AWS Management Console.

Pour modifier votre mot de passe

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).

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 Paramètres, accessible depuis la barre de navigation. Vous pouvez effectuer cette modification n’importe où dans la console.

> **Note**
>
> Cette procédure change la langue de toutes les consoles, mais pas celle de la documentation AWS . Pour changer la langue utilisée pour la documentation, utilisez le menu des langues en haut à droite de la page de la documentation.

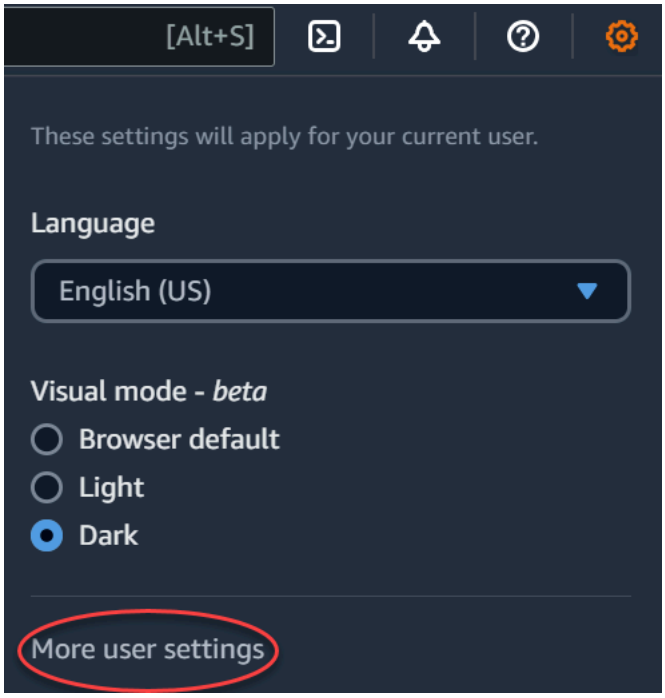
Les langues suivantes AWS Management Console sont actuellement prises en charge :

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

- Japonais
- Espagnol
- Italien
- Portugais
- Coréen
- Chinois (simplifié)
- Chinois (Traditionnel)

Pour changer la langue par défaut dans Paramètres unifiés

1. Connectez-vous à la AWS Management Console.
2. Dans la barre de navigation, cliquez sur l'icône Paramètres.
3. Pour ouvrir la page Paramètres unifiés, choisissez Autres 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.

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, cliquez sur l'icône Paramètres.
3. Pour Langue, choisissez Paramètre par défaut du navigateur ou votre langue préférée dans la liste déroulante.

Mise en route avec un service

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 plus d'informations, consultez Recherche de produits, de services, de fonctionnalités, etc. à l'aide de la recherche unifiée.
- Dans le widget Recently visited services (Services récemment visités), choisissez un nom de service.
- Dans le widget Recently visited services (Services récemment visités), choisissez View all AWS services (Afficher tous les services AWS). Ensuite, sur la page All AWS services (Tous les services AWS), 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.

Recherche de produits, de services, de fonctionnalités, etc. à l'aide de la recherche unifiée

Le champ de recherche de la barre de navigation fournit un outil de recherche unifié pour retrouver les AWS services et les fonctions, la documentation relative aux services et AWS Marketplace. Il suffit de saisir quelques caractères pour afficher les résultats de toutes ces catégories. Plus vous saisirez de caractères, plus la recherche affinera vos résultats.

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, entrez tout ou partie de vos termes de recherche.
2. Effectuez l'une des actions suivantes pour affiner votre recherche et obtenir plus de détails :
   - Pour limiter les résultats au type de contenu souhaité, choisissez l'une des catégories sur la gauche.
   - Pour afficher plus de résultats pour une catégorie particulière, choisissez Afficher tous les ***n*** résultats par titre de chaque catégorie. Pour revenir à la liste des résultats principaux, choisissez Retour dans le coin supérieur gauche.
   - Pour accéder rapidement aux fonctions populaires d'un service, mettez en pause le nom du service dans les résultats et cliquez sur un lien.
   - Pour obtenir plus de détails sur une documentation ou un AWS Marketplace résultat, faites une pause sur le titre du résultat.
3. Cliquez sur n'importe quel lien pour accéder à votre service, rubrique ou AWS Marketplace page.

> **Tip**
>
> Vous pouvez également utiliser votre clavier pour accéder rapidement au résultat de recherche le plus élevé. Premièrement, appuyez sur Appuyez sur les touches Alt+s (Windows) ou Option+s (macOS) pour accéder à la barre de recherche. Commencez ensuite à saisir votre terme de recherche. Lorsque le résultat souhaité s'affichera en haut de la liste, appuyez sur la touche Entrée. Par exemple, pour accéder rapidement à la console Amazon EC2, saisissez ec2 et appuyez sur la touche Entrée.

Discutez avec le développeur Amazon Q

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?`

Qu'est-ce que MyApplications est activé ? AWS

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. 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

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 API AWS Management Console, les CLI et les SDK. 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

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)

Démarrage avec myApplications

Pour démarrer avec myApplications afin de créer, de surveiller et de gérer vos applications, procédez comme suit.

Étape 1 : Création d'une application

Créez une nouvelle application ou intégrez une AppRegistry application existante créée avant le 8 novembre 2023 pour commencer à utiliser MyApplications.

Create an application

Pour créer une application

1. Connectez-vous à la AWS Management Console.
2. Dans la barre latérale gauche, 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 et peut être utilisée pour identifier les ressources associées à votre application. 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 existantes :

> **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.

a. Choisissez Sélectionner les ressources.

b. (Facultatif) Choisissez une vue.

c. 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.

d. Cochez la case à côté des ressources que vous souhaitez ajouter.

e. Choisissez Ajouter.

f. Choisissez Suivant.

10. Vérifiez vos choix.

11. 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 .

12. Choisissez Créer une application.

Onboard existing application

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 Intégrer ***`nom de l'application`***.
6. Si vous CloudFormation associez une pile, cochez la case dans la zone d'alerte.
7. Choisissez Intégrer l'application.

Étape 2 : Affichage des applications

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.

Gestion d'applications

Cette rubrique explique comment vous pouvez gérer vos applications.

Modification d'applications

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 myApplications, choisissez Actions, puis Modifier l'application.
5. Dans Modifier la description de l'application, mettez à jour la description, puis choisissez Enregistrer les modifications.

Pour modifier des balises

- Suivez les étapes décrites dans la section Gestion des balises du Guide de AWS Service Catalog AppRegistry l'administrateur.

Pour modifier des groupes d'attributs

- Suivez les étapes décrites dans la section Modification des groupes d'attributs dans le guide de AWS Service Catalog AppRegistry l'administrateur.

Suppression d'applications

Vous pouvez supprimer des applications lorsqu'elles ne sont plus requises.

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. Sélectionnez Delete (Supprimer).
7. Confirmez votre suppression, puis choisissez Supprimer l'application.

Création d'extraits de code

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.

Gestion des ressources

Cette rubrique explique comment gérer vos ressources.

Ajout de ressources

L'ajout de ressources à vos applications vous permet de les regrouper et de gérer leur sécurité, leurs performances et leur conformité.

Pour ajouter 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.

Suppression de ressources

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

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 plus d'informations, consultez Utilisation des widgets.

Widget de configuration du tableau de bord des applications

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

Widget récapitulatif des applications

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

Widget de calcul

Ce widget affiche les informations et les métriques relatives aux ressources de calcul que vous ajoutez à votre application. Cela inclut le nombre total d'alarmes et le nombre total de types de ressources de calcul. Le widget affiche également des graphiques de tendance relatifs aux

indicateurs de performance des ressources issus Amazon CloudWatch de l'utilisation du processeur des instances Amazon EC2 et des appels Lambda.

Configuration du widget de calcul

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

Widget de coûts et d'utilisation

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

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 plus d’informations, consultez 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 .

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 de correctifs automatisés pour les instances Amazon EC2 en AWS Systems Manager configurant le gestionnaire de correctifs. Pour plus d'informations, consultez Utilisation des stratégies de correctifs Quick Setup dans le Guide de l'utilisateur AWS Systems Manager .

Pour en savoir plus sur la tarification, consultez Tarification AWS Systems Manager.

Widget de surveillance et d'opérations

Ce widget affiche :

- Alarmes et alertes pour les ressources associées à votre application
- Objectifs de niveau de service (SLO) et métriques des applications
- 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 informations sur les CloudWatch applications 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.

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. AWS Management Console L'accès privé 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.

Rubriques

Consoles Régions AWS de service et fonctionnalités 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 (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)
- 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
- Amazon Athena
- AWS Auto Scaling
- AWS Billing Conductor
- AWS Certificate Manager
- AWS Cloud Map
- Amazon CloudFront
- Amazon CloudWatch
- AWS CodeArtifact
- AWS CodeBuild
- Amazon CodeGuru
- Amazon Comprehend
- Amazon Comprehend Medical
- AWS Compute Optimizer
- AWS Console Home
- AWS Database Migration Service
- AWS DeepRacer
- Amazon DocumentDB
- Amazon DynamoDB
- Amazon EC2
- Amazon EC2 Global View (Amazon EC2 Global View)
- EC2 Image Builder
- Amazon EC2 Instance Connect
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- AWS Elastic Disaster Recovery
- Amazon Elastic File System
- Amazon Elastic Kubernetes Service
- Amazon ElastiCache

- Amazon EMR
- Amazon EventBridge
- Amazon GameLift
- AWS Global Accelerator
- AWS Glue DataBrew
- AWS Ground Station
- Amazon GuardDuty
- 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 Video Streams
- AWS Lambda
- Amazon Lex
- AWS License Manager
- Amazon Managed Grafana
- 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 Manager
- Amazon OpenSearch Service
- AWS Organizations
- Amazon S3 on Outposts
- Amazon SageMaker Runtime

- Données SageMaker synthétiques Amazon
- AWS Secrets Manager
- Service Quotas
- AWS Signer
- Amazon Simple Email Service
- Amazon Simple Queue Service
- Amazon Simple Storage Service (Amazon S3)
- AWS SQL Workbench
- AWS Step Functions
- AWS Support
- AWS Systems Manager
- AWS Transfer Family
- Paramètres unifiés
- Amazon VPC IP Address Manager (IPAM)

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 plus d'informations, consultez 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.comhealth.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 vos propres informations de région.

1. com.amazonaws. *`region`* .console pour AWS Management Console
2. com.amazonaws. *`region`* .signin for 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 Options de connectivité Amazon VPC à Amazon VPC dans le livre blanc Option de connectivité Amazon Virtual Private Cloud.

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 :

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

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

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

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

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

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

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

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

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

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

Points de terminaison VPC et configuration des services DNSAWS

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

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

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

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

Pour de plus amples informations sur les SCP, veuillez consulter Politiques de contrôle de service (SCP) dans le Guide de l'utilisateur AWS Organizations .

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

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

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

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

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

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

```
{
  "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 condition `aws:SourceVpce` est définie en fonction des identifiants des points de terminaison de VPC de connexion et de console respectifs.

> **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 de VPC. Cette rubrique décrit comment tester l'accès privé AWS Management Console sans une infrastructure à grande échelle.

Rubriques

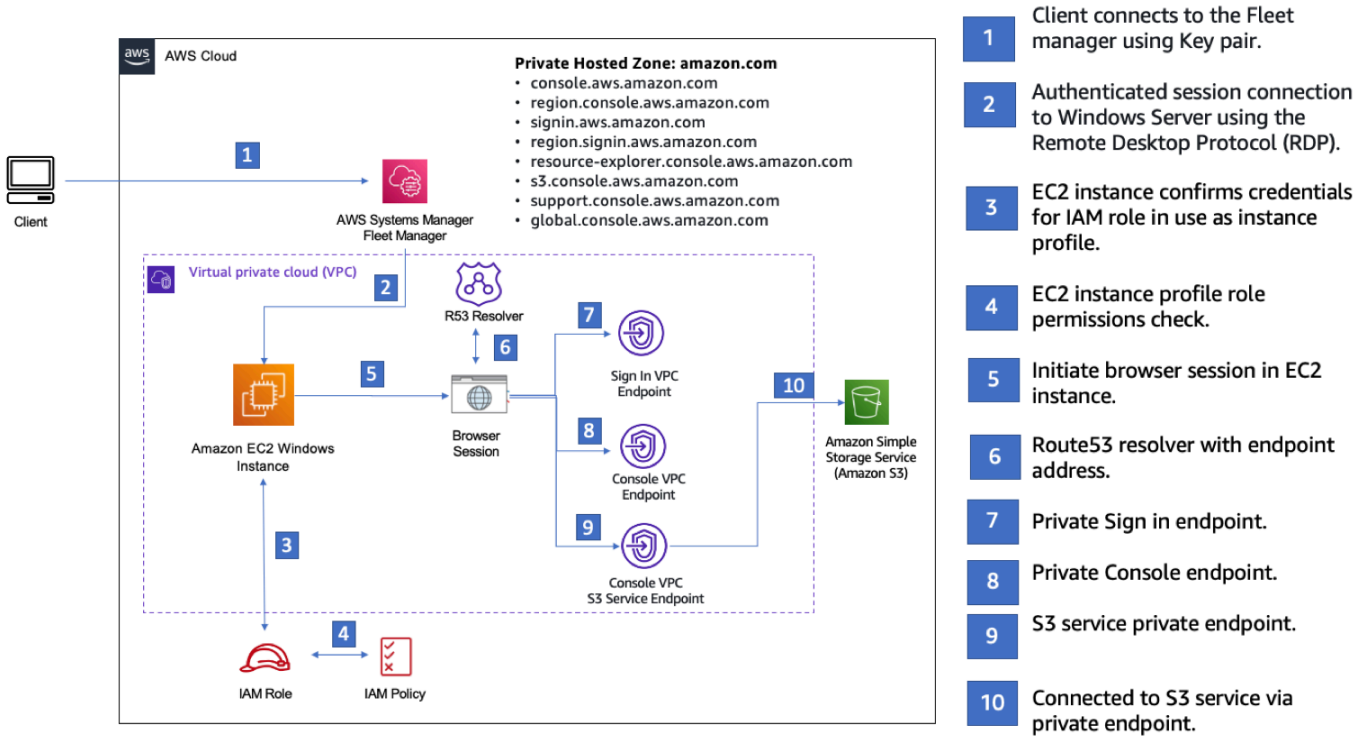
- Configuration test avec Amazon EC2
- Configuration des tests avec Amazon WorkSpaces
- Configuration test du VPC avec des politiques IAM

Configuration test avec Amazon EC2

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

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

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



Copiez le 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 Modèle Amazon AWS CloudFormation EC2 d'environnement d'accès privé

```
Description: |
  AWS Management Console Private Access.
Parameters:
  VpcCIDR:
    Type: String
    Default: 172.16.0.0/16
    Description: CIDR range for VPC
```

```
  Ec2KeyPair:
    Type: AWS::EC2::KeyPair::KeyName
    Description: The EC2 KeyPair to use to connect to the Windows instance

  PublicSubnet1CIDR:
    Type: String
    Default: 172.16.1.0/24
    Description: CIDR range for Public Subnet A

  PublicSubnet2CIDR:
    Type: String
    Default: 172.16.0.0/24
    Description: CIDR range for Public Subnet B

  PublicSubnet3CIDR:
    Type: String
    Default: 172.16.2.0/24
    Description: CIDR range for Public Subnet C

  PrivateSubnet1CIDR:
    Type: String
    Default: 172.16.4.0/24
    Description: CIDR range for Private Subnet A

  PrivateSubnet2CIDR:
    Type: String
    Default: 172.16.5.0/24
    Description: CIDR range for Private Subnet B

  PrivateSubnet3CIDR:
    Type: String
    Default: 172.16.3.0/24
    Description: CIDR range for Private Subnet C

  LatestWindowsAmiId:
    Type: 'AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>'
    Default: '/aws/service/ami-windows-latest/Windows_Server-2022-English-Full-Base'

  InstanceTypeParameter:
    Type: String
    Default: 't2.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

  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

  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 clés Amazon EC2 existantes dans votre compte. Si vous ne disposez pas d'une paire de clés Amazon EC2 existante, vous devez en créer une avant de passer à l'étape suivante. Pour plus d'informations, consultez la section Création d'une paire de clés à l'aide d'Amazon EC2 dans le guide de l'utilisateur Amazon EC2.
7. Sélectionnez Créer la pile.
8. Une fois la pile créée, choisissez l'onglet Ressources pour afficher les ressources qui ont été créées.

Pour vous connecter à l'instance Amazon EC2

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

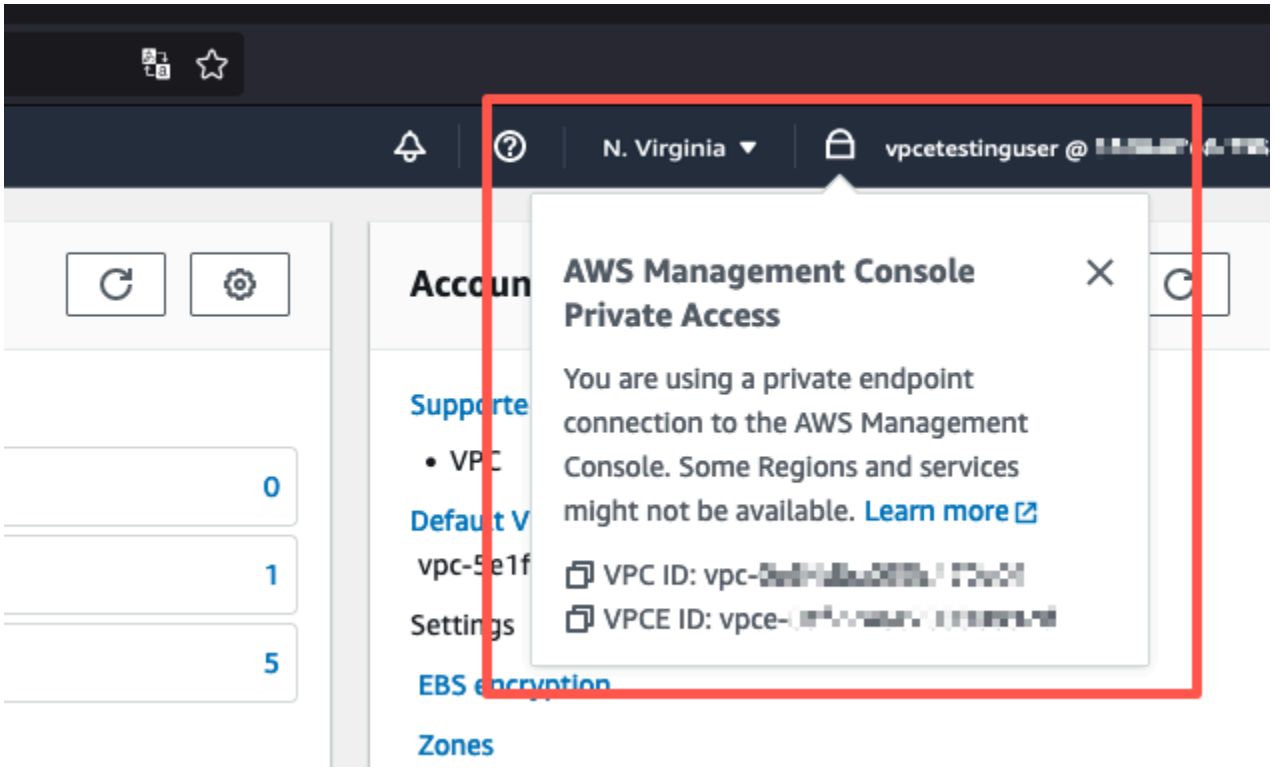
> **Note**
>
> Cet exemple utilise Fleet Manager, une fonctionnalité de AWS Systems Manager Explorer, pour se connecter à votre serveur Windows. Plusieurs minutes peuvent être nécessaires pour démarrer la connexion.

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'instance Amazon EC2 et accéder au bureau Windows via l'interface Web, utilisez la clé privée associée à la paire de clés Amazon EC2 que vous avez utilisée lors AWS CloudFormation de la création du modèle.

7. À partir de l'instance Windows Amazon EC2, ouvrez-la AWS Management Console 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.



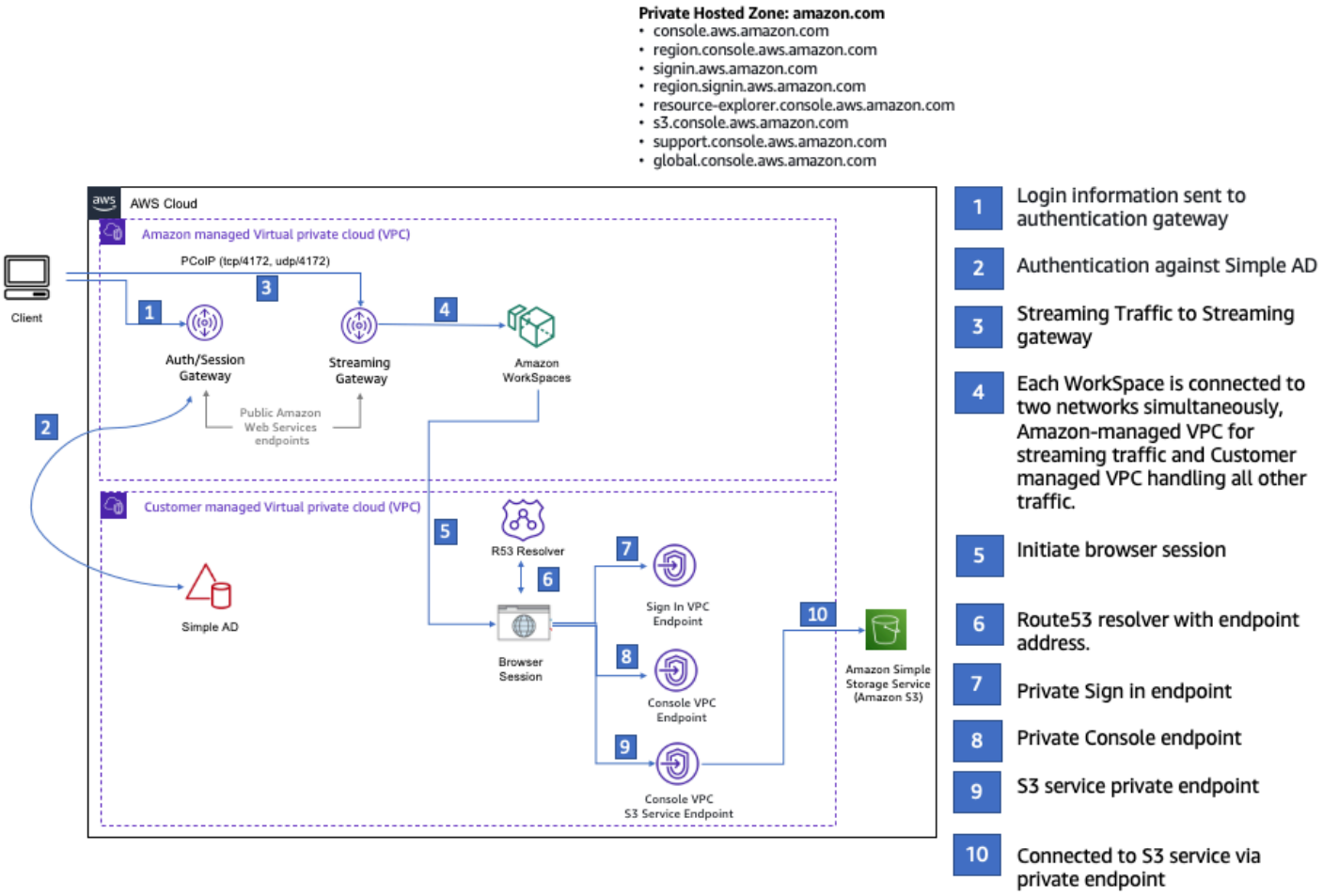
Configuration des tests avec Amazon WorkSpaces

Amazon vous WorkSpaces permet de fournir des ordinateurs de bureau Windows, Amazon Linux ou Ubuntu Linux virtuels basés sur le cloud pour vos utilisateurs, appelés WorkSpaces. 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

# 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

  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

  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: "ADAdminSecret"
      Description: "Password for directory services admin"
      GenerateSecretString:
        SecretStringTemplate: '{"username": "Admin"}'
        GenerateStringKey: password
        PasswordLength: 30
        ExcludeCharacters: '"@/\'

  WorkspaceSimpleDirectory:
    Type: AWS::DirectoryService::SimpleAD
    DependsOn: AppVPC
    DependsOn: PrivateSubnetA
    DependsOn: PrivateSubnetB
    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:
```

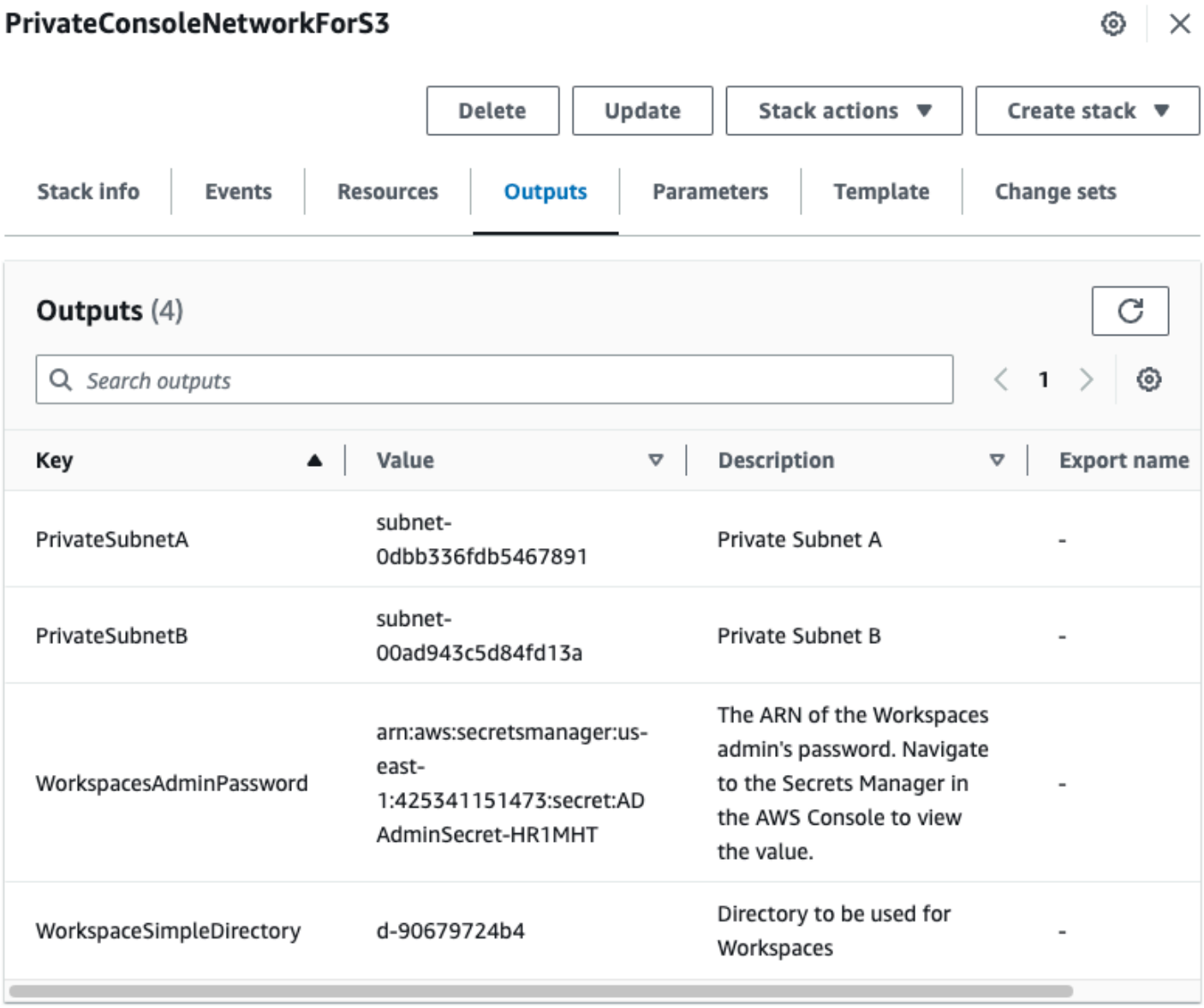
```
    Description: Directory to be used for Workspaces
    Value: !Ref WorkspaceSimpleDirectory

  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.

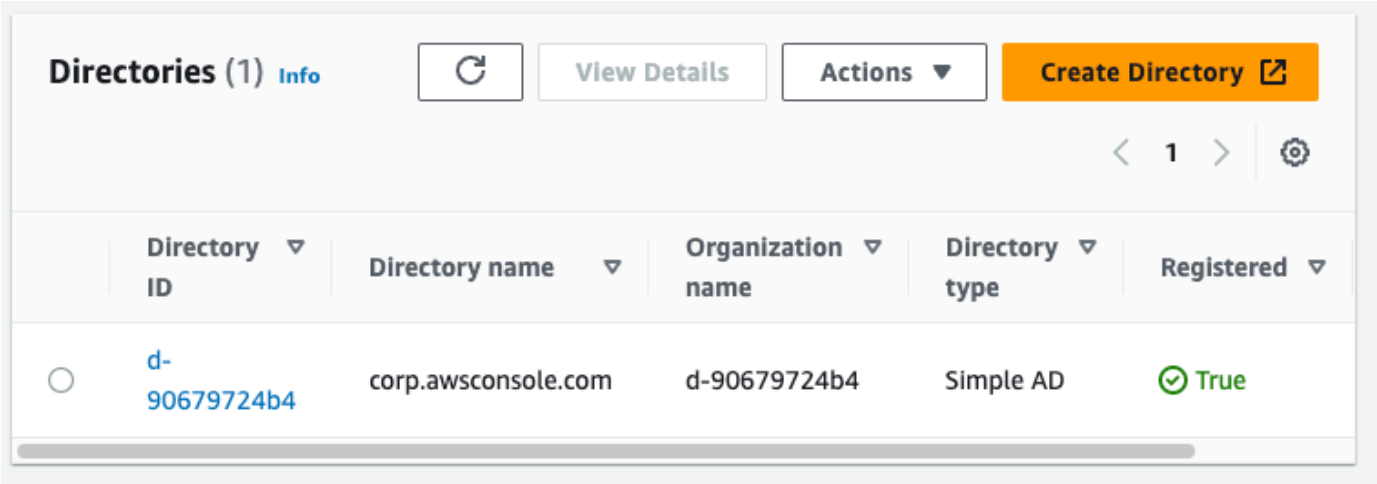
La capture d'écran suivante montre l'onglet Sorties qui affiche les valeurs des sous-réseaux privés et de l'annuaire Workspace Simple Directory.



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 e-mail pour vous permettre d'utiliser le WorkSpace. Vérifiez que l'adresse e-mail est valide car les informations de WorkSpace connexion sont envoyées à cette adresse e-mail.
10. Choisissez Suivant.
11. Sur la page Identifier les utilisateurs, sélectionnez l'utilisateur que vous avez créé à l'étape 9, puis choisissez Suivant.
12. Sur la page Sélectionner un bundle, choisissez Standard avec Amazon Linux 2, puis choisissez Suivant.
13. Utilisez les paramètres par défaut pour le mode d'exécution et la personnalisation utilisateur, puis sélectionnez Créer des instances WorkSpaces. Le `Pending` statut WorkSpace commence et passe à `Available` environ 20 minutes.
14. Lorsque le sera WorkSpace disponible, vous recevrez un e-mail contenant les instructions pour y accéder à l'adresse e-mail que vous avez fournie à l'étape 9.

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

Pour accéder à un WorkSpace

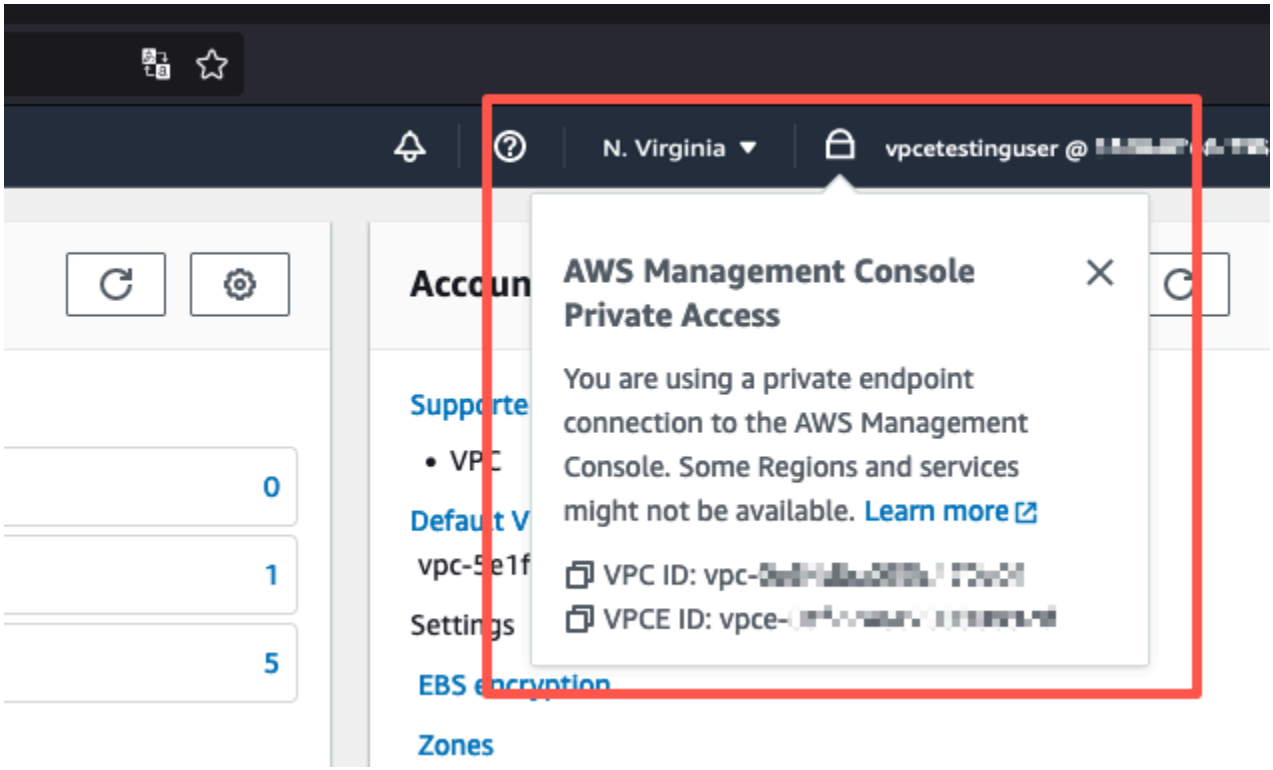
1. Ouvrez l'e-mail que vous avez reçu à l'étape 14 de la procédure précédente.
2. Dans l'e-mail, choisissez le lien unique fourni pour configurer votre profil et télécharger le WorkSpaces client.
3. Définissez votre mot de passe.
4. Téléchargez le client de votre choix.
5. Installez et lancez le client.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

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

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

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

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



Configuration test du VPC avec des politiques IAM

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

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

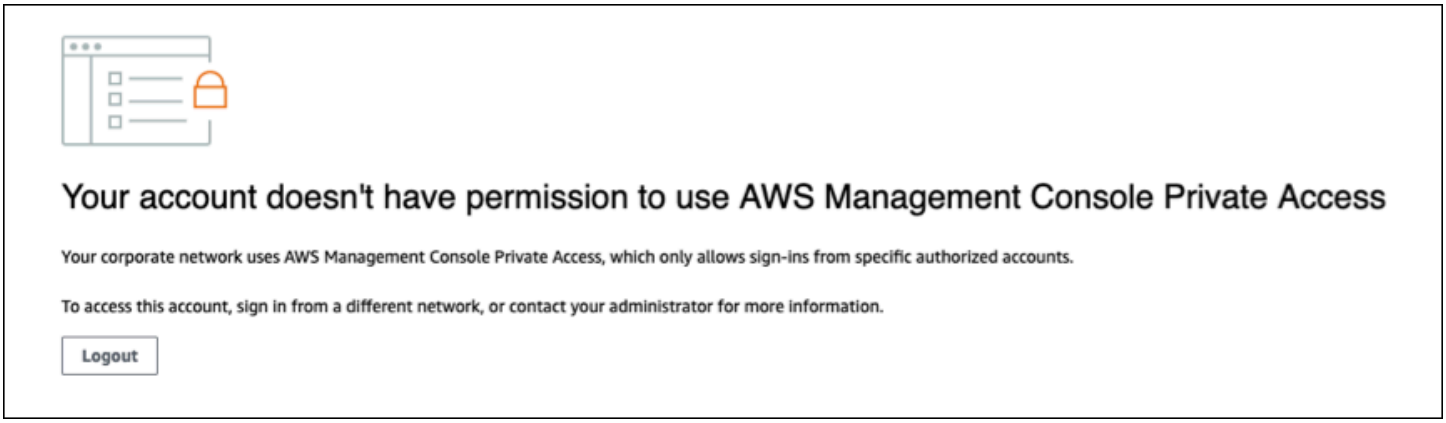
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "S3:*",
            "Resource": "*",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "aws:SourceVpc": "sourceVPC"
                },
       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

```
            }
        }
    ]
}
```

La politique suivante limite la connexion aux Compte AWS identifiants sélectionnés en utilisant 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"
                    ]
                }
            }
        }
    ]
}
```

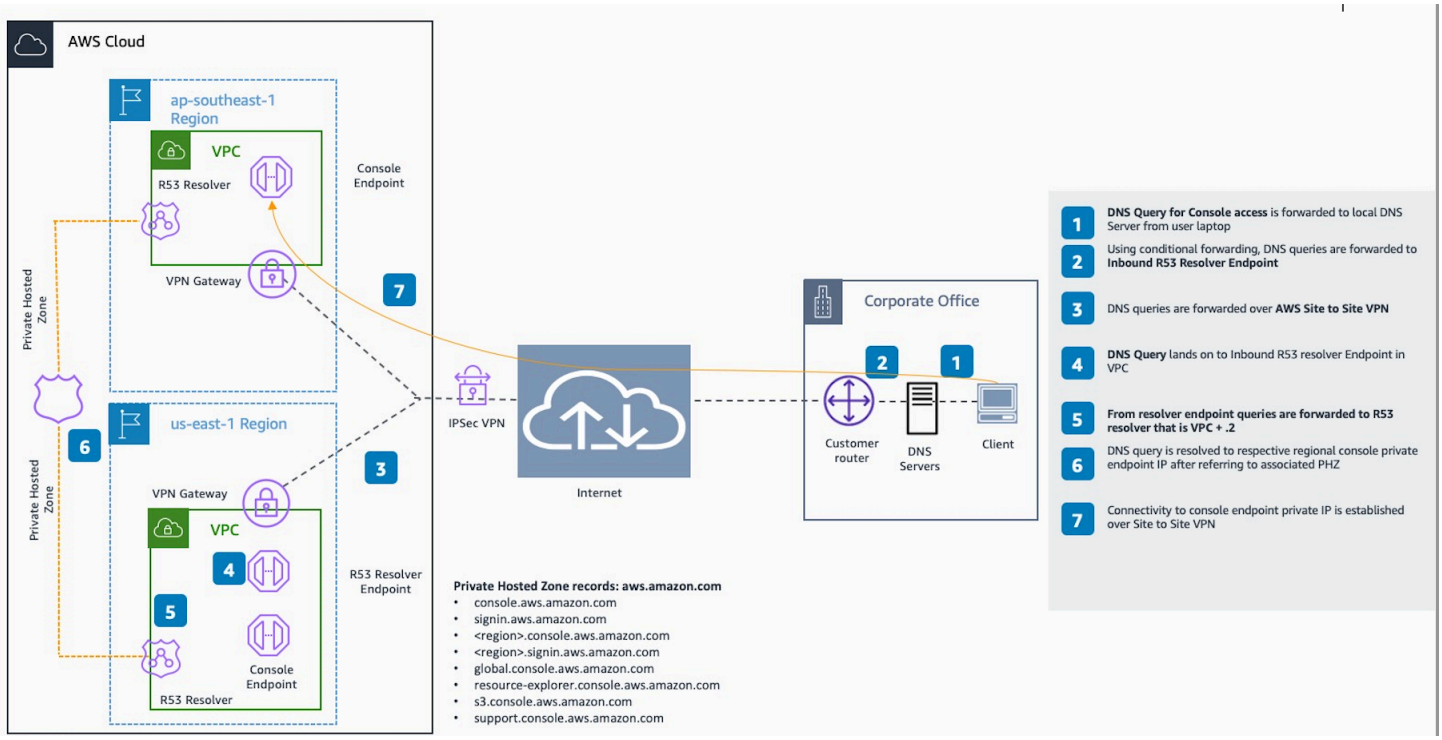
Si vous vous connectez avec une identité qui n'appartient pas à votre compte, la page d'erreur suivante s'affiche.



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 d'un VPN de site à site.AWS 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 les adresses IP privées des points de terminaison d'accès AWS Management Console privé.

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.

Lancement de AWS CloudShell depuis la barre d'outils de la console

AWS CloudShell est un shell préauthentifié, basé sur un navigateur, que vous pouvez lancer directement dans la AWS Management Console à partir de la barre d'outils de la console. Vous pouvez exécuter des commandes AWS CLI contre les services utilisant votre shell préféré (Bash, PowerShell ou Z).

Vous pouvez lancer CloudShell à partir de la Console Toolbar en utilisant l'une des deux méthodes suivantes :

- Choisissez l'icône CloudShell en bas à gauche de la console.
- Choisissez l'icône CloudShell 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 où AWS CloudShell est disponible, consultez la liste des services AWS régionaux. La sélection de la région de la console est synchronisée avec la région CloudShell. Si CloudShell n'est pas disponible dans une région sélectionnée, CloudShell fonctionnera dans la région la plus proche.

Obtention d'informations sur la facturation

Si vous disposez des autorisations nécessaires, vous pouvez obtenir des informations sur vos frais AWS dans la console.

Pour obtenir des informations sur votre facturation

1. Sur la barre de navigation, choisissez le nom de votre compte.
2. Choisissez Billing Dashboard (Tableau de bord de facturation).
3. Utilisez le tableau de bord AWS Billing and Cost Management pour afficher un résumé et une répartition de vos dépenses mensuelles. Pour en savoir plus, consultez le AWS Billingguide de l'utilisateur.

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 vous utilisez tous les éléments suivants :

- Un navigateur depuis un VPC.
- Points de terminaison VPC.
- Politiques IAM contenant une clé de condition `aws:SourceIp` globale.

Dans la console, accédez à la page des politiques IAM. Nous vous recommandons de consulter les politiques IAM qui contiennent une clé de condition `aws:SourceIp` globale et une clé d'ajout`aws:SourceVpc`.

Vous pouvez également envisager d'intégrer la fonctionnalité d'accès AWS Management Console privé pour y accéder AWS Management Console via un point de terminaison VPC et

d'`aws:SourceVpc`utiliser les conditions de vos politiques. Pour plus d'informations, consultez AWS Management Console Accès privé.

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-code.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
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
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	25 février 2022

Modification	Description	Date
	vers les AWS services. Pour plus d'informations, consultez Utilisation des widgets.	
Modification de la langue de la console	Choisissez une autre langue pour la AWS Management Console. Pour de plus amples informations, veuillez consulter la section Modification de la langue de la AWS Management Console.	1 avril 2021
Lancement CloudShell	Ouvrez AWS CloudShell depuis AWS Management Console et exécutez les commandes AWS CLI. Pour plus d'informations, consultez la section Lancement AWS CloudShell.	22 mars 2021

Glossaire AWS

Pour connaître la terminologie la plus récente d'AWS, consultez le Glossaire AWS dans la Référence Glossaire AWS.

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.