aws

Guide d’administration

Navigateur Amazon WorkSpaces Secure

Navigateur Amazon WorkSpaces Secure: Guide d’administration

Table of Contents

Qu'est-ce qu'Amazon WorkSpaces Secure Browser ?

> **Note**
>
> Amazon WorkSpaces Secure Browser était auparavant connu sous le nom d'Amazon WorkSpaces Web.

Amazon WorkSpaces Secure Browser est un service de navigateur hébergé entièrement géré, natif du cloud, utilisé pour accéder en toute sécurité à des sites Web privés et à des applications Web software-as-a-service (SaaS), interagir avec des ressources en ligne et naviguer sur Internet à partir d'un contenant jetable. WorkSpaces Secure Browser fonctionne avec les navigateurs Web existants d'un utilisateur, sans surcharger le service informatique lié à la gestion des appliances, de l'infrastructure, des logiciels clients spécialisés ou des connexions de réseau privé virtuel (VPN). Le contenu Web est diffusé vers le navigateur Web de l'utilisateur, tandis que le navigateur et le contenu Web sont isolés dans AWS. En utilisant les mêmes technologies sous-jacentes qui alimentent les services informatiques destinés aux utilisateurs AWS finaux tels qu'Amazon WorkSpaces et Amazon AppStream 2.0, WorkSpaces Secure Browser peut être plus rentable que les bureaux virtuels traditionnels et réduire la complexité par rapport à la fourniture de logiciels de gestion aux appareils appartenant à l'entreprise. WorkSpaces Secure Browser réduit le risque d'exfiltration de données en diffusant du contenu Web. Aucun code HTML, aucun modèle d'objet de document (DOM) ou aucune donnée d'entreprise sensible n'est transmis à la machine locale. En isolant l'appareil, le réseau d'entreprise et Internet les uns des autres, la surface d'attaque du navigateur est pratiquement éliminée.

Vous pouvez appliquer la politique de navigation de l'entreprise (y compris l'autorisation/le blocage des URL) à toutes les sessions, et inclure des contrôles au niveau de la session pour le presse-papiers, le transfert de fichiers et l'imprimante. Vous pouvez également restreindre l'accès à des réseaux ou à des appareils fiables à l'aide des contrôles d'accès IP. WorkSpaces Secure Browser est facile à configurer et à utiliser. Chaque session démarre avec une nouvelle version entièrement corrigée du navigateur Chrome, avec les politiques et les paramètres de l'entreprise appliqués.

Historique de versions

Le 20 mai 2024, Amazon WorkSpaces Web a été renommé Amazon WorkSpaces Secure Browser. Pour les clients existants, aucun changement n'a été apporté à la façon dont ils gèrent les utilisateurs

ou les ressources avec le service. La liste suivante décrit les mises à jour applicables qui ont également eu lieu à la suite de ce changement de nom.

L'espace de noms de l'API workspaces-web reste inchangé pour des raisons de rétrocompatibilité. Par conséquent, les ressources suivantes sont toujours les mêmes :

- Commandes CLI.
- CloudWatch Métriques Amazon. Pour plus d'informations, consultez the section called "Surveillance avec CloudWatch".
- Points de terminaison de service. Pour plus d'informations, consultez la section Points de terminaison et quotas Amazon WorkSpaces Secure Browser.
- AWS CloudFormation ressources. Pour plus d'informations, consultez la référence des types de ressources Amazon WorkSpaces Secure Browser.
- Rôle lié à un service contenant workspaces-web. Pour plus d'informations, consultez the section called "Utilisation des rôles liés à un service".
- URL de console contenant des espaces de travail Web.
- URL de documentation contenant des espaces de travail Web. Pour plus d'informations, consultez la documentation Amazon WorkSpaces Secure Browser.
- Rôle ReadOnly géré existant. Pour plus d'informations, consultez the section called "AWS politiques gérées".
- Nom de la subvention KMS.
- Préfixe de flux Kinesis UAL (User-Activity Logging).

En outre, les URL des portails existants restent les mêmes. Les URL des portails créés avant le 20 mai 2024 utilisaient le format <UUID>.workspaces-web.com. WorkSpaces Les portails Secure Browser continuent d'utiliser ce format et le domaine workspaces-web.com.

Termes à connaître lors de l'utilisation de WorkSpaces Secure Browser

Pour vous aider à démarrer avec WorkSpaces Secure Browser, vous devez vous familiariser avec les concepts suivants.

Identity provider (IdP) (Fournisseur d'identité)

Un fournisseur d'identité vérifie les informations d'identification de vos utilisateurs. Il émet ensuite des assertions d'authentification afin d'autoriser l'accès à un fournisseur de services. Vous pouvez configurer votre IdP existant pour qu'il fonctionne avec WorkSpaces Secure Browser.

La procédure de configuration d’un fournisseur d’identité (IdP) varie d’un IdP à l’autre.

Vous devez charger le fichier de métadonnées du fournisseur de services sur votre IdP. À défaut, vos utilisateurs ne pourront pas se connecter. Vous devez également autoriser vos utilisateurs à utiliser WorkSpaces Secure Browser dans votre IdP.

Document de métadonnées du fournisseur d’identité (IdP)

WorkSpaces Secure Browser nécessite des métadonnées spécifiques de la part de votre fournisseur d'identité (IdP) pour établir la confiance. Vous pouvez ajouter ces métadonnées à WorkSpaces Secure Browser en chargeant un fichier d'échange de métadonnées téléchargé depuis votre IdP.

Fournisseur de services (SP)

Un fournisseur de services accepte les assertions d’authentification et fournit un service à l’utilisateur. WorkSpaces Secure Browser agit en tant que fournisseur de services pour les utilisateurs authentifiés par leur IdP.

Document de métadonnées du fournisseur de services (SP)

Vous devrez ajouter les détails des métadonnées du fournisseur de services à l’interface de configuration de votre fournisseur d’identité (IdP). Les détails de cette procédure de configuration varient d’un fournisseur à l’autre.

SAML 2.0

Norme d'échange de données d'authentification et d'autorisation entre un fournisseur d'identité et un fournisseur de services.

Virtual Private Cloud (VPC)

Vous pouvez utiliser un VPC existant ou nouveau, les sous-réseaux correspondants et les groupes de sécurité pour lier votre contenu à Secure Browser. WorkSpaces

Les sous-réseaux doivent disposer d’une connexion stable à Internet, tout comme le VPC et les sous-réseaux qui doivent pouvoir se connecter aux sites web internes et SaaS (Software-as-a-Service) pour que les utilisateurs puissent accéder à ces ressources.

Les VPC, les sous-réseaux et les groupes de sécurité répertoriés proviennent de la même région que votre console WorkSpaces Secure Browser.

Trust store (Magasin d'approbations)

Si un utilisateur accédant à un site Web via WorkSpaces Secure Browser reçoit une erreur de confidentialité, telle que NET : :ERR_CERT_INVALID, ce site utilise peut-être un certificat signé par une autorité de certification privée (PCA). Vous devrez peut-être ajouter ou modifier les PCA dans votre magasin de confiance. En outre, si l'appareil d'un utilisateur nécessite que vous installiez un certificat spécifique pour charger un site Web, vous devrez ajouter ce certificat à votre magasin de confiance pour permettre à votre utilisateur d'accéder à ce site dans WorkSpaces Secure Browser.

En principe, les sites web accessibles au public ne nécessitent pas d’apporter de modifications à un magasin de confiance.

Portail web

Un portail web permet à vos utilisateurs d’accéder aux sites web internes et SaaS depuis leur navigateur. Vous pouvez créer un seul portail web par compte dans n’importe quelle région prise en charge. Pour demander à ce que cette limite soit portée à plus d’un portail, contactez le support.

Point de terminaison du portail web

Le point de terminaison du portail web est le point d’accès à partir duquel vos utilisateurs lanceront votre portail web après s’être connectés avec le fournisseur d’identité configuré pour le portail.

Le point de terminaison est accessible au public sur Internet et peut être intégré à votre réseau.

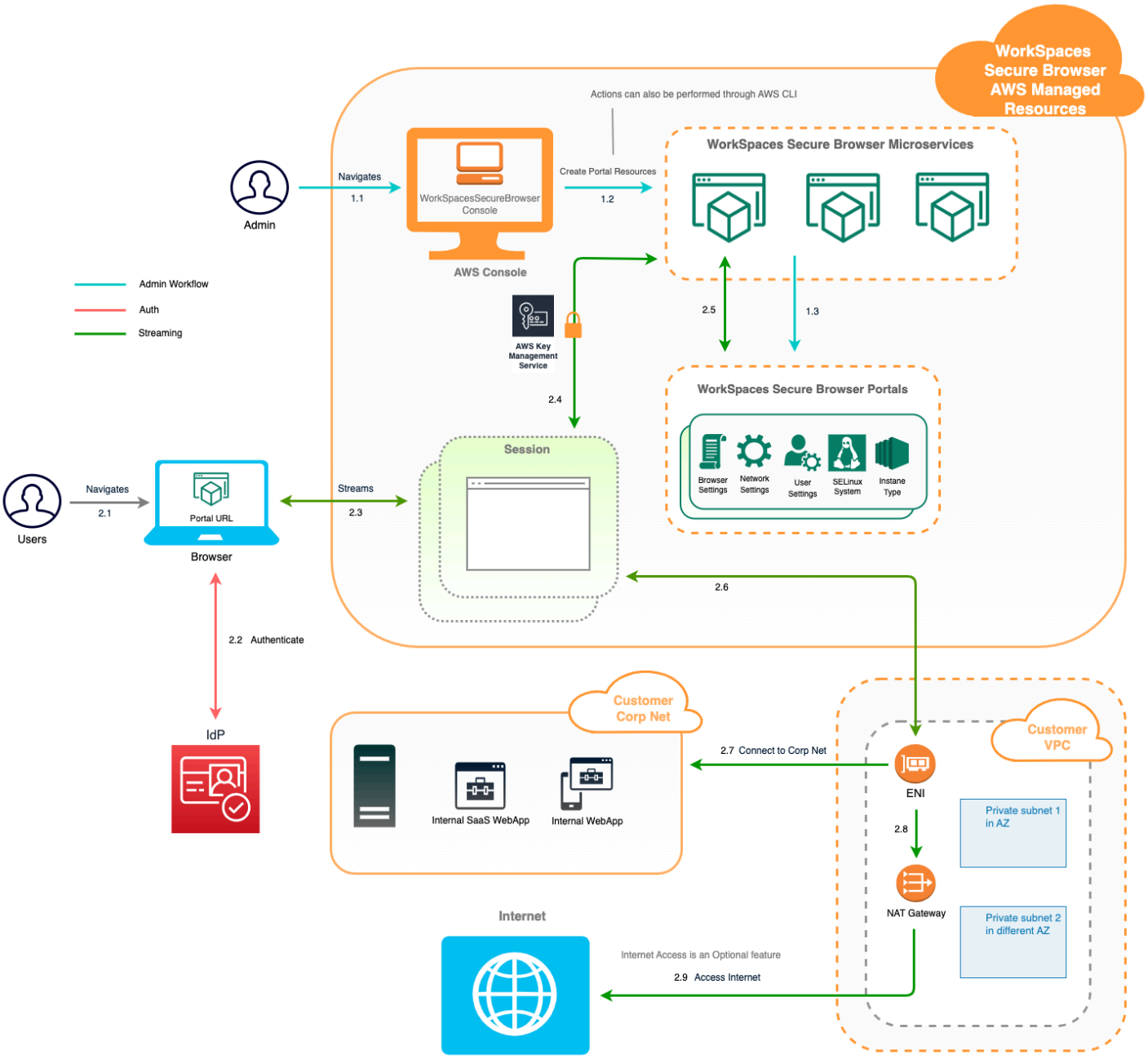
Services connexes

WorkSpaces Secure Browser est une fonctionnalité d'Amazon qui fait WorkSpaces partie du portefeuille AWS End User Computing. Par rapport à WorkSpaces et AppStream 2.0, WorkSpaces Secure Browser est conçu spécifiquement pour faciliter les charges de travail sécurisées sur le Web. WorkSpaces Secure Browser est géré automatiquement, la capacité, le dimensionnement et les images étant fournis et mis à jour à la demande par AWS. Par exemple, vous pouvez choisir de proposer un Workspace Desktop permanent à vos développeurs de logiciels qui ont besoin d'accéder aux ressources de bureau, et un navigateur WorkSpaces sécurisé aux utilisateurs du centre d'appels

qui n'ont besoin que d'un accès à une poignée de sites Web internes et SaaS (y compris ceux hébergés en dehors de votre réseau) sur des ordinateurs de bureau.

Architecture

Le schéma suivant montre l'architecture de WorkSpaces Secure Browser.



Accès au navigateur WorkSpaces sécurisé

Les administrateurs accèdent à WorkSpaces Secure Browser par le biais de la console WorkSpaces Secure Browser, du SDK, de la CLI ou de l'API. Vos utilisateurs y accèdent via le point de terminaison WorkSpaces Secure Browser.

Configuration de WorkSpaces Secure Browser

Avant de configurer WorkSpaces Secure Browser pour accéder à vos sites Web internes et à vos applications SaaS, vous devez remplir les conditions préalables suivantes.

Rubriques

Inscription et création d'un utilisateur

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des AWS services et des ressources de ce compte. Pour des raisons de sécurité, attribuez un accès administratif à un utilisateur et utilisez uniquement l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Après vous être inscrit à un Compte AWS, sécurisez Utilisateur racine d'un compte AWS AWS IAM Identity Center, activez et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, accordez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connectez-vous en tant qu'utilisateur disposant d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribuer l'accès à des utilisateurs supplémentaires

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme aux meilleures pratiques en matière d'application des autorisations du moindre privilège.

   Pour obtenir des instructions, voir Création d'un ensemble d'autorisations dans le guide de AWS IAM Identity Center l'utilisateur.
2. Affectez des utilisateurs à un groupe, puis attribuez un accès d'authentification unique au groupe.

   Pour obtenir des instructions, consultez la section Ajouter des groupes dans le guide de AWS IAM Identity Center l'utilisateur.

Accorder un accès par programmation

Les utilisateurs ont besoin d'un accès programmatique s'ils souhaitent interagir avec AWS l'extérieur du AWS Management Console. La manière d'accorder un accès programmatique dépend du type d'utilisateur qui y accède AWS.

Pour accorder aux utilisateurs un accès programmatique, choisissez l'une des options suivantes.

Quel utilisateur a besoin d'un accès programmatique ?	Pour	Par
Identité de la main-d'œuvre (Utilisateurs gérés dans IAM Identity Center)	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour le AWS CLI, voir Configuration du AWS CLI à utiliser AWS IAM Identity Center dans le guide de AWS Command Line Interface l'utilisateur. • Pour les AWS SDK, les outils et les AWS API, consultez la section Authentification IAM Identity

Quel utilisateur a besoin d'un accès programmatique ?	Pour	Par
		Center dans le Guide de référence AWS des SDK et des outils.
IAM	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées aux AWS CLI AWS SDK ou AWS aux API.	Suivez les instructions de la section Utilisation d'informations d'identification temporaires avec AWS les ressources du Guide de l'utilisateur IAM.
IAM	(Non recommandé) Utilisez des informations d'identification à long terme pour signer les AWS CLI demandes programmatiques adressées aux AWS SDK ou AWS aux API.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour le AWS CLI, voir Authentification à l'aide des informations d'identification utilisateur IAM dans le Guide de l'AWS Command Line Interface utilisateur. • Pour les AWS SDK et les outils, voir Authentifier à l'aide d'informations d'identification à long terme dans le Guide de AWS référence des SDK et des outils. • Pour les AWS API, consultez la section Gestion des clés d'accès pour les utilisateurs IAM dans le guide de l'utilisateur IAM.

Mise en réseau et accès

Les rubriques suivantes expliquent comment configurer des instances de streaming WorkSpaces Secure Browser afin que les utilisateurs puissent s'y connecter. Il explique également comment activer vos instances de streaming WorkSpaces Secure Browser pour accéder aux ressources VPC, ainsi qu'à Internet.

Rubriques

Exigences du VPC

Lors de la création du portail WorkSpaces Secure Browser, vous allez sélectionner un VPC dans votre compte. Vous choisirez également au moins deux sous-réseaux dans deux zones de disponibilité différentes. Ces VPC et sous-réseaux doivent répondre aux exigences suivantes :

- Le VPC doit disposer de la location par défaut. Les VPC dotés d'une location dédiée ne sont pas pris en charge.
- Pour des raisons de disponibilité, nous exigeons la création d'au moins deux sous-réseaux situés dans deux zones de disponibilité différentes. Vos sous-réseaux doivent avoir suffisamment d'adresses IP pour prendre en charge le trafic WorkSpaces Secure Browser attendu. Configurez chacun de vos sous-réseaux avec un masque de sous-réseau qui permet d'avoir un nombre suffisant d'adresses IP client pour prendre en considération le nombre maximal de sessions simultanées. Pour plus d'informations, consultez Création et configuration d'un VPC.
- Tous les sous-réseaux doivent disposer d'une connexion stable à tout contenu interne, situé dans AWS Cloud ou sur site, auquel les utilisateurs pourront accéder avec WorkSpaces Secure Browser.

Pour des raisons de disponibilité et de mise à l'échelle, nous vous recommandons de choisir trois sous-réseaux situés dans des zones de disponibilité différentes. Pour plus d'informations, consultez Création et configuration d'un VPC.

WorkSpaces Secure Browser n'attribue aucune adresse IP publique aux instances de streaming pour permettre l'accès à Internet. En effet, vos instances de streaming seraient dans ce cas accessibles depuis Internet. Autrement dit, aucune instance de streaming connectée à votre sous-réseau public ne disposera d'un accès Internet. Si vous souhaitez que votre portail WorkSpaces Secure Browser ait accès à la fois au contenu Internet public et au contenu VPC privé, suivez les étapes décrites dans. Activation de la navigation Internet sans restriction (recommandé)

Création et configuration d'un VPC

Cette section explique comment utiliser l'assistant VPC pour créer un VPC avec un sous-réseau public et un sous-réseau privé. Dans le cadre de cette procédure, l'assistant crée une passerelle Internet et une passerelle NAT. Il crée également une table de routage personnalisée associée au sous-réseau public. Il met ensuite à jour la table de routage principale associée au sous-réseau privé. La passerelle NAT est automatiquement créée dans le sous-réseau public de votre VPC.

Après avoir créé une configuration de VPC à l'aide de l'assistant, vous allez ajouter un deuxième sous-réseau privé. Pour en savoir plus sur cette configuration, consultez VPC avec des sous-réseaux publics et privés (NAT).

Étape 1 : Allocation d'une adresse IP Elastic

Avant de créer votre VPC, vous devez attribuer une adresse IP élastique dans votre région WorkSpaces Secure Browser. Une fois l'adresse IP Elastic allouée, vous pouvez l'associer à votre passerelle NAT. Une adresse IP Elastic vous permet de masquer une défaillance de votre instance de streaming en remappant rapidement l'adresse à une autre instance de streaming de votre VPC. Pour en savoir plus, consultez Adresses IP Elastic.

> **Note**
>
> Des frais peuvent s'appliquer aux adresses IP Elastic que vous utilisez. Pour en savoir plus, consultez la page de tarification des adresses IP Elastic.

Si vous ne disposez pas déjà d'une adresse IP Elastic, effectuez les étapes suivantes. Si vous voulez utiliser une adresse IP Elastic existante, vous devez d'abord vérifier qu'elle n'est pas actuellement associée à une autre instance ou interface réseau.

Pour allouer une adresse IP Elastic

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.

2. Dans le volet de navigation, sous Réseau et sécurité, choisissez Adresses IP Elastic.
3. Choisissez Allouer une nouvelle adresse, puis Allouer.
4. Notez l'adresse IP Elastic affichée sur la console.
5. Dans l'angle supérieur droit du volet Adresses IP Elastic, cliquez sur l'icône x pour fermer le volet.

Étape 2 : Création d'un VPC

Pour créer un VPC avec un sous-réseau public et un sous-réseau privé, effectuez les étapes suivantes.

Pour créer un VPC

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Tableau de bord du VPC.
3. Choisissez Launch VPC Wizard (Démarrer l'assistant VPC).
4. À l'Étape 1 : sélectionner une configuration VPC, choisissez VPC avec des sous-réseaux publics et privés, puis Sélectionner.
5. À l'Étape 2 : VPC avec des sous-réseaux publics et privés, configurez le VPC comme suit :
   - Pour Bloc d'adresse CIDR IPv4, spécifiez un bloc d'adresse CIDR IPv4 pour le VPC.
   - Pour Bloc d'adresse CIDR IPv6, conservez la valeur par défaut, Pas de bloc CIDR IPv6.
   - Dans Nom du VPC, donnez un nom unique au VPC.
   - Configurez le sous-réseau public en procédant comme suit :
     - Pour Bloc CIDR IPv4 du sous-réseau public, spécifiez le bloc d'adresse CIDR du sous-réseau.
     - Pour Zone de disponibilité, conservez la valeur par défaut, Aucune préférence.
     - Dans Nom du sous-réseau public, donnez un nom au sous-réseau. Par exemple, **`WorkSpaces Secure Browser Public Subnet`**.
   - Configurez le premier sous-réseau privé en procédant comme suit :
     - Pour Bloc CIDR IPv4 du sous-réseau privé, spécifiez le bloc d'adresse CIDR du sous-réseau. Notez la valeur que vous spécifiez.
     - Pour Zone de disponibilité, sélectionnez une zone spécifique et notez-la.

  - Dans Nom du sous-réseau privé, donnez un nom au sous-réseau. Par exemple, **`WorkSpaces Secure Browser Private Subnet1`**.
- Dans les champs restants, conservez les valeurs par défaut si elles conviennent.
- Dans ID d'allocation d'adresses IP Elastic, saisissez la valeur qui correspond à l'adresse IP Elastic que vous avez créée. Cette adresse est alors assignée à la passerelle NAT. Si vous n'avez pas d'adresse IP Elastic, créez-en une en utilisant la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
- Dans Points de terminaison de service, spécifiez un point de terminaison Amazon S3 si votre environnement en a besoin d'un.

  Pour spécifier un point de terminaison Amazon S3, procédez comme suit :

  1. Choisissez Ajouter un point de terminaison.
  2. Pour Service, sélectionnez com.amazonaws. Entrée ***`Region`*** .s3, où *`Region`* est la région dans laquelle Région AWS vous créez votre VPC.
  3. Pour Sous-réseau, choisissez Sous-réseau privé.
  4. Pour Stratégie, conservez la valeur par défaut Accès complet.
- Pour Activer les noms d'hôte DNS, conservez la valeur par défaut Oui.
- Pour Location matérielle, conservez la valeur par défaut Par défaut.
- Sélectionnez Create VPC (Créer un VPC).
- La configuration de votre VPC prend quelques minutes. Après avoir créé le VPC, choisissez OK.

Étape 3 : Ajout d'un deuxième sous-réseau privé

Dans l'étape précédente, vous avez créé un VPC avec un sous-réseau public et un sous-réseau privé. Pour ajouter un deuxième sous-réseau privé à votre VPC, effectuez les étapes suivantes. Nous vous recommandons d'ajouter un deuxième sous-réseau privé dans une autre zone de disponibilité que celle de votre premier sous-réseau privé.

Pour ajouter un deuxième sous-réseau privé

1. Dans le panneau de navigation, choisissez Subnets (Sous-réseaux).
2. Sélectionnez le premier sous-réseau privé que vous avez créé à l'étape précédente. Sous l'onglet Description, sous la liste des sous-réseaux, notez la zone de disponibilité de ce sous-réseau.

3. Dans l'angle supérieur gauche du volet des sous-réseaux, choisissez Créer le sous-réseau.
4. Dans Balise Nom, donnez un nom au sous-réseau privé. Par exemple, **`WorkSpaces Secure Browser Private Subnet2`**.
5. Pour VPC, sélectionnez le VPC que vous avez créé à l'étape précédente.
6. Pour Zone de disponibilité, sélectionnez une zone de disponibilité différente de celle que vous utilisez pour votre premier sous-réseau privé. La sélection d'une autre zone de disponibilité augmente la tolérance aux pannes et permet de réduire le risque d'erreurs de capacité insuffisante.
7. Pour Bloc d'adresse CIDR IPv4, spécifiez une plage de bloc d'adresse CIDR unique pour le nouveau sous-réseau. Par exemple, si votre premier sous-réseau privé possède une plage de bloc d'adresses CIDR IPv4 **`10.0.1.0/24`**, vous pouvez spécifier la plage **`10.0.2.0/24`** pour le deuxième sous-réseau privé.
8. Choisissez Créer.
9. Une fois le sous-réseau créé, choisissez Fermer.

Étape 4 : Vérification et désignation de vos tables de routage de sous-réseau

Après avoir créé et configuré votre VPC, effectuez les étapes suivantes pour nommer vos tables de routage. Vous devez vérifier que les points suivants sont respectés pour votre table de routage :

- La table de routage associée au sous-réseau dans lequel réside votre passerelle NAT doit comporter une route qui dirige le trafic Internet vers une passerelle Internet. Votre passerelle NAT peut ainsi accéder à Internet.
- Les tables de routage associées à vos sous-réseaux privés doivent être configurées pour diriger le trafic Internet vers la passerelle NAT. Les instances de streaming de vos sous-réseaux privés peuvent ainsi communiquer avec Internet.

Pour vérifier et nommer les tables de routage de vos sous-réseaux

1. Dans le volet de navigation, choisissez Sous-réseaux, puis sélectionnez le sous-réseau public que vous avez créé. Par exemple, le sous-réseau public WorkSpaces Secure Browser 2.0.
2. Dans l'onglet Route Table (Table de routage), choisissez l'ID de la table de routage. Par exemple, rtb-12345678.

3. Sélectionnez la table de routage. Sous Nom, choisissez l'icône de modification (crayon), puis nommez la table. Par exemple, saisissez le nom **`workspacesweb-public-routetable`**. Sélectionnez ensuite la coche pour enregistrer le nom.
4. Alors que la table de routage publique est toujours sélectionnée, dans l'onglet Routes, vérifiez qu'il existe bien deux routes : une pour le trafic local et une qui fait passer l'ensemble du trafic restant par la passerelle Internet du VPC. Le tableau suivant décrit ces deux routes :

Destination	Cible	Description
Bloc d'adresses CIDR IPv4 du sous-réseau public (par exemple, 10.0.0/20)	Local	Ensemble du trafic en provenance des ressource s destiné aux adresses IPv4 du bloc d'adresses CIDR IPv4 du sous-réseau public. Ce trafic est acheminé localement au sein du VPC.
Trafic destiné à toutes les autres adresses IPv4 (par exemple, 0.0.0.0/0)	Sortant (igw-ID)	Le trafic destiné à toutes les autres adresses IPv4 est acheminé vers la passerell e Internet (identifiée par igw-ID) qui a été créée par l'assistant VPC.

5. Dans le panneau de navigation, choisissez Subnets (Sous-réseaux). Sélectionnez ensuite le premier sous-réseau privé que vous avez créé (par exemple, **`WorkSpaces Secure Browser Private Subnet1`**).
6. Dans l'onglet Table de routage, sélectionnez l'ID de la table de routage.
7. Sélectionnez la table de routage. Sous Nom, choisissez l'icône de modification (crayon), puis nommez la table. Par exemple, saisissez le nom **`workspacesweb-private-routetable`**. Sélectionnez ensuite la coche pour enregistrer le nom.
8. Sous l'onglet Routes, vérifiez que la table de routage comprend les routes suivantes :

Destination	Cible	Description
Bloc d'adresses CIDR IPv4 du sous-réseau public (par exemple, 10.0.0/20)	Local	Tout le trafic provenant des ressources destinées aux adresses IPv4 dans le bloc d'adresse CIDR IPv4 du sous-réseau public est acheminé localement au sein du VPC.
Trafic destiné à toutes les autres adresses IPv4 (par exemple, 0.0.0.0/0)	Sortant (nat-ID)	Le trafic destiné à toutes les autres adresses IPv4 est acheminé vers la passerelle NAT (identifiée par nat-ID).
Trafic destiné aux compartiments S3 (applicable si vous avez spécifié un point de terminaison S3) [pl-ID (com.amazonaws.region.s3)]	Stockage (vpce-ID)	Le trafic destiné aux compartiments S3 est acheminé vers le point de terminaison S3 (identifié par vpce-ID).

9. Dans le panneau de navigation, choisissez Subnets (Sous-réseaux). Sélectionnez ensuite le deuxième sous-réseau privé que vous avez créé (par exemple, **`WorkSpaces Secure Browser Private Subnet2`**).
10. Dans l'onglet Table de routage, vérifiez que la table de routage sélectionnée correspond bien à la table de routage privée (par exemple, **`workspacesweb-private-routetable`**). Si ce n'est pas le cas, choisissez Modifier, puis sélectionnez votre table de routage privée.

Activation de la navigation Internet sans restriction (recommandé)

Suivez ces étapes pour configurer un VPC avec une passerelle NAT pour une navigation Internet sans restriction. Cela permet à WorkSpaces Secure Browser d'accéder aux sites Internet publics et aux sites privés hébergés dans ou avec une connexion à votre VPC.

Pour configurer un VPC avec une passerelle NAT pour une navigation Internet sans restriction

Si vous souhaitez que votre portail WorkSpaces Secure Browser ait accès à la fois au contenu Internet public et au contenu VPC privé, procédez comme suit :

> **Note**
>
> Si vous avez déjà configuré un VPC, effectuez les étapes suivantes pour ajouter une passerelle NAT à votre VPC. Si vous devez créer un VPC, consultez Création et configuration d'un VPC.

1. Pour créer votre passerelle NAT, effectuez les étapes décrites dans Créer une passerelle NAT. Vérifiez que cette passerelle NAT dispose d'une connectivité publique et qu'elle se trouve dans un sous-réseau public de votre VPC.
2. Vous devez spécifier au moins deux sous-réseaux privés issus de deux zones de disponibilité différentes. En affectant vos sous-réseaux à des zones de disponibilité différentes, vous avez l'assurance de bénéficier d'une disponibilité et d'une tolérance aux pannes supérieures. Pour plus d'informations sur la création d'un deuxième sous-réseau privé, consultez the section called "Étape 3 : Ajout d'un deuxième sous-réseau privé".

   > **Note**
   >
   > Pour vous assurer que chaque instance de streaming dispose d'un accès à Internet, n'associez pas de sous-réseau public à votre portail WorkSpaces Secure Browser.

3. Mettez à jour la table de routage associée à vos sous-réseaux privés pour diriger le trafic Internet vers la passerelle NAT. Les instances de streaming de vos sous-réseaux privés peuvent ainsi communiquer avec Internet. Pour savoir comment associer une table de routage à un sous-réseau privé, effectuez les étapes décrites dans Configuration des tables de routage.

Activer la navigation Internet restreinte (à l'aide d'un proxy HTTP sortant)

La configuration réseau recommandée d'un portail WorkSpaces Secure Browser consiste à utiliser des sous-réseaux privés dotés d'une passerelle NAT, afin que le portail puisse naviguer à la fois sur Internet public et sur du contenu privé. Pour plus d'informations, consultez the section called "Activation de la navigation Internet sans restriction (recommandé)". Toutefois, il se peut que vous deviez contrôler les communications sortantes d'un portail WorkSpaces Secure Browser vers

Internet à l'aide d'un proxy Web. Par exemple, si vous utilisez un proxy Web comme passerelle vers Internet, vous pouvez mettre en œuvre des contrôles de sécurité préventifs, tels que la liste des domaines autorisés et le filtrage du contenu. Cela permet également de réduire l'utilisation de la bande passante et d'améliorer les performances du réseau en mettant en cache les ressources fréquemment consultées, telles que les pages Web ou les mises à jour logicielles en local. Dans certains cas d'utilisation, il se peut que vous disposiez d'un contenu privé accessible uniquement à l'aide d'un proxy Web.

Vous êtes peut-être déjà familiarisé avec la configuration des paramètres de proxy sur les appareils administrés ou sur l'image de vos environnements virtuels. Mais cela pose des problèmes si vous ne contrôlez pas l'appareil (par exemple, lorsque les utilisateurs utilisent des appareils qui ne sont pas détenus ou gérés par l'entreprise) ou si vous devez gérer l'image de votre environnement virtuel. WorkSpaces Secure Browser vous permet de définir les paramètres du proxy à l'aide des politiques de Chrome intégrées au navigateur Web. Vous pouvez le faire en configurant un proxy sortant HTTP pour WorkSpaces Secure Browser.

Cette solution est basée sur une configuration de proxy VPC sortante recommandée. La solution proxy est basée sur le proxy HTTP open source Squid. Il utilise ensuite les paramètres du navigateur WorkSpaces Secure Browser pour configurer le portail WorkSpaces Secure Browser afin de se connecter au point de terminaison du proxy. Pour plus d'informations, consultez Comment configurer un proxy VPC sortant avec liste blanche de domaines et filtrage de contenu.

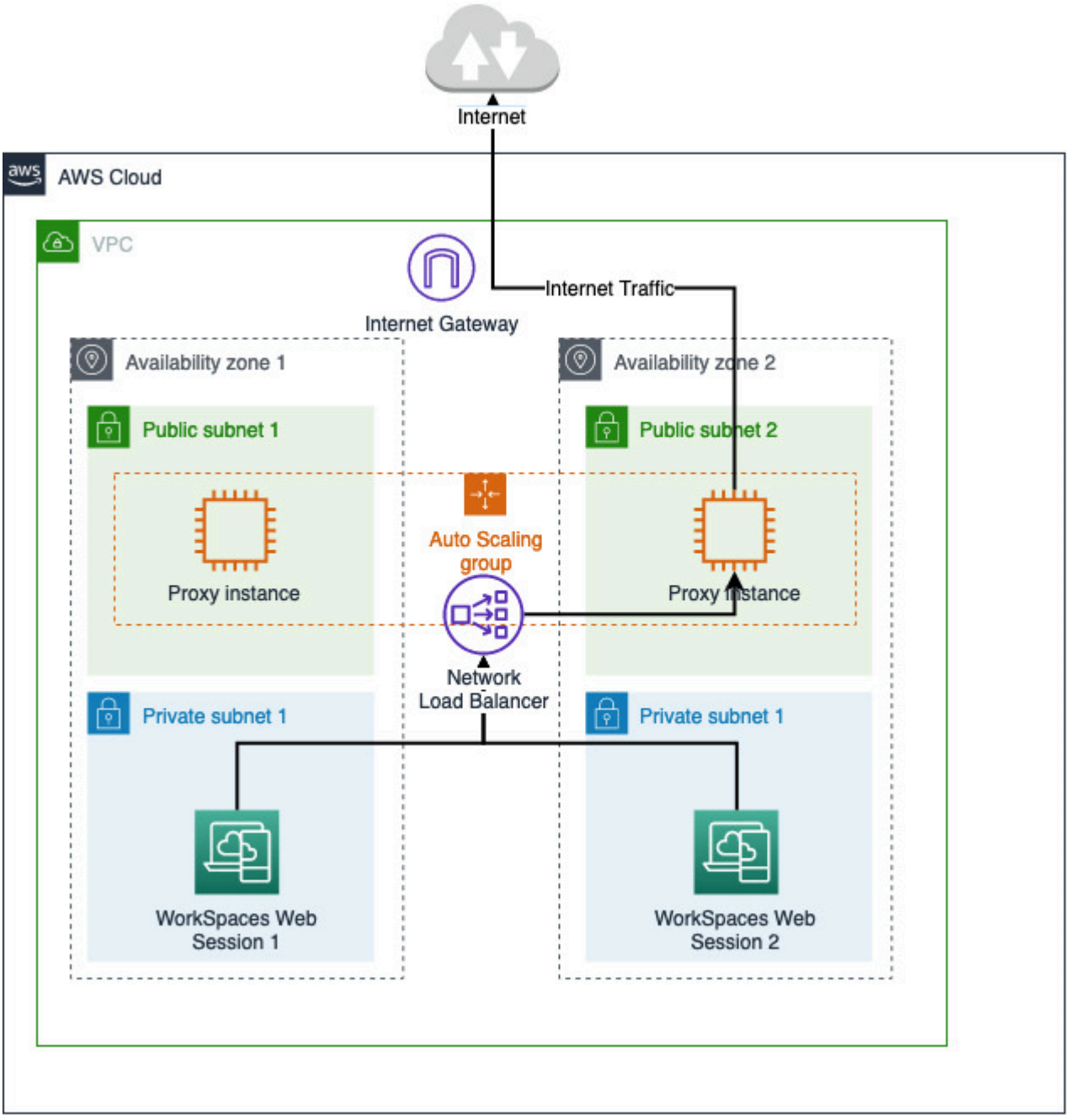
Cette solution vous offre les avantages suivants :

- Un proxy sortant qui inclut un groupe d'instances Amazon EC2 à mise à l'échelle automatique, hébergées par un équilibreur de charge réseau. Les instances de proxy résident dans un sous-réseau public et chacune d'entre elles est associée à une adresse IP élastique, ce qui leur permet d'accéder à Internet.
- Un portail WorkSpaces Secure Browser déployé sur des sous-réseaux privés. Il n'est pas nécessaire de configurer la passerelle NAT pour permettre l'accès à Internet. Au lieu de cela, vous configurez la politique de votre navigateur afin que tout le trafic Internet passe par le proxy sortant. Si vous souhaitez utiliser votre propre proxy, la configuration du portail WorkSpaces Secure Browser sera similaire.

Architecture

Voici un exemple de configuration de proxy typique dans votre VPC. L'instance proxy Amazon EC2 se trouve dans des sous-réseaux publics et est associée à Elastic IP, de sorte qu'elle a

accès à Internet. Un équilibreur de charge réseau héberge un groupe d'instances de proxy à dimensionnement automatique. Cela garantit que les instances de proxy peuvent évoluer automatiquement et que l'équilibreur de charge réseau est le point de terminaison du proxy unique, qui peut être utilisé par les sessions WorkSpaces Secure Browser.



Prérequis

Avant de commencer, assurez-vous de remplir les conditions préalables suivantes :

- Vous avez besoin d'un VPC déjà déployé, avec des sous-réseaux publics et privés répartis sur plusieurs zones de disponibilité (AZ). Pour plus d'informations sur la configuration de votre environnement VPC, consultez la section VPC par défaut.
- Vous avez besoin d'un point de terminaison proxy unique accessible à partir de sous-réseaux privés où résident les sessions WorkSpaces Secure Browser (par exemple, le nom DNS de l'équilibreur de charge réseau). Si vous souhaitez utiliser votre proxy existant, assurez-vous qu'il possède également un point de terminaison unique accessible depuis vos sous-réseaux privés.

Configuration d'un proxy sortant HTTP pour WorkSpaces Secure Browser

Pour configurer un proxy sortant HTTP pour WorkSpaces Secure Browser, procédez comme suit.

1. Pour déployer un exemple de proxy sortant sur votre VPC, suivez les étapes décrites dans Comment configurer un proxy VPC sortant avec liste blanche de domaines et filtrage de contenu.
   a. Suivez les étapes de la section « Installation (configuration unique) » pour déployer le CloudFormation modèle sur votre compte. Assurez-vous de choisir le VPC et les sous-réseaux appropriés comme paramètres de CloudFormation modèle.
   b. Après le déploiement, recherchez les paramètres CloudFormation de sortie OutboundProxyDomain et OutboundProxyPort. Il s'agit du nom et du port DNS de votre proxy.
   c. Si vous possédez déjà votre propre proxy, ignorez cette étape et utilisez le nom et le port DNS de votre proxy.
2. Dans la console WorkSpaces Secure Browser, sélectionnez votre portail, puis choisissez Modifier.
   a. Dans les détails de la connexion réseau, choisissez le VPC et les sous-réseaux privés qui ont accès au proxy.
   b. Dans les paramètres de stratégie, ajoutez la ProxySettings politique suivante à l'aide d'un éditeur JSON. Le `ProxyServer` champ doit être le nom et le port DNS de votre proxy. Pour plus de détails sur ProxySettings la politique, voir ProxySettings.

```
{
    "chromePolicies":
    {
        ...
        "ProxySettings": {
            "value": {
                "ProxyMode": "fixed_servers",
                "ProxyServer": "OutboundProxyLoadBalancer-0a01409a46943c47.elb.us-
west-2.amazonaws.com:3128",
```

```
                "ProxyBypassList": "https://www.example1.com,https://
www.example2.com,https://internalsite/"
            }
        },
    }
}
```

3. Dans votre session WorkSpaces Secure Browser, vous verrez que le proxy est appliqué à Chrome. Chrome utilise les paramètres de proxy de votre administrateur.
4. Accédez à chrome : //policy et à l'onglet Chrome policy pour vérifier que la politique est appliquée.
5. Vérifiez que votre session WorkSpaces Secure Browser peut parcourir correctement le contenu Internet sans passerelle NAT. Dans les CloudWatch journaux, vérifiez que les journaux d'accès au proxy Squid sont enregistrés.

Résolution des problèmes

Une fois les règles de Chrome appliquées, si votre session WorkSpaces Secure Browser ne parvient toujours pas à accéder à Internet, procédez comme suit pour tenter de résoudre le problème :

- Vérifiez que le point de terminaison du proxy est accessible depuis les sous-réseaux privés sur lesquels se trouve votre portail WorkSpaces Secure Browser. Pour ce faire, créez une instance EC2 dans le sous-réseau privé et testez la connexion entre l'instance EC2 privée et votre point de terminaison proxy.
- Vérifiez que le proxy dispose d'un accès à Internet.
- Vérifiez que la politique de Chrome est correcte.
  - Confirmez le formatage suivant pour le `ProxyServer` champ de la politique : `<Proxy DNS name>:<Proxy port>` Il ne doit y avoir aucun `http://` ou `https://` dans le préfixe.
  - Dans la session WorkSpaces Secure Browser, utilisez Chrome pour accéder à chrome : //policy et assurez-vous que la ProxySettings politique est correctement appliquée.

Recommandations concernant la configuration d’un VPC

Les recommandations suivantes peuvent vous aider à configurer votre VPC de façon plus efficace et sécurisée.

Configuration générale du VPC

- Assurez-vous que la configuration de votre VPC peut répondre à vos besoins de mise à l’échelle.

- Assurez-vous que vos quotas de service WorkSpaces Secure Browser (également appelés limites) sont suffisants pour répondre à la demande prévue. Pour demander une augmentation de quota, vous pouvez utiliser la console Service Quotas à l'adresse :https://console.aws.amazon.com/servicequotas/. Pour plus d'informations sur les quotas par défaut de WorkSpaces Secure Browser, consultezthe section called "Gérez les quotas de service pour votre portail".
- Si vous prévoyez de fournir à vos sessions de streaming un accès à Internet, nous vous recommandons de configurer un VPC avec une passerelle NAT dans un sous-réseau public.

Interfaces réseau Elastic

- Chaque session WorkSpaces Secure Browser nécessite sa propre interface Elastic Network pendant la durée du streaming. WorkSpaces Secure Browser crée autant d'interfaces réseau élastiques (ENI) que la capacité maximale souhaitée de votre flotte. Par défaut, la limite pour les interfaces ENI par région est de 5 000. Pour en savoir plus, consultez Interfaces réseau.

  Si vous avez besoin de planifier la capacité pour des déploiements de très grande envergure, par exemple pour plusieurs milliers de sessions de streaming simultanées, réfléchissez au nombre d'interfaces ENI qui pourraient être nécessaires en période de pointe. Nous vous recommandons de maintenir votre limite d'interfaces ENI à un niveau égal ou supérieur à la limite maximale d'utilisation simultanée que vous configurez pour votre portail web.

Sous-réseaux

- Lorsque vous élaborez votre plan pour augmenter le nombre d'utilisateurs, gardez à l'esprit que chaque session WorkSpaces Secure Browser nécessite une adresse IP client unique provenant de vos sous-réseaux configurés. Par conséquent, la taille de l'espace d'adressage IP client configuré sur vos sous-réseaux détermine le nombre d'utilisateurs pouvant diffuser simultanément.
- Nous vous recommandons de configurer chaque sous-réseau avec un masque de sous-réseau qui permet d'avoir un nombre suffisant d'adresses IP client pour prendre en considération le nombre maximal d'utilisateurs simultanés attendu. De plus, prévoyez des adresses IP supplémentaires pour répondre à la demande à venir. Pour plus d'informations, consultez Dimensionnement des VPC et des sous-réseaux pour IPv4.
- Nous vous recommandons de configurer un sous-réseau dans chaque zone de disponibilité unique prise en charge par WorkSpaces Secure Browser dans la région de votre choix pour des raisons de disponibilité et de dimensionnement. Pour plus d'informations, consultez the section called "Création et configuration d'un VPC".

- Vérifiez que les ressources réseau dont vos applications web ont besoin sont accessibles depuis vos sous-réseaux.

Groupes de sécurité

- Utilisez des groupes de sécurité pour fournir un contrôle d'accès supplémentaire à votre VPC.

  Les groupes de sécurité appartenant à votre VPC vous permettent de contrôler le trafic réseau entre les instances de streaming WorkSpaces Secure Browser et les ressources réseau requises par les applications Web. Veillez à ce que les groupes de sécurité donnent accès aux ressources réseau dont vos applications web ont besoin.

Zones de disponibilité prises en charge

Lorsque vous créez un cloud privé virtuel (VPC) à utiliser avec WorkSpaces Secure Browser, les sous-réseaux de votre VPC doivent résider dans différentes zones de disponibilité de la région dans laquelle vous lancez Secure Browser. WorkSpaces Les zones de disponibilité sont des emplacements distincts conçus pour être isolés des défaillances dans d'autres zones de disponibilité. En lançant des instances dans des zones de disponibilité distinctes, vous pouvez protéger vos applications de la défaillance d'un seul emplacement. Chaque sous-réseau doit résider entièrement dans une zone de disponibilité et ne peut pas s'étendre sur plusieurs zones. Pour bénéficier d'une résilience maximale, nous vous recommandons de configurer un sous-réseau pour chaque zone de disponibilité prise en charge de la région souhaitée.

Une zone de disponibilité est représentée par un code de région suivi d'un identifiant à lettre ; par exemple, `us-east-1a`. Pour garantir que les ressources sont réparties entre les zones de disponibilité d'une région, nous mappons indépendamment les zones de disponibilité aux noms de chaque compte AWS . Par exemple, la zone de disponibilité `us-east-1a` pour votre compte AWS peut avoir un emplacement autre que `us-east-1a` pour un autre compte AWS .

Pour coordonner les zones de disponibilité entre les comptes, vous devez utiliser un ID de zone de disponibilité, qui représente l'identifiant unique et cohérent d'une zone de disponibilité. Par exemple, `use1-az2` il s'agit d'un identifiant AZ pour la `us-east-1` région et il a le même emplacement dans tous les AWS comptes.

Le nom des ID de zone de disponibilité vous permet de déterminer l'emplacement des ressources d'un compte par rapport aux ressources d'un autre compte. Par exemple, si vous partagez avec un autre compte un sous-réseau dans la zone de disponibilité portant l'ID `use1-az2`, ce sous-réseau

est accessible par cet autre compte dans la zone de disponibilité portant également l'ID `use1-az2`. L'ID de zone de disponibilité de chaque VPC et de chaque sous-réseau s'affiche dans la console Amazon VPC.

WorkSpaces Secure Browser est disponible dans un sous-ensemble de zones de disponibilité pour chaque région prise en charge. Le tableau suivant répertorie les ID de zone de disponibilité que vous pouvez utiliser pour chaque région. Pour voir le mappage des ID de zone de disponibilité aux zones de disponibilité de votre compte, consultez Identifiants de zone de disponibilité pour vos ressources dans le Guide de l'utilisateur AWS RAM .

Nom de la région	Code région	Identifiants de zone de disponibilité pris en charge
USA Est (Virginie du Nord)	`us-east-1`	`use1-az1`, `use1-az2`, `use1-az4`, `use1-az5`, `use1-az6`
USA Ouest (Oregon)	`us-west-2`	`usw2-az1`, `usw2-az2`, `usw2-az3`
Asie-Pacifique (Mumbai)	`ap-south-1`	`aps1-az1`, `aps1-az3`
Asie-Pacifique (Séoul)	`ap-northeast-2`	`apne2-az1` , `apne2-az2` , `apne2-az3`
Asie-Pacifique (Singapour)	`ap-southeast-1`	`apse1-az1` , `apse1-az2` , `apse1-az3`
Asie-Pacifique (Sydney)	`ap-southeast-2`	`apse2-az1` , `apse2-az2` , `apse2-az3`
Asie-Pacifique (Tokyo)	`ap-northeast-1`	`apne1-az1` , `apne1-az2` , `apne1-az4`
Canada (Centre)	`ca-central-1`	`cac1-az1`, `cac1-az2`, `cac1-az4`
Europe (Francfort)	`eu-central-1`	`euc1-az2`, `euc1-az2`, `euc1-az3`

Nom de la région	Code région	Identifiants de zone de disponibilité pris en charge
Europe (Irlande)	`eu-west-1`	`euw1-az1`, `euw1-az2`, `euw1-az3`
Europe (Londres)	`eu-west-2`	`euw2-az1`, `euw2-az2`

Pour plus d'informations sur les zones de disponibilité et les ID AZ, consultez Régions, zones de disponibilité et zones locales dans le guide de l'utilisateur Amazon EC2.

Connexion VPC

Chaque instance de streaming WorkSpaces Secure Browser possède une interface réseau client qui fournit une connectivité aux ressources de votre VPC, ainsi qu'à Internet si des sous-réseaux privés dotés d'une passerelle NAT sont configurés.

Pour la connectivité Internet, les ports suivants doivent être ouverts à tous les destinations. Si vous utilisez un groupe de sécurité modifié ou personnalisé, vous devez ajouter les règles nécessaires manuellement. Pour en savoir plus, consultez Règles des groupes de sécurité.

> **Note**
>
> Cela s'applique au trafic sortant.

- TCP 80 (HTTP)
- TCP 443 (HTTPS)
- UDP 8433

Connexion client/utilisateur

WorkSpaces Secure Browser est configuré pour acheminer les connexions de streaming sur l'Internet public. La connectivité Internet est nécessaire pour authentifier les utilisateurs et fournir les ressources Web dont WorkSpaces Secure Browser a besoin pour fonctionner. Pour autoriser ce trafic, vous devez autoriser les domaines répertoriés dans Domaines autorisés.

Les rubriques suivantes fournissent des informations sur la manière d'activer les connexions utilisateur à WorkSpaces Secure Browser.

Rubriques

Exigences relatives aux adresses IP et aux ports

Pour accéder aux instances de WorkSpaces Secure Browser, les appareils utilisateur ont besoin d'un accès sortant sur les ports suivants :

- Port 443 (TCP)
  - Le port 443 est utilisé pour les communications HTTPS entre les appareils utilisateur et les instances de streaming lorsque les points de terminaison Internet sont utilisés. En général, lorsque les utilisateurs finaux parcourent le Web au cours de sessions de streaming, le navigateur Web sélectionne de façon aléatoire un port source dans la plage supérieure en vue d'une utilisation pour le trafic de streaming. Vous devez vérifier que le trafic de retour renvoyé vers ce port est autorisé.
  - Ce port doit être ouvert aux domaines requis répertoriés dans Domaines autorisés.
  - AWS publie ses plages d'adresses IP actuelles, y compris les plages vers lesquelles la passerelle de session et CloudFront les domaines peuvent être résolus, au format JSON. Pour savoir comment télécharger le fichier .json et examiner les plages actuelles, consultez Plages d'adresses IP AWS. Ou, si vous utilisez AWS Tools for Windows PowerShell, vous pouvez accéder aux mêmes informations à l'aide de la Get-AWSPublicIpAddressRange PowerShell commande. Pour en savoir plus, consultez Querying the Public IP Address Ranges for AWS.
- (Facultatif) Port 53 (UDP)
  - Le port 53 est utilisé pour les communications entre les appareils utilisateur et vos serveurs DNS.
  - Ce port est facultatif si vous n'utilisez pas de serveurs DNS pour la résolution de noms de domaine.
  - Le port doit être ouvert sur les adresses IP de vos serveurs DNS de manière à permettre la résolution des noms de domaine public.

Domaines autorisés

Pour que les utilisateurs puissent accéder aux portails Web depuis leur navigateur local, vous devez ajouter les domaines suivants à la liste d'autorisation du réseau à partir duquel l'utilisateur tente d'accéder au service.

Dans le tableau suivant, remplacez *{region}* par le code de la région du portail Web en cours d'exploitation. Par exemple, s3. *{region}* .amazonaws.com doit être s3.eu-west-1.amazonaws.com pour un portail Web de la région Europe (Irlande). Pour obtenir la liste des codes de région, consultez la section Points de terminaison et quotas Amazon WorkSpaces Secure Browser.

Catégorie	Domaine ou adresse IP
WorkSpaces Ressources de streaming de Secure Browser	s3.*{region}*.amazonaws.com s3.amazonaws.com appstream2.*{region}*.aws.amazon.com *.amazonappstream.com *.shortbread.aws.dev
WorkSpaces Ressources statiques de Secure Browser	*.workspaces-web.com di5ry4hb4263e.cloudfront.net
WorkSpaces Authentification sécurisée par navigateur	*.auth.*{region}*.amazoncognito.com cognito-identity.*{region}*.amazonaws.com cognito-idp.*{region}*.amazonaws.com *.cloudfront.net
WorkSpaces Mesures et rapports relatifs à Secure Browser	*.execute-api.*{region}*.amazonaws.com unagi-na.amazon.com

Selon le fournisseur d'identité que vous configurez, vous devrez peut-être aussi autoriser d'autres domaines. Consultez la documentation de votre IdP pour identifier les domaines dont vous devez autoriser la liste pour que WorkSpaces Secure Browser puisse utiliser ce fournisseur. Si vous utilisez IAM Identity Center, prenez connaissance des prérequis IAM Identity Center.

Commencer à utiliser WorkSpaces Secure Browser

Suivez ces étapes pour créer un portail Web WorkSpaces Secure Browser et permettre aux utilisateurs d'accéder à des sites Web internes et SaaS à partir de leurs navigateurs existants. Vous pouvez créer un seul portail web par compte dans n'importe quelle région prise en charge.

> **Note**
>
> Pour demander une augmentation de limite pour plusieurs portails, veuillez contacter l'assistance en indiquant votre Compte AWS identifiant, le nombre de portails à demander et Région AWS.

Ce processus prend généralement cinq minutes avec l'assistant de création de portail web, et il faut compter jusqu'à 15 minutes supplémentaires pour que le portail devienne actif.

Il n'y a aucun coût associé à la mise en place d'un portail Web. WorkSpaces Secure Browser propose pay-as-you-go des tarifs, y compris un prix mensuel modique pour les utilisateurs qui utilisent activement le service. Il n'y a ni frais initiaux, ni licences, ni engagements à long terme.

> **Important**
>
> Avant de commencer, vous devez réunir les prérequis pour un portail web. Pour en savoir plus sur les prérequis d'un portail web, consultez Configuration de WorkSpaces Secure Browser.

Rubriques

Étape 1 : Création d'un portail web

Pour créer un portail web, procédez comme suit.

Rubriques

Configurer les paramètres réseau

1. Ouvrez la console WorkSpaces Secure Browser à l'adresse https://console.aws.amazon.com/workspaces-web/home.
2. Choisissez WorkSpaces Secure Browser, Portails Web, puis Créer un portail Web.
3. Sur la page Étape 1 : Spécifier une connexion réseau, effectuez les étapes suivantes pour connecter votre VPC à votre portail web et configurer le VPC et les sous-réseaux.

    1. Pour les informations relatives à la mise en réseau, choisissez un VPC connecté au contenu auquel vous souhaitez que vos utilisateurs accèdent avec WorkSpaces Secure Browser.
    2. Vous pouvez choisir jusqu'à trois sous-réseaux privés qui remplissent les conditions suivantes. Pour plus d'informations, consultez Mise en réseau et accès.
        - Vous devez choisir au moins deux sous-réseaux privés pour créer un portail.
        - Pour que votre portail web bénéficie d'une haute disponibilité, nous vous recommandons de fournir le nombre maximal de sous-réseaux privés dans des zones de disponibilité uniques pour votre VPC.
    3. Sélectionnez un groupe de sécurité.

Configuration des paramètres du portail

Sur la page Étape 2 : Configurer les paramètres du portail web, effectuez les étapes suivantes pour personnaliser l'expérience de navigation de vos utilisateurs lorsqu'ils démarrent une session.

1. Sous Détails du portail web, dans Nom d'affichage, donnez un nom identifiable à votre portail web.

2. Sous Type d'instance, sélectionnez le type d'instance pour votre portail Web dans le menu déroulant. Entrez ensuite votre limite maximale d'utilisateurs simultanés pour le portail Web. Pour plus d'informations, consultez the section called "Gérez les quotas de service pour votre portail".

> **Note**
>
> La sélection d'un nouveau type d'instance modifiera le coût pour chaque utilisateur actif mensuel. Pour plus d'informations, consultez la section Tarification d'Amazon WorkSpaces Secure Browser.

3. Sous Journalisation des accès utilisateur, pour ID de flux Kinesis, sélectionnez le flux de données Amazon Kinesis auquel vous souhaitez envoyer vos données. Pour plus d'informations, consultez the section called "Configuration de la journalisation des accès utilisateur".
4. Sous Paramètres de politiques, procédez comme suit :

   - Pour Options de politiques, sélectionnez Éditeur visuel ou Chargement de fichier JSON. Vous pouvez utiliser l'une ou l'autre de ces méthodes pour fournir les détails de configuration des politiques de votre portail web. Pour plus d'informations, consultez the section called "Définition ou modification de votre politique de navigateur".
     - WorkSpaces Secure Browser inclut la prise en charge des politiques d'entreprise de Chrome. Vous pouvez ajouter et gérer des politiques à l'aide d'un éditeur visuel ou en chargeant manuellement des fichiers de politiques. Vous pouvez passer d'une méthode à l'autre à tout moment.
     - Lorsque vous chargez un fichier de politiques, les politiques disponibles dans le fichier sont visibles dans la console. En revanche, vous ne pouvez pas modifier toutes les politiques dans l'éditeur visuel. Les politiques du fichier JSON que vous ne pouvez pas modifier avec l'éditeur visuel sont répertoriées dans la console sous Politiques JSON supplémentaires. Pour apporter des modifications à ces politiques, vous devez le faire manuellement.
   - (Facultatif) Dans URL de démarrage – facultatif, indiquez le domaine à utiliser comme page d'accueil lorsque les utilisateurs lancent leur navigateur. Votre VPC doit disposer d'une connexion stable à cette URL.
   - Cochez ou décochez Navigation privée et Suppression de l'historique pour activer ou désactiver ces fonctionnalités durant la session d'un utilisateur

> **Note**
>
> Les URL visitées dans le cadre d'une navigation privée, ou avant la suppression de l'historique du navigateur de l'utilisateur, ne peuvent pas être consignées dans la journalisation des accès utilisateur. Pour plus d'informations, consultez the section called "Configuration de la journalisation des accès utilisateur".

- Dans le cadre du filtrage des URL, vous pouvez configurer les URL que les utilisateurs peuvent consulter au cours d'une session. Pour plus d'informations, consultez the section called "Configurer le filtrage des URL".
- (Facultatif) Dans Marque-pages du navigateur – facultatif, saisissez le Nom d'affichage, le Domaine et le Dossier pour les marque-pages (ou « favoris ») que vos utilisateurs doivent pouvoir trouver dans leur navigateur. Sélectionnez ensuite Ajouter un marque-page.

> **Note**
>
> Le champ Domaine est obligatoire pour les marque-pages du navigateur.
> Dans Chrome, les utilisateurs peuvent retrouver les marque-pages gérés dans le dossier Favoris gérés sur la barre d'outils des favoris.

- (Facultatif) Ajoutez des Balises à votre portail. Vous pouvez utiliser des balises pour rechercher ou filtrer vos AWS ressources. Les balises se composent d'une clé et d'une valeur facultative et sont associées à votre ressource de portail.

5. Sous Contrôle d'accès IP (facultatif), indiquez si vous voulez limiter l'accès aux réseaux approuvés. Pour plus d'informations, consultez the section called "Configuration des contrôles d'accès IP (facultatif)".
6. Choisissez Next (Suivant) pour continuer.

Configuration des paramètres utilisateur

Sur la page Étape 3 : Sélectionner les paramètres utilisateur, effectuez les étapes suivantes pour sélectionner les fonctionnalités auxquelles vos utilisateurs doivent pouvoir accéder depuis la barre de navigation du haut durant leur session, puis sélectionnez Suivant :

1. Pour Autorisations utilisateur, choisissez d'activer ou non l'extension pour l'authentification unique. Pour en savoir plus, consultez the section called "Activation d'extension pour l'authentification unique (facultatif)".
2. Pour Autorisations du presse-papiers, choisissez Désactivé ou Activé.
3. Sous Transfert de fichiers, choisissez Désactivé ou Activé.
4. Pour Autoriser les utilisateurs à imprimer sur un appareil local depuis leur portail Web, choisissez Autorisé ou Non autorisé.
5. Pour Autoriser les utilisateurs à créer des liens profonds vers leur portail Web, choisissez Autorisé ou Non autorisé. Pour plus d'informations sur les liens profonds, consultezthe section called "Autoriser les liens profonds (facultatif)".
6. Pour Détails de session utilisateur, spécifiez les paramètres suivants :

   - Pour Disconnect timeout in minutes (Délai avant déconnexion en minutes), choisissez la durée pendant laquelle une session de streaming doit rester active après la déconnexion des utilisateurs. Si les utilisateurs essaient de se reconnecter à la session de streaming après une déconnexion ou une interruption réseau dans cet intervalle de temps, ils sont connectés à leur session précédente. Sinon, ils sont connectés à une nouvelle session avec une nouvelle instance de streaming.

     Si un utilisateur met fin à la session, le délai de déconnexion ne s'applique pas. Au lieu de cela, l'utilisateur est invité à enregistrer les documents ouverts, puis il est immédiatement déconnecté de l'instance de streaming. L'instance que l'utilisateur utilisait est ensuite supprimée.
   - Pour Idle disconnect timeout in minutes (Délai d'inactivité avant déconnexion en minutes), choisissez la durée pendant laquelle les utilisateurs peuvent rester inactifs avant d'être déconnectés de leur session de streaming et avant le début de l'intervalle Disconnect timeout in minutes (Délai avant déconnexion en minutes). Les utilisateurs sont avertis avant d'être déconnectés en raison de leur inactivité. S'ils essaient de se reconnecter à la session de streaming avant que l'intervalle de temps spécifié dans Délai avant déconnexion en minutes se soit écoulé, ils sont connectés à leur session précédente. Sinon, ils sont connectés à une nouvelle session avec une nouvelle instance de streaming. Si vous définissez la valeur sur 0, celle-ci est désactivée. Lorsque cette valeur est désactivée, les utilisateurs ne sont pas déconnectés en raison de leur inactivité.

> **Note**
>
> Les utilisateurs sont considérées comme inactifs lorsqu'ils arrêtent de se servir du clavier ou de la souris lors de leur session de streaming. Les chargements et téléchargements, les entrées audio, les sorties audio, et les modifications de pixels ne sont pas considérés comme une activité de l'utilisateur. Si les utilisateurs continuent d'être inactifs après que l'intervalle de temps défini par Délai d'inactivité avant déconnexion en minutes se soit écoulé, ils sont déconnectés.

Configuration du fournisseur d'identité

Suivez les étapes ci-dessous pour configurer votre fournisseur d'identité (IdP).

Rubriques

Choisissez le type de fournisseur d'identité

WorkSpaces Secure Browser propose deux types d'authentification : Standard et AWS IAM Identity Center. Vous choisissez le type d'authentification à utiliser avec votre portail sur la page Configurer le fournisseur d'identité.

- Pour Standard (option par défaut), fédérez votre fournisseur d'identité SAML 2.0 tiers (tel qu'Okta ou Ping) directement avec votre portail. Pour plus d'informations, consultez the section called "Configuration du type d'authentification standard". Le type standard prend en charge les flux d'authentification initiés par le SP et par l'IDP.
- Pour IAM Identity Center (option avancée), fédérez le IAM Identity Center avec votre portail. Pour utiliser ce type d'authentification, votre centre d'identité IAM et votre portail WorkSpaces Secure Browser doivent tous deux résider dans le même Région AWS emplacement. Pour plus d'informations, consultez the section called "Configuration du type d'authentification IAM Identity Center".

Configuration du type d'authentification standard

Pour Standard (par défaut), fédérez votre fournisseur d'identité SAML 2.0 tiers (tel qu'Okta ou Ping) directement avec votre portail.

Le type d'identité standard peut prendre en charge les flux de connexion service-provider-initiated (initiés par le SP) et identity-provider-initiated (initiés par l'IdP) avec votre IdP conforme à SAML 2.0.

Étape 1 : Commencez à configurer votre fournisseur d'identité sur WorkSpaces Secure Browser

Procédez comme suit pour configurer votre fournisseur d'identité :

1. Sur la page Configurer le fournisseur d’identité de l’assistant de création, sélectionnez Standard.
2. Choisissez Continuer avec un IdP standard.
3. Téléchargez le fichier de métadonnées SP et laissez l'onglet ouvert pour les valeurs de métadonnées individuelles.
   - Si le fichier de métadonnées SP est disponible, choisissez Télécharger le fichier de métadonnées pour télécharger le document de métadonnées du fournisseur de services (SP), puis téléchargez le fichier de métadonnées du fournisseur de services sur votre IdP à l'étape suivante. Sans cela, les utilisateurs ne pourront pas se connecter.
   - Si votre fournisseur ne télécharge pas les fichiers de métadonnées SP, entrez manuellement les valeurs des métadonnées.
4. Sous Choisir le type de connexion SAML, choisissez entre les assertions SAML initiées par le SP et l'IDP, ou les assertions SAML initiées par le SP uniquement.
   - Les assertions SAML initiées par le SP et par l'IdP permettent à votre portail de prendre en charge les deux types de flux de connexion. Les portails qui prennent en charge les flux initiés par l'IdP vous permettent de présenter des assertions SAML au point de terminaison de fédération des identités de service sans obliger les utilisateurs à lancer une session en accédant à l'URL du portail.
     - Choisissez cette option pour autoriser le portail à accepter les assertions SAML non sollicitées initiées par un IdP.
     - Cette option nécessite la configuration d'un état de relais par défaut dans votre fournisseur d'identité SAML 2.0. Le paramètre d'état du relais pour votre portail se trouve dans la console lors de la connexion SAML initiée par l'IdP, ou vous pouvez le copier à partir du fichier de métadonnées SP situé sous. `<md:IdPInitRelayState>`
     - Remarque

- Voici le format de l'état du relais :`redirect_uri=https%3A%2F%2Fportal-id.workspaces-web.com%2Fsso&response_type=code&client_id=1example23456789&identity_provider=Ex Identity-Provider`.
- Si vous copiez et collez la valeur à partir du fichier de métadonnées SP, assurez-vous de passer `&` à`&`. `&`est un caractère d'échappement XML.

- Choisissez les assertions SAML initiées par le SP uniquement pour que le portail ne prenne en charge que les flux de connexion initiés par le SP. Cette option rejettera les assertions SAML non sollicitées provenant des flux de connexion initiés par l'IdP.

> **Note**
>
> Certains tiers vous IdPs permettent de créer une application SAML personnalisée capable de fournir des expériences d'authentification initiées par l'IdP en tirant parti des flux initiés par le SP. Pour voir un exemple, consultez Add an Okta bookmark application.

5. Choisissez si vous souhaitez activer les demandes de signature SAML adressées à ce fournisseur. L'authentification initiée par le SP permet à votre IdP de valider que la demande d'authentification provient du portail, ce qui empêche d'accepter d'autres demandes de tiers.
   a. Téléchargez le certificat de signature et chargez-le sur votre IdP. Le même certificat de signature peut être utilisé pour une déconnexion unique.
   b. Activez la demande signée dans votre IdP. Le nom peut être différent en fonction de l'IdP.

> **Note**
>
> RSA-SHA256 est le seul algorithme de demande et de signature de demande par défaut pris en charge.

6. Choisissez si vous souhaitez activer Exiger des assertions SAML chiffrées. Cela vous permet de chiffrer l'assertion SAML provenant de votre IdP. Cela peut empêcher les données d'être interceptées dans les assertions SAML entre l'IdP et Secure Browser. WorkSpaces

> **Note**
>
> Le certificat de chiffrement n'est pas disponible à cette étape. Il sera créé après le lancement de votre portail. Après avoir lancé le portail, téléchargez le certificat de

chiffrement et chargez-le sur votre IdP. Activez ensuite le chiffrement des assertions dans votre IdP (le nom peut être différent en fonction de l'IdP).

7. Choisissez si vous souhaitez activer la déconnexion unique. La déconnexion unique permet à vos utilisateurs finaux de se déconnecter à la fois de leur IdP WorkSpaces et de leur session Secure Browser en une seule action.
   a. Téléchargez le certificat de signature depuis WorkSpaces Secure Browser et chargez-le sur votre IdP. Il s'agit du même certificat de signature que celui utilisé pour la signature des demandes à l'étape précédente.
   b. L'utilisation de la déconnexion unique vous oblige à configurer une URL de déconnexion unique dans votre fournisseur d'identité SAML 2.0. Vous trouverez l'URL de déconnexion unique de votre portail dans la console sous Détails du fournisseur de services (SP) - Afficher les valeurs de métadonnées individuelles, ou dans le fichier de métadonnées SP sous`<md:SingleLogoutService>`.
   c. Activez la déconnexion unique dans votre IdP. Le nom peut être différent en fonction de l'IdP.

Étape 2 : configurer votre fournisseur d'identité sur votre propre IdP

Ouvrez un nouvel onglet dans votre navigateur. Effectuez ensuite les étapes suivantes auprès de votre IdP :

1. Ajoutez les métadonnées de votre portail à votre IdP SAML.

   Téléchargez le document de métadonnées SP que vous avez téléchargé à l'étape précédente sur votre IdP, ou copiez et collez les valeurs des métadonnées dans les champs appropriés de votre IdP. Certains fournisseurs n'autorisent pas le téléchargement de fichiers.

   Les détails de ce processus peuvent varier d'un fournisseur à l'autre. Consultez la documentation de votre fournisseur the section called “Conseils pour des questions spécifiques IdPs” pour obtenir de l'aide sur la façon d'ajouter les détails du portail à la configuration de votre IdP.
2. Confirmez le NameID de votre assertion SAML.

   Assurez-vous que votre IdP SAML renseigne NameID dans l'assertion SAML avec le champ e-mail de l'utilisateur. Le NameID et l'adresse e-mail de l'utilisateur sont utilisés pour identifier de manière unique votre utilisateur fédéré SAML auprès du portail. Utilisez le format d'identifiant de nom SAML persistant.
3. Facultatif : configurez l'état du relais pour l'authentification initiée par l'IDP.

Si vous avez choisi Accepter les assertions SAML initiées par le SP et par l'IdP à l'étape précédente, suivez les étapes de l'étape 2 pour définir l'état du the section called "Étape 1 : Commencez à configurer votre fournisseur d'identité sur WorkSpaces Secure Browser" relais par défaut pour votre application IdP.

4. Facultatif : configurez la signature des demandes. Si vous avez choisi Signer les demandes SAML à ce fournisseur à l'étape précédente, suivez les étapes de l'étape 3 the section called "Étape 1 : Commencez à configurer votre fournisseur d'identité sur WorkSpaces Secure Browser" pour télécharger le certificat de signature sur votre IdP et activer la signature des demandes. Certains IdPs , comme Okta, peuvent exiger que votre NameID appartienne au type « persistant » pour utiliser la signature des demandes. Assurez-vous de confirmer votre NameID pour votre assertion SAML en suivant les étapes ci-dessus.
5. Facultatif : configurez le chiffrement des assertions. Si vous avez choisi Exiger des assertions SAML chiffrées auprès de ce fournisseur, attendez que la création du portail soit terminée, puis suivez l'étape 4 de la section « Charger les métadonnées » ci-dessous pour télécharger le certificat de chiffrement sur votre IdP et activer le chiffrement des assertions.
6. Facultatif : configurez une déconnexion unique. Si vous avez choisi Single Logout, suivez les étapes de l'étape 5 the section called "Étape 1 : Commencez à configurer votre fournisseur d'identité sur WorkSpaces Secure Browser" pour télécharger le certificat de signature sur votre IdP, renseigner l'URL de déconnexion unique et activer la déconnexion unique.
7. Accordez l'accès à vos utilisateurs dans votre IdP pour utiliser WorkSpaces Secure Browser.
8. Téléchargez un fichier d'échange de métadonnées auprès de votre IdP. Vous téléchargerez ces métadonnées dans WorkSpaces Secure Browser à l'étape suivante.

Étape 3 : Terminez la configuration de votre fournisseur d'identité sur WorkSpaces Secure Browser

Retournez à la console WorkSpaces Secure Browserconsole. Sur la page Configurer le fournisseur d'identité de l'assistant de création, sous Métadonnées de l'IdP, téléchargez un fichier de métadonnées ou entrez une URL de métadonnées depuis votre IdP. Le portail utilise ces métadonnées provenant de votre IdP pour établir la confiance.

1. Pour télécharger un fichier de métadonnées, sous Document de métadonnées IdP, sélectionnez Choisir un fichier. Chargez le fichier de métadonnées au format XML que vous avez téléchargé auprès de votre IdP à l'étape précédente.
2. Pour utiliser une URL de métadonnées, accédez à votre IdP que vous avez configuré à l'étape précédente et obtenez son URL de métadonnées. Revenez à la console WorkSpaces Secure

Browser et, sous URL des métadonnées de l'IdP, entrez l'URL des métadonnées que vous avez obtenue auprès de votre IdP.

3. Lorsque vous avez terminé, cliquez sur Next.
4. Pour les portails sur lesquels vous avez activé l'option Exiger des assertions SAML cryptées auprès de ce fournisseur, vous devez télécharger le certificat de chiffrement depuis la section des détails de l'IdP du portail et le télécharger sur votre IdP. Ensuite, vous pouvez activer l'option ici.

> **Note**
>
> WorkSpaces Secure Browser nécessite que le sujet ou le NameID soit mappé et défini dans l'assertion SAML dans les paramètres de votre IdP. Votre IdP peut créer ces mappages automatiquement. Si ces mappages ne sont pas configurés correctement, vos utilisateurs ne peuvent pas se connecter au portail web et démarrer une session. WorkSpaces Secure Browser nécessite que les affirmations suivantes soient présentes dans la réponse SAML. Vous pouvez trouver <Your SP Entity ID>et consulter les <Your SP ACS URL>informations du fournisseur de services ou le document de métadonnées de votre portail, via la console ou la CLI.
>
> - Une `AudienceRestriction` réclamation dont `Audience` la valeur définit votre ID d'entité SP comme cible de la réponse. Exemple :
>
> ```
> <saml:AudienceRestriction>
>     <saml:Audience><Your SP Entity ID></saml:Audience>
> </saml:AudienceRestriction>
> ```
>
> - Un champ standard `Response` avec une valeur `InResponseTo` de l'ID de demande SAML d'origine. Exemple :
>
> ```
> <samlp:Response ... InResponseTo="<originalSAMLrequestId>">
> ```
>
> - Une `SubjectConfirmationData` réclamation avec `Recipient` la valeur de votre URL SP ACS et une `InResponseTo` valeur correspondant à l'ID de demande SAML d'origine. Exemple :
>
> ```
> <saml:SubjectConfirmation>
>     <saml:SubjectConfirmationData ...
>         Recipient="<Your SP ACS URL>"
>         InResponseTo="<originalSAMLrequestId>"
>         />
> ```

```
</saml:SubjectConfirmation>
```

WorkSpaces Secure Browser valide les paramètres de votre demande et vos assertions SAML. Pour les assertions SAML initiées par l'IdP, les détails de votre demande doivent être formatés en tant que `RelayState` paramètre dans le corps d'une requête HTTP POST. Le corps de la demande doit également contenir votre assertion SAML en tant que `SAMLResponse` paramètre. Ces deux éléments devraient être présents si vous avez suivi l'étape précédente.
Voici un exemple de `POST` corps pour un fournisseur SAML initié par un IDP.

```
SAMLResponse=<Base64-encoded SAML assertion>&RelayState=<RelayState>
```

Conseils pour des questions spécifiques IdPs

Pour vous assurer de configurer correctement la fédération SAML pour votre portail, consultez les liens ci-dessous pour accéder à la documentation couramment utilisée IdPs.

IdP	Configuration de l'application SAML	Gestion des utilisateurs	Authentification initiée par l'IDP	Signature de la demande	Cryptage des assertions	Déconnexion unique
Okta	Créez des intégrations d'applications SAML	Gestion des utilisateurs	Référence de champ SAML de l'assistant d'intégration des applications	Référence de champ SAML de l'assistant d'intégration des applications	Référence de champ SAML de l'assistant d'intégration des applications	Référence de champ SAML de l'assistant d'intégration des applications
Entrer	Créez votre propre application	Démarrage rapide : créer et attribuer un compte utilisateur	Activer l'authentification unique pour une application	Vérification de la signature des demandes SAML	Configurer le chiffrement par jeton SAML	Protocole SAML de connexion unique

IdP	Configuration de l'application SAML	Gestion des utilisateurs	Authentification initiée par l'IDP	Signature de la demande	Cryptage des assertions	Déconnexion unique
			d'entreprise		Microsoft Entra	
Ping	Ajouter une application SAML	Utilisateurs	Activation du SSO initié par l'IdP	Configuration de la connexion aux demandes d'authentification PingOne pour Enterprise	Est-ce que PingOne for Enterprise prend en charge le chiffrement ?	Déconnexion unique SAML 2.0
Un seul identifiant	Connecteur personnalisé SAML (avancé) (4266907)	Ajouter des utilisateurs OneLogin manuellement	Connecteur personnalisé SAML (avancé) (4266907)	Connecteur personnalisé SAML (avancé) (4266907)	Connecteur personnalisé SAML (avancé) (4266907)	Connecteur personnalisé SAML (avancé) (4266907)
IAM Identity Center	Configurez votre propre application SAML 2.0	Configurez votre propre application SAML 2.0	Configurez votre propre application SAML 2.0	N/A	N/A	N/A

Configuration du type d'authentification IAM Identity Center

Pour le type IAM Identity Center (avancé), vous fédérez IAM Identity Center avec votre portail. Sélectionnez cette option uniquement si les conditions suivantes s'appliquent à vous :

- Votre centre d'identité IAM est configuré de la même manière Compte AWS Région AWS que votre portail Web.

- Si vous utilisez AWS Organizations, vous utilisez un compte de gestion.

Avant de créer un portail Web avec le type d'authentification IAM Identity Center, vous devez configurer IAM Identity Center en tant que fournisseur autonome. Pour plus d'informations, voir Commencer à exécuter les tâches courantes dans IAM Identity Center. Vous pouvez également connecter votre IdP SAML 2.0 à IAM Identity Center. Pour plus d'informations, voir Se connecter à un fournisseur d'identité externe. À défaut, vous n'aurez aucun utilisateur ou groupe à affecter à votre portail web.

Si vous utilisez déjà IAM Identity Center, vous pouvez choisir IAM Identity Center comme type de fournisseur et suivre les étapes ci-dessous pour ajouter, afficher ou supprimer des utilisateurs ou des groupes de votre portail Web.

> **Note**
>
> Pour utiliser ce type d'authentification, votre centre d'identité IAM doit se trouver dans le même emplacement Compte AWS Région AWS que votre portail WorkSpaces Secure Browser. Si votre centre d'identité IAM se trouve dans un autre Compte AWS ou Région AWS, suivez les instructions relatives au type d'authentification standard. Pour plus d'informations, consultez the section called "Configuration du type d'authentification standard".
>
> Si vous utilisez AWS Organizations, vous ne pouvez créer des portails WorkSpaces Secure Browser intégrés à IAM Identity Center qu'à l'aide d'un compte de gestion.

Pour créer un portail web avec IAM Identity Center

1. Lors de la création du portail, à l'étape 4 : Configurer le fournisseur d'identité, choisissez AWS IAM Identity Center.
2. Choisissez Continuer avec IAM Identity Center.
3. Sur la page Attribuer des utilisateurs et des groupes, choisissez l'onglet Utilisateurs et/ou groupes.
4. Cochez la case à côté du ou des utilisateurs ou groupes que vous souhaitez ajouter au portail.
5. Après avoir créé votre portail, les utilisateurs que vous avez associés peuvent se connecter à WorkSpaces Secure Browser à l'aide de leur nom d'utilisateur et de leur mot de passe IAM Identity Center.

Pour gérer votre portail web avec IAM Identity Center

1. Une fois que vous avez créé votre portail, il est répertorié dans la console IAM Identity Center en tant qu'application configurée.
2. Pour accéder à la configuration de cette application, sélectionnez Applications dans la barre latérale et recherchez une application configurée dont le nom correspond au nom d'affichage de votre portail web.

> **Note**
>
> Si vous n'avez pas saisi de nom d'affichage, le GUID de votre portail est présenté à la place. Le GUID est l'ID qui est ajouté sous forme de préfixe à l'URL du point de terminaison de votre portail web.

Pour ajouter des utilisateurs et des groupes supplémentaires à un portail web existant

1. Ouvrez la console WorkSpaces Secure Browser à l'adressehttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Choisissez WorkSpaces Secure Browser, Portails Web, choisissez votre portail Web, puis sélectionnez Modifier.
3. Sélectionnez Paramètres du fournisseur d'identité et Attribuer des utilisateurs et des groupes supplémentaires. De là, vous pouvez ajouter des utilisateurs et des groupes à votre portail web.

> **Note**
>
> Vous ne pouvez pas ajouter d'utilisateurs ou de groupes depuis la console IAM Identity Center. Vous devez le faire à partir de la page d'édition de votre portail WorkSpaces Secure Browser.

Pour afficher ou supprimer des utilisateurs et des groupes pour votre portail Web

- Vous pouvez afficher ou supprimer l'accès des utilisateurs à cette application en utilisant les actions disponibles dans le tableau Utilisateurs assignés. Pour plus d'informations, consultez la section Gérer l'accès aux applications.

> **Note**
>
> Vous ne pouvez pas afficher ou supprimer des utilisateurs et des groupes depuis la page d'édition du portail WorkSpaces Secure Browserportal. Vous devez le faire à partir de la page de modification de votre console IAM Identity Center.

Modifier le type de fournisseur d'identité

Procédez comme suit pour modifier le type d'authentification de votre portail à tout moment :

- Pour passer d'IAM Identity Center à Standard, suivez les étapes décrites dansthe section called "Configuration du type d'authentification standard".
- Pour passer de Standard à IAM Identity Center, suivez les étapes décrites dansthe section called "Configuration du type d'authentification IAM Identity Center".

Les modifications apportées au type de fournisseur d'identité peuvent prendre jusqu'à 15 minutes pour être déployées et ne mettront pas automatiquement fin aux sessions en cours.

Vous pouvez consulter les modifications de type de fournisseur d'identité apportées à votre portail AWS CloudTrail en inspectant les `UpdatePortal` événements. Le type est visible dans les charges utiles de demande et de réponse de l'événement.

Vérification et lancement

1. Sur la page Étape 5 : Vérifier et lancer, passez en revue les paramètres que vous avez sélectionnés pour votre portail web. Vous pouvez sélectionner Modifier pour modifier les paramètres dans une section donnée. Vous pouvez également modifier ces paramètres ultérieurement dans l'onglet Portails web de la console.
2. Lorsque vous avez terminé, sélectionnez Lancer le portail web.
3. Pour voir le statut de votre portail web, choisissez Portails Web, sélectionnez votre portail, puis choisissez Afficher les détails.

   Un portail web peut avoir l'un des statuts suivants :

   - Incomplet – Les paramètres de fournisseur d'identité obligatoires sont manquants dans la configuration du portail web.

- En attente – Le portail web est en train d'appliquer des modifications à ses paramètres.
- Actif – Le portail web est prêt et peut être utilisé.

4. Patientez au maximum 15 minutes avant que votre portail devienne Actif.

Étape 2 : Test de votre portail web

Après avoir créé un portail Web, vous pouvez vous connecter au point de terminaison WorkSpaces Secure Browser pour parcourir vos sites Web connectés comme le ferait un utilisateur final.

Si vous avez déjà effectué ces étapes dans the section called "Configuration du fournisseur d'identité", vous pouvez ignorer cette section et passer à l'Étape 3 : Partage de votre portail web.

1. Ouvrez la console WorkSpaces Secure Browser à l'adresse https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Choisissez WorkSpaces Secure Browser, Portails Web, choisissez votre portail Web, puis sélectionnez Afficher les détails
3. Sous Point de terminaison du portail web, accédez à l'URL spécifiée pour votre portail. Le point de terminaison du portail web est le point d'accès à partir duquel vos utilisateurs lanceront votre portail web après s'être connectés avec le fournisseur d'identité configuré pour le portail. Il est accessible au public sur Internet et peut être intégré à votre réseau.
4. Sur la page de connexion à WorkSpaces Secure Browser, choisissez Se connecter, SAML, puis entrez vos informations d'identification SAML.
5. Lorsque la page Votre session est en cours de préparation s'affiche, votre session WorkSpaces Secure Browser est lancée. Veillez à ne pas fermer ou quitter cette page.
6. Le navigateur web se lance en présentant votre URL de démarrage ainsi que tout autre comportement supplémentaire configuré via vos paramètres de politique de navigateur.
7. Vous pouvez désormais accéder aux sites web connectés en choisissant des liens ou en saisissant les URL dans la barre d'adresse.

Étape 3 : Partage de votre portail web

Lorsque vous êtes prêt à ce que vos utilisateurs commencent à utiliser WorkSpaces Secure Browser, vous pouvez choisir l'une des options suivantes pour distribuer le portail :

- Ajoutez votre portail à votre passerelle d'applications SAML pour permettre aux utilisateurs de lancer une session directement depuis leur IdP. Vous pouvez le faire via le flux de connexion initié par l'IdP avec votre IdP compatible SAML 2.0. Pour plus d'informations, consultez la section Assertions SAML initiées par le SP et l'IdP dans. the section called "Configuration du type d'authentification standard" Vous pouvez également créer une application SAML personnalisée capable de fournir des expériences d'authentification initiées par l'IdP en utilisant des flux initiés par le SP. Pour plus d'informations, consultez la section Création d'une application Bookmark.
- Ajoutez l'URL du portail à un site web dont vous êtes propriétaire, et utilisez une redirection de navigateur pour diriger les utilisateurs vers le portail web.
- Envoyez l'URL du portail à vos utilisateurs par e-mail ou incorporez-la à un appareil que vous gérez en tant que page d'accueil ou marque-page (ou « favori ») du navigateur.

Étapes suivantes

Après avoir créé votre premier portail web, vous pouvez à tout moment consulter les détails, les modifier ou supprimer le portail web. Pour plus d'informations, consultez Gestion de votre portail web.

Compte AWS Vous pouvez créer un portail Web dans chaque Région AWS endroit où WorkSpaces Secure Browser est disponible. Chaque portail web peut gérer jusqu'à 25 connexions utilisateur à n'importe quel moment. Pour augmenter le nombre de portails que vous pouvez créer dans une région, ou pour permettre à un portail de prendre en charge un plus grand nombre de sessions simultanées, consultez the section called "Gérez les quotas de service pour votre portail".

Gestion de votre portail web

Après avoir configuré votre portail web, vous pouvez en afficher les détails ou les modifier, vous pouvez même supprimer le portail s'il n'a plus d'utilité.

Rubriques

Affichage des détails d'un portail web

Pour afficher les détails d'un portail web

1. Ouvrez la console WorkSpaces Secure Browser à l'adressehttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Choisissez WorkSpaces Secure Browser, Portails Web, choisissez votre portail Web, puis sélectionnez Afficher les détails.

Modification d'un portail web

Pour modifier un portail web

1. Ouvrez la console WorkSpaces Secure Browser à l'adressehttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Choisissez WorkSpaces Secure Browser, Portails Web, choisissez votre portail Web, puis sélectionnez Modifier.

> **Note**
>
> Les modifications apportées aux paramètres réseau ou aux paramètres de délai mettent immédiatement fin à toutes les sessions actives du portail. Les utilisateurs sont déconnectés et doivent se reconnecter pour commencer une nouvelle session. Les modifications apportées aux paramètres Autorisations du presse-papiers, Autorisations de transfert de fichiers ou Imprimer sur l'appareil local s'appliquent à la prochaine nouvelle session. Les sessions actives ne sont pas déconnectées. Les utilisateurs connectés à des sessions actives ne sont pas affectés par les modifications tant qu'ils ne se déconnectent pas et ne se connectent pas à une nouvelle session.

Suppression d'un portail web

Pour supprimer un portail web

1. Ouvrez la console WorkSpaces Secure Browser à l'adressehttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Choisissez WorkSpaces Secure Browser, Portails Web, choisissez votre portail Web, puis sélectionnez Supprimer.

Gérez les quotas de service pour votre portail

Lorsque vous créez votre Compte AWS, nous définissons automatiquement des quotas de service par défaut (également appelés limites) pour l'utilisation des ressources avec AWS services. Les administrateurs doivent être conscients de deux quotas qui devront peut-être être augmentés pour répondre à leur cas d'utilisation. Ces deux quotas correspondent au nombre de portails Web que vous pouvez créer dans chaque région et au nombre maximal de sessions simultanées que vous pouvez prendre en charge avec chaque type d'instance disponible dans chaque région. Vous pouvez demander une augmentation de ces quotas depuis la page Service Quotas de la AWS console.

Le tableau suivant répertorie les limites de quotas de service par défaut.

Quotas par défaut au sein et Région AWS par compte	Valeur
Portails web	3
Nombre maximum de sessions simultanées - standard.regular	25
Nombre maximum de sessions simultanées : standard.large	10
Nombre maximal de sessions simultanées - standard.xlarge	5

> **Important**
>
> Les quotas de service s' Région AWS appliquent un par un. Vous devez demander une augmentation du quota de service dans chaque Région AWS cas où vous avez besoin de plus de ressources. Pour plus d'informations, consultez les points de terminaison et les quotas Amazon WorkSpaces Secure Browser.

Pour demander une augmentation de quota de service

1. Ouvrez le tableau de bord AWS Support.
2. Sélectionnez Augmentation des limites de service.

   > **Important**
   >
   > WorkSpaces Les quotas du service Secure Browser s'appliquent à une région à la fois. Vous devez demander une augmentation de quota de service dans chaque région AWS où vous avez besoin de ressources supplémentaires. Pour de plus amples informations, veuillez consulter Points de terminaison de service AWS.

3. Sous Description du cas d'utilisation, fournissez les informations suivantes :

- Si votre demande d'augmentation porte sur le nombre de portails web, spécifiez ce type de ressource et indiquez l'ID de votre compte AWS, la région pour laquelle vous souhaitez l'augmentation et la valeur de la nouvelle limite.
- Si votre demande d'augmentation concerne le nombre maximal de sessions simultanées, spécifiez ce type de ressource et indiquez l'ID de votre compte AWS, la région pour laquelle vous souhaitez l'augmentation, l'ARN du portail web et la valeur de la nouvelle limite.

4. (Facultatif) Pour demander plusieurs augmentations de quota de service à la fois, complétez une demande d'augmentation de quota dans la section Demandes, puis choisissez Ajouter une autre demande.

Demander une extension du portail

Un portail est la ressource fondamentale du service. Chaque portail est une association entre votre fournisseur d'identité SAML 2.0 et votre connexion réseau à Internet et à tout contenu Web privé. Chaque portail peut avoir une politique de navigateur de portail et des paramètres utilisateur distincts, de sorte que les administrateurs créent généralement plusieurs portails dans la même région pour répondre à différents cas d'utilisation. Par exemple, vous pouvez donner au groupe A l'accès à un site Web spécifique avec des politiques restrictives (par exemple, le presse-papiers et le transfert de fichiers désactivés), et au groupe B l'accès à Internet en général sans filtrage d'URL. Vous pouvez créer un portail dans n'importe quel portail pris en charge Région AWS. Pour connaître la disponibilité actuelle des services, consultez la section Services AWS par région.

Pour demander une augmentation de quota de service

1. Ouvrez la page Service Quotas dans la région de votre choix.
2. Choisissez le nombre de portails Web.
3. Choisissez Demander une augmentation au niveau du compte.
4. Sous Augmenter la valeur du quota, entrez le montant total que vous souhaitez attribuer au quota.

Demander une augmentation du nombre maximum de sessions simultanées

Le quota maximal de sessions simultanées est le plus grand nombre d'utilisateurs pouvant être connectés simultanément à un portail. Si la limite de quota de service pour le nombre maximal de

sessions simultanées n'est pas définie de manière appropriée, les utilisateurs peuvent constater qu'une session n'est pas disponible lorsqu'ils se connectent. Outre l'augmentation de ce quota de service, les clients doivent également s'assurer que leur VPC et leurs sous-réseaux disposent d'un espace IP suffisant pour prendre en charge le maximum de sessions simultanées.

Pour demander une augmentation maximale du nombre maximal de sessions simultanées

1. Ouvrez la page Service Quotas dans la région de votre choix.
2. Choisissez le nombre maximal de sessions simultanées par portail pour le type d'instance que vous souhaitez augmenter.
3. Choisissez Demander une augmentation au niveau du compte.
4. Sous Augmenter la valeur du quota, entrez le montant total que vous souhaitez attribuer au quota.

> **Note**
>
> Pour les augmentations importantes ou urgentes, rendez-vous sur la page d'historique de vos Services Quotas, sélectionnez le lien dans la colonne de statut de votre demande, le lien vers votre dossier d'assistance et ajoutez une réponse avec des détails sur votre cas d'utilisation et/ou l'urgence. Ces informations aident l'équipe du service à hiérarchiser les demandes et à s'assurer qu'une capacité suffisante est allouée à votre compte.

Exemple de limite

Supposons, par exemple, qu'un administrateur configure deux portails Web dans l'est des États-Unis (Virginie du Nord) pour 125 utilisateurs au total. Avant de créer le portail Web, l'administrateur identifie le premier portail Web (portail A) qui prendra en charge 100 utilisateurs. Lors du test du flux de travail pour ces utilisateurs, l'administrateur détermine qu'ils auront besoin du type d'instance XL pour prendre en charge le streaming audio et vidéo pendant la session. Le deuxième portail Web (portail B) doit être accessible à un maximum de 25 utilisateurs afin de permettre l'accès à une seule page Web statique hébergée dans le VPC du client. Lors du test de ce cas d'utilisation, l'administrateur détermine que le type d'instance standard peut prendre en charge ce cas d'utilisation.

Pour le portail A, l'administrateur doit soumettre une demande d'augmentation du quota de service afin de faire passer la limite des instances XL de la valeur par défaut de la région (c'est-à-dire 5) à

100. Une fois rempli, l'administrateur peut allouer la capacité en modifiant le portail Web. Pour le portail B, l'administrateur peut avancer sans demander d'augmentation de quota (c'est-à-dire, étant donné que la région a un quota par défaut de 25 pour le type d'instance standard).

Gérer les quotas de service

Pour consulter à tout moment les quotas de service alloués à votre compte pour chaque région, consultez la page Quotas de service.

Autres quotas de service

Vous pouvez consulter et demander des augmentations pour les autres quotas répertoriés sur la page Quotas de Service. Dans la pratique, la plupart des clients trouveront inutile de demander des augmentations pour ces limites. Ces quotas sont généralement regroupés en deux types : nombre et taux.

Pour les quotas numériques, lorsque vous soumettez une augmentation de quota de service pour le nombre de portails Web, vous recevez automatiquement une augmentation du nombre de sous-ressources nécessaires pour créer un portail unique. Cela sera reflété sur la page Service Quotas. Par exemple, si vous demandez une augmentation du nombre de portails de 3 à 5, vous recevrez automatiquement une augmentation du quota de service de 3 à 5 pour les paramètres du navigateur et de l'utilisateur. Vous avez la possibilité de réutiliser ou de créer de nouvelles sous-ressources comme vous le souhaitez.

En de rares occasions, les clients peuvent trouver un cas d'utilisation pour augmenter le nombre ou le taux d'autres quotas de ressources. Par exemple, les administrateurs peuvent souhaiter augmenter le nombre de paramètres du navigateur pour tester des configurations de portail supplémentaires. Ces demandes de quotas de service seront examinées et satisfaites sur une case-by-case base régulière.

Pour les quotas tarifaires, il n'est pas nécessaire d'ajuster les limites de taux indiquées dans Service Quotas, quelle que soit la limite du portail du compte.

Contrôle de l'intervalle de réauthentification d'un jeton d'IdP SAML

Lorsqu'un utilisateur visite un portail WorkSpaces Secure Browser, il peut se connecter pour lancer une session de streaming. Toutes les sessions commencent sur la page d'accueil, sauf si l'utilisateur s'est connecté moins de 5 minutes auparavant. Le portail vérifie la présence de jetons de fournisseur d'identité (IdP) pour déterminer s'il convient de demander à l'utilisateur de fournir des

informations d'identification au lancement de la session. Un utilisateur qui ne possède pas de jeton d'IdP valide doit saisir un nom d'utilisateur, un mot de passe et (éventuellement) une authentification multifactorielle (MFA) pour lancer une session de streaming. Si l'utilisateur a déjà généré un jeton d'IdP SAML en s'étant connecté à son IdP ou à une application protégée par ce même IdP, les informations d'identification de connexion ne lui sont pas demandées.

Si un utilisateur possède un jeton IdP SAML valide, il peut WorkSpaces accéder à Secure Browser. Vous pouvez contrôler l'intervalle de réauthentification requis pour un jeton d'IdP SAML.

Pour contrôler l'intervalle de réauthentification d'un jeton d'IdP SAML

1. Définissez le délai d'expiration du jeton d'IdP SAML auprès du fournisseur d'identité lui-même. Nous vous recommandons de configurer le délai d'expiration de votre jeton d'IdP de sorte qu'il corresponde à la durée minimale nécessaire pour permettre à un utilisateur d'effectuer ses tâches.

   - Pour en savoir plus sur Okta, consultez Enforce a limited session lifetime for all policies.
   - Pour en savoir plus sur Azure AD, consultez Configuration des contrôles de la session d'authentification.
   - Pour en savoir plus sur Ping, consultez Sessions.
   - Pour plus d'informations à ce sujet AWS IAM Identity Center, consultez la section Définir la durée de session.
2. Définissez les valeurs d'inactivité et de délai d'inactivité de votre portail WorkSpaces Secure Browser. Ces valeurs contrôlent le temps écoulé entre la dernière interaction d'un utilisateur et la fin d'une session WorkSpaces Secure Browser pour cause d'inactivité. Quand une session prend fin, l'utilisateur perd l'état de sa session (notamment les onglets ouverts, le contenu web non enregistré et l'historique) et retrouve un nouvel état au début de la prochaine session. Pour plus d'informations, consultez l'étape 5 de la rubrique the section called "Étape 1 : Création d'un portail web".

   > **Note**
   >
   > Si la session d'un utilisateur expire mais que celui-ci dispose toujours d'un jeton IDP SAML valide, il n'est pas obligé de saisir son nom d'utilisateur et son mot de passe pour démarrer une WorkSpaces nouvelle session Secure Browser. Pour contrôler la manière dont les jetons sont réauthentifiés, suivez les instructions de l'étape précédente.

Configuration de la journalisation des accès utilisateur

Vous pouvez configurer la journalisation des accès utilisateur pour enregistrer les événements utilisateur suivants :

- Début de session : marque le début d'une session WorkSpaces Secure Browser.
- Fin de session : marque la fin d'une session WorkSpaces Secure Browser.
- Navigation par URL – Journalise l'URL chargée par l'utilisateur.

> **Note**
>
> Les journaux de navigation par URL sont enregistrés à partir de l'historique du navigateur. Les URL qui ne sont pas enregistrées dans l'historique du navigateur (en raison d'un accès en mode navigation privée ou d'une suppression de l'historique du navigateur) ne sont pas enregistrées dans les journaux. Il appartient aux clients de déterminer s'ils souhaitent désactiver le mode navigation privée ou la suppression de l'historique avec leur politique de navigateur.

Par ailleurs, les informations incluses pour chaque événement sont les suivantes :

- Heure de l'événement
- Nom d'utilisateur
- ARN du portail web

Les clients sont tenus de comprendre les problèmes juridiques potentiels liés à leur utilisation de WorkSpaces Secure Browser et de s'assurer que leur utilisation de WorkSpaces Secure Browser est conforme à toutes les lois et réglementations applicables. Il s'agit notamment des lois qui réglementent la capacité d'un employeur à surveiller l'utilisation de WorkSpaces Secure Browser par un employé, y compris les activités effectuées au sein de l'application.

L'activation des journaux d'accès des utilisateurs sur votre portail WorkSpaces Secure Browser peut entraîner des frais pour Amazon Kinesis Data Streams. Pour en savoir plus sur la tarification, consultez Tarification d'Amazon Kinesis Data Streams.

Pour activer la journalisation des accès utilisateur dans la console WorkSpaces Secure Browser, sous Journalisation des accès utilisateurs, sélectionnez le Kinesis Stream ID que vous souhaitez utiliser pour recevoir des données. Les données enregistrées seront transmises directement à ce flux.

Pour en savoir plus sur la création d'un flux de donnes Amazon Kinesis, consultez What is Amazon Kinesis Data Streams?.

> **Note**
>
> Pour recevoir les journaux de WorkSpaces Secure Browser, vous devez disposer d'un flux de données Amazon Kinesis commençant par « amazon-workspaces-web -* ». Le chiffrement côté serveur de votre flux de données Amazon Kinesis doit être désactivé ou doit être utilisé Clés gérées par AWS pour le chiffrement côté serveur.
> Pour en savoir plus sur la configuration du chiffrement côté serveur dans Amazon Kinesis, consultez How Do I Get Started with Server-Side Encryption?.

Exemples de journaux

Vous trouverez ci-dessous un exemple de chaque événement disponible, y compris Validation StartSession, VisitPage, et EndSession.

Les champs suivants sont toujours inclus pour chaque événement :

- timestamp est inclus sous forme d'heure epoch en millisecondes.
- eventType est inclus sous forme de chaîne.
- details est inclus sous forme d'objet json distinct.
- portalArn et userName sont inclus pour tous les événements hormis Validation.

```
{
  "timestamp": "1665430373875",
  "eventType": "Validation",
  "details": {
    "permission": "Kinesis:PutRecord",
    "userArn": "userArn",
    "operation": "AssociateUserAccessLoggingSettings",
    "userAccessLoggingSettingsArn": "userAccessLoggingSettingsArn"
  }
}
```

```
{
  "timestamp": "1665179071723",
  "eventType": "StartSession",
  "details": {},
  "portalArn": "portalArn",
  "userName": "userName"
}

{
  "timestamp": "1665179084578",
  "eventType": "VisitPage",
  "details": {
    "title": "Amazon",
    "url": "https://www.amazon.com/"
  },
  "portalArn": "portalArn",
  "userName": "userName"
}

{
  "timestamp": "1665179155953",
  "eventType": "EndSession",
  "details": {},
  "portalArn": "portalArn",
  "userName": "userName"
}
```


Définition ou modification de votre politique de navigateur

WorkSpaces Secure Browser vous permet de définir une politique de navigation personnalisée à l'aide des politiques Chrome disponibles pour la dernière version stable. Il existe plus de 300 régles applicables à un portail web. Pour en savoir plus, consultez the section called "Définition d'une politique de navigateur personnalisée (exemple)" et Liste des règles Chrome Enterprise.

En créant un portail web depuis la vue de la console, vous pouvez appliquer les politiques suivantes :

- `StartURL`
- Favoris et dossiers de favoris
- Activation et désactivation de la navigation privée
- Suppression d'historique

- Filtrage d'URL avec `AllowURL` et `BlockURL`

Pour en savoir plus sur l'utilisation des politiques de la vue de la console, consultez Commencer à utiliser WorkSpaces Secure Browser.

WorkSpaces Secure Browser applique une configuration de politique de navigateur de base à tous les portails, ainsi qu'à toutes les politiques que vous spécifiez. Vous pouvez modifier certaines de ces politiques à l'aide de votre fichier JSON personnalisé. Pour plus d'informations, consultez the section called "Modification de la politique de navigateur de référence".

Rubriques

- Définition d'une politique de navigateur personnalisée (exemple)
- Modification de la politique de navigateur de référence

Définition d'une politique de navigateur personnalisée (exemple)

Vous pouvez définir n'importe quelle politique (ou « règle ») Chrome prise en charge pour Linux en chargeant un fichier JSON. Pour en savoir plus sur les règles Chrome, consultez Liste des règles Chrome Enterprise et sélectionnez la plateforme Linux. Ensuite, recherchez et examinez les règles pour la version stable la plus récente.

Dans l'exemple suivant, vous allez créer un portail web avec les contrôles de politique suivants :

- Configurer des favoris
- Configurer des pages de démarrage par défaut
- Empêcher l'utilisateur d'installer d'autres extensions
- Empêcher l'utilisateur de supprimer l'historique
- Empêcher l'utilisateur d'accéder au mode navigation privée
- Préinstaller l'extension plug-in Okta pour toutes les sessions.

Rubriques

- Étape 1 : Création d'un portail web
- Étape 2 : Regroupement des règles
- Étape 3 : Création d'un fichier de politiques JSON personnalisé
- Étape 4 : Ajout de vos politiques au modèle

- Étape 5 : Chargement de votre fichier JSON de politiques sur votre portail web

Étape 1 : Création d'un portail web

Pour télécharger votre fichier JSON de politique Chrome, vous devez créer un portail WorkSpaces Secure Browser. Pour plus d'informations, consultez the section called "Étape 1 : Création d'un portail web".

Étape 2 : Regroupement des règles

Recherchez et localisez les règles qui vous intéressent dans Chrome Policy. Vous utiliserez ensuite ces règles pour créer un fichier JSON à l'étape suivante.

1. Accédez à la Liste des règles Chrome Enterprise.
2. Choisissez la plateforme Linux, puis sélectionnez la version la plus récente de Chrome.
3. Recherchez les règles que vous souhaitez définir. Pour cet exemple, faites une recherche sur extensions pour trouver des règles permettant de les gérer. Chaque règle comporte une description, un nom de préférence Linux et un exemple de valeur.
4. D'après les résultats de la recherche, 3 règles répondent aux exigences de l'entreprise si elles sont utilisées ensemble :
   - ExtensionSettings— Installe une extension au démarrage du navigateur.
   - ExtensionInstallBlocklist— Empêche l'installation d'extensions spécifiques.
   - ExtensionInstallAllowlist— Autorise l'installation de certaines extensions.
5. Des règles supplémentaires satisfont aux exigences restantes :
   - ManagedBookmarks— Ajoute des signets aux pages Web.
   - RestoreOnStartupURL — Configure les pages Web qui sont ouvertes chaque fois qu'une nouvelle fenêtre de navigateur est ouverte.
   - AllowDeletingBrowserHistory— Configure si les utilisateurs peuvent supprimer leur historique de navigation.
   - IncognitoModeAvailability— Détermine si les utilisateurs peuvent accéder au mode navigation privée.

Étape 3 : Création d'un fichier de politiques JSON personnalisé

Créez un fichier JSON en utilisant un éditeur de texte, un modèle et les politiques (ou « règles ») que vous avez trouvées à l'étape précédente.

1. Ouvrez un éditeur de texte.
2. Copiez le modèle suivant et collez-le dans votre éditeur de texte :

```
{
  "chromePolicies":
    {
        "ManagedBookmarks":
        {
            "value":
            [
                {
                    "name": "Bookmark 1",
                    "url": "bookmark-url-1"
                },
                {
                    "name": "Bookmark 2",
                    "url": "bookmark-url-2"
                },
            ]
        },
        "RestoreOnStartup":
        {
            "value": 4
        },
        "RestoreOnStartupURLs":
        {
            "value":
            [
                "startup-url"
            ]
        },
        "ExtensionInstallBlocklist": {
            "value": [
                "insert-extensions-value-to-block",
            ]
        },
        "ExtensionInstallAllowlist": {
```

```
            "value": [
                "insert-extensions-value-to-allow",
            ]
        },
        "ExtensionSettings":
        {
            "value":
            {
                "insert-extension-value-to-force-install":
                {
                    "installation_mode": "force_installed",
                    "update_url": "https://clients2.google.com/service/update2/crx",
                    "toolbar_pin": "force_pinned"
                },
            }
        },
        "AllowDeletingBrowserHistory":
        {
            "value": should-allow-history-deletion
        },
        "IncognitoModeAvailability":
        {
            "value": incognito-mode-availability
        }
    }
}
```

Étape 4 : Ajout de vos politiques au modèle

Ajoutez vos politiques personnalisées au modèle pour chaque exigence de l'entreprise.

1. Configurez les URL des favoris.
   a. Sous la clé `value`, ajoutez des paires de clés `name` et `url` pour chaque favori à ajouter.
   b. Définissez `bookmark-url-1` sur `https://www.amazon.com`.
   c. Définissez `bookmark-url-2` sur `https://docs.aws.amazon.com/workspaces-web/latest/adminguide/`.

```
    "ManagedBookmarks":
```

```
        {
            "value":
            [
                {
                    "name": "Amazon",
                    "url": "https//www.amazon.com"
                },
                {
                    "name": "Bookmark 2",
                    "url": "https://docs.aws.amazon.com/workspaces-web/latest/
adminguide/"
                },
            ]
        },
```

2. Configurez les URL de démarrage. Cette politique permet aux administrateurs de définir les pages web qui s'affichent lorsqu'un utilisateur lance une nouvelle fenêtre de navigateur.

   a. Définissez `RestoreOnStartup` sur `4`. Cela amène l'action `RestoreOnStartup` à ouvrir une liste d'URL. Vous pouvez également utiliser d'autres actions sur vos URL de démarrage. Pour en savoir plus, consultez Liste de règles Chrome Enterprise.

   b. Définissez `RestoreOnStartupURLs` sur https://www.aboutamazon.com/news.

```
    "RestoreOnStartup":
       {
           "value": 4
       },
   "RestoreOnStartupURLs":
       {
           "value":
           [
               "https://www.aboutamazon.com/news"
           ]
       },
```

3. Pour empêcher l'utilisateur de supprimer l'historique de son navigateur, définissez `AllowDeletingBrowserHistory` sur `false`.

```
    "AllowDeletingBrowserHistory":
```

```
    {
        "value": false
    },
```

4. Pour désactiver l'accès au mode navigation privée pour vos utilisateurs, définissez `IncognitoModeAvailability` sur `1`.

```
"IncognitoModeAvailability":
   {
       "value": 1
   }
```

5. Définissez et appliquez le plug-in Okta avec les politiques suivantes :

   - `ExtensionSettings` – Installe une extension au démarrage du navigateur. La valeur d'extension est disponible sur la page d'aide du plug-in Okta.
   - `ExtensionInstallBlocklist` – Empêche l'installation d'extensions spécifiques. Utilisez la valeur `*` pour bloquer toutes les extensions par défaut. Les administrateurs peuvent décider des extensions à autoriser dans `ExtensionInstallAllowlist`.
   - `ExtensionInstallAllowlist` vous permet d'installer certaines extensions. Comme `ExtensionInstallBlocklist` est défini sur `*`, ajoutez la valeur du plug-in Okta ici pour l'autoriser.

   Voici un exemple de politique permettant d'activer le plug-in Okta :

```
    "ExtensionInstallBlocklist": {
        "value": [
            "*",
            ]
    },
    "ExtensionInstallAllowlist": {
        "value": [
            "glnpjglilkicbckjpbgcfkogebgllemb",
           ]
    },
    "ExtensionSettings": {
        "value": {
            "glnpjglilkicbckjpbgcfkogebgllemb": {
```

```
                    "installation_mode": "force_installed",
                    "update_url": "https://clients2.google.com/service/update2/crx",
                    "toolbar_pin": "force_pinned"
                }
            }
```

Étape 5 : Chargement de votre fichier JSON de politiques sur votre portail web

1. Ouvrez la console WorkSpaces Secure Browser à l'adressehttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Choisissez WorkSpaces Secure Browser, puis Portails Web.
3. Sélectionnez votre portail web, puis choisissez Modifier.
4. Sélectionnez Paramètres de politiques, puis Chargement de fichier JSON.
5. Sélectionnez Choisir un fichier. Accédez à votre fichier JSON, sélectionnez-le et chargez-le.
6. Choisissez Enregistrer.

Modification de la politique de navigateur de référence

Afin de fournir le service, WorkSpaces Secure Browser applique une politique de navigation de base à tous les portails. Cette politique de référence est appliquée en plus de celles que vous spécifiez à partir de la vue de la console ou du chargement JSON. Voici la liste des politiques appliquées par le service au format JSON :

```
{
    "chromePolicies":
    {
        "DefaultDownloadDirectory": {
            "value": "/home/as2-streaming-user/MyFiles/TemporaryFiles"
        },
        "DownloadDirectory": {
            "value": "/home/as2-streaming-user/MyFiles/TemporaryFiles"
        },
        "DownloadRestrictions": {
            "value": 1
        },
        "URLBlocklist": {
```

```
            "value": [
                "file://",
                "http://169.254.169.254",
                "http://[fd00:ec2::254]",
            ]
        },
        "URLAllowlist": {
            "value": [
                "file:///home/as2-streaming-user/MyFiles/TemporaryFiles",
                "file:///opt/appstream/tmp/TemporaryFiles",
            ]
        }
    }
}
```

Les clients ne peuvent pas apporter de modifications aux politiques suivantes :

- `DefaultDownloadDirectory` – Cette politique ne peut pas être modifiée. Le service annule toute modification apportée à cette politique.
- `DownloadDirectory` – Cette politique ne peut pas être modifiée. Le service annule toute modification apportée à cette politique.

Les clients peuvent mettre à jour les politiques suivantes pour leur portail web :

- `DownloadRestrictions` – La valeur par défaut est définie sur `1` pour empêcher les téléchargements identifiés comme étant malveillants par la navigation sécurisée dans Chrome. Pour en savoir plus, consultez Empêcher les utilisateurs de télécharger des fichiers dangereux. Vous pouvez définir une valeur de `0` à `4`.
- Les politiques `URLAllowlist` et `URLBlocklist` peuvent être étendues à l'aide de la fonctionnalité Filtrage d'URL de la vue de la console ou du chargement JSON. Toutefois, les URL de référence ne peuvent pas être remplacées. Ces politiques ne sont pas visibles dans un fichier JSON téléchargé depuis votre portail web. Cependant, si vous accédez à « chrome://policy » au cours d'une session, le navigateur distant affiche les politiques (ou « règles ») appliquées.

Configuration de l'éditeur de méthode d'entrée (IME)

Un éditeur de méthode d'entrée (IME) est un utilitaire qui offre à l'utilisateur final la possibilité de saisir du texte dans une langue qui n'utilise pas la disposition de clavier QWERTY. Les IME

permettent aux utilisateurs de saisir du texte dans des langues présentant des ensembles de caractères plus importants et complexes, comme le japonais, le chinois et le coréen. WorkSpaces Les sessions Secure Browser incluent le support IME par défaut. Les utilisateurs peuvent sélectionner d’autres langues dans la barre d’outils IME de la session ou par le biais de raccourcis clavier.

Les langues suivantes sont actuellement prises en charge par l'IME de WorkSpaces Secure Browser :

- Anglais
- Chinois simplifié (pinyin)
- Chinois traditionnel (bopomofo)
- Japonais
- Coréen

Pour sélectionner une langue dans la barre d’outils IME, procédez comme suit :

1. Sélectionnez le menu déroulant du sélecteur de langue situé à droite de la barre noire du panneau supérieur. Par défaut, le sélecteur indique en, pour l’anglais.
2. Dans le menu déroulant, sélectionnez la langue souhaitée.
3. Dans le sous-menu qui apparaît après avoir choisi la langue, sélectionnez des informations supplémentaires sur la langue.

Pour sélectionner une langue à l’aide de raccourcis clavier, procédez comme suit :

- Tous les IME
  - Pour parcourir les IME (ou passer à la bonne disposition de clavier), appuyez sur Shift+Control+Left Alt.
- Japonais
  - Pour sélectionnez Hiragana, appuyez sur F6.
  - Pour sélectionner Katakana, appuyez sur F7.
  - Pour sélectionner Latin, appuyez sur F10.
  - Pour sélectionner Latin large, appuyez sur F9.
  - Pour sélectionner Entrée directe, appuyez sur ALT +, ALT+@, Zenkaku Hankaku.

- Coréen
  - Pour sélectionner Hangul, appuyez sur Shift+Space.
  - Pour sélectionner Hanja, appuyez sur F9.

Pour supprimer la barre d'outils et le menu IME, ou pour désactiver le clavier virtuel de vos sessions WorkSpaces Secure Browser, contactez AWS Support.

Configuration de la localisation dans la session

Lorsqu'un utilisateur démarre une session, WorkSpaces Secure Browser détecte les paramètres de langue et de fuseau horaire du navigateur local de l'utilisateur et les applique à la session. Cela a une incidence sur la langue affichée pendant la session, et l’heure affichée correspond à celle de la localisation de l’utilisateur.

La liste suivante indique les codes de langue actuellement pris en charge par WorkSpaces Secure Browser. Si le navigateur local de l’utilisateur est configuré pour utiliser un code de langue non pris en charge, l’anglais américain (en-US) devient la langue par défaut de la session.

- Allemand
  - de – Allemand
  - de-AT – Allemand (Autriche)
  - de-DE – Allemand (Allemagne)
  - de-CH – Allemand (Suisse)
  - de-LI – Allemand (Liechtenstein)
- Anglais
  - en – Anglais
  - en-AU – Anglais (Australie)
  - en-CA – Anglais (Canada)
  - en-IN – Anglais (Inde)
  - en-NZ – Anglais (Nouvelle-Zélande)
  - en-za – Anglais (Afrique australe)
  - en-GB – Anglais (Royaume-Uni)
  - en-US – Anglais (États-Unis)
- Espagnol

  - es – Espagnol
  - es-AR – Espagnol (Argentine)
  - es-CL – Espagnol (Chili)
  - es-CO – Espagnol (Colombie)
  - es-CR – Espagnol (Costa Rica)
  - es-HN – Espagnol (Honduras)
  - es-419 – Espagnol (Amérique latine)
  - es-MX – Espagnol (Mexique)
  - es-PE – Espagnol (Pérou)
  - es-ES – Espagnol (Espagne)
  - es-US – Espagnol (États-Unis)
  - es-UY – Espagnol (Uruguay)
  - es-VE – Espagnol (Venezuela)
- Français
  - fr – Français
  - fr-CA – Français (Canada)
  - fr-FR – Français (France)
  - fr-CH – Français (Suisse)
- Indonésien
  - id – Indonésien
  - Id-ID – Indonésien (Indonésie)
- Italien
  - it – Italien
  - It-it – Italien (Italie)
  - IT-ch – Italien (Suisse)
- Japonais
  - ja – Japonais
  - ja-JP – Japonais (Japon)
- Coréen
  - ko – Coréen

  - ko-KR – Coréen (Corée)
- Portugais
  - pt – Portugais
  - pt-BR – Portugais (Brésil)
  - pt-PT – Portugais (Portugal)
- Chinois
  - zh – Chinois
  - zh-CN – Chinois (Chine)
  - zh-HK – Chinois (Hong Kong)
  - zh-TW – Chinois (Taïwan)

La langue de session est déterminée dans l'ordre de priorité suivant :

1. La ForcedLanguagespolitique dans les paramètres du navigateur du portail Web. Pour plus d'informations, consultez ForcedLanguages.
2. Paramètre de langue du navigateur local de l'utilisateur final.
3. Valeur par défaut, Anglais (en-US).

Le fuseau horaire est déterminé par les paramètres de fuseau horaire locaux spécifiés dans le navigateur de l'utilisateur final. Si le paramètre de fuseau horaire n'est pas valide, UTC est utilisé.

Les composants suivants de WorkSpaces Secure Browser prennent en charge la localisation :

- WorkSpaces Page de connexion au navigateur sécurisé
- WorkSpaces Messages d'état du portail Secure Browser (y compris les messages de chargement et les erreurs)
- Navigateur Chrome
- Menu contextuel et fenêtre Enregistrer sous du système

Pour définir les paramètres du navigateur local d'un utilisateur, procédez de l'une des manières suivantes :

- Dans Chrome, sélectionnez Paramètres, Langues, puis classez les langues selon vos préférences.

- Dans Firefox, sélectionnez Paramètres, Général, Langue, puis sélectionnez la langue dans le menu déroulant.
- Dans Edge, sélectionnez Paramètres, Langues, puis classez les langues selon vos préférences.

Configuration des contrôles d'accès IP (facultatif)

WorkSpaces Secure Browser vous permet de contrôler les adresses IP à partir desquelles votre portail Web est accessible. En utilisant les paramètres d'accès IP, vous pouvez définir et gérer des groupes d'adresses IP approuvées et autoriser les utilisateurs à accéder à leur portail uniquement lorsqu'ils sont connectés à un réseau approuvé.

Par défaut, WorkSpaces Secure Browser permet aux utilisateurs d'accéder à leur portail Web de n'importe où. Un groupe de contrôles d'accès IP fait office de pare-feu virtuel qui filtre l'adresse IP qu'un utilisateur peut utiliser pour se connecter au portail web. Lorsqu'ils sont associés à votre portail web, les paramètres d'accès IP détectent l'adresse IP de l'utilisateur avant l'authentification afin de déterminer s'il est habilité à se connecter. Une fois connecté, WorkSpaces Secure Browser surveille en permanence l'adresse IP d'un utilisateur pour s'assurer qu'il reste connecté depuis un réseau fiable. Si l'adresse IP d'un utilisateur change, WorkSpaces Secure Browser détecte et met fin à la session.

Pour spécifier les plages d'adresses CIDR, ajoutez des règles à votre groupe de contrôles d'accès IP, puis associez le groupe à votre portail web. Vous pouvez associer chaque paramètre d'accès IP à un ou plusieurs portails web. Pour spécifier les adresses IP publiques et les plages d'adresses IP de vos réseaux approuvés, ajoutez des règles à vos groupes de contrôle d'accès IP. Si vos utilisateurs accèdent à leur portail web via une passerelle NAT ou un VPN, vous devez créer des règles qui autorisent le trafic en provenance d'adresses IP publiques pour la passerelle NAT ou le VPN.

> **Note**
>
> Les clients sont tenus de comprendre les problèmes juridiques potentiels liés à leur utilisation de WorkSpaces Secure Browser et doivent s'assurer que leur utilisation de WorkSpaces Secure Browser est conforme à toutes les lois et réglementations applicables. Cela inclut les lois qui réglementent la capacité d'un employeur à surveiller l'utilisation de WorkSpaces Secure Browser par un employé, y compris les activités effectuées au sein de l'application.

Création d'un groupe de contrôles d'accès IP

Pour créer un groupe de contrôles d'accès IP, procédez comme suit.

1. Ouvrez la console WorkSpaces Secure Browser à l'adressehttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Dans le volet de navigation, sélectionnez Contrôles d'accès IP.
3. Sélectionnez Créer un groupe de contrôle d'accès IP.
4. Dans la boîte de dialogue Créer un groupe de contrôle d'accès IP, saisissez un nom (obligatoire) et une description (facultatif) pour le groupe.
5. Saisissez l'adresse IP ou la plage d'adresses IP CIDR qui sera associée à la Source, ainsi qu'une Description (facultatif).
6. Sous Balises, indiquez si vous souhaitez baliser une paire clé-valeur pour chaque groupe de contrôles d'accès IP.
7. Lorsque vous avez fini d'ajouter des règles et des balises, sélectionnez Enregistrer.

Association d'un paramètre d'accès IP à un portail web

Pour associer un groupe de contrôles d'accès IP à un portail web existant, procédez comme suit.

1. Ouvrez la console WorkSpaces Secure Browser à l'adressehttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Dans le panneau de navigation, sélectionnez Portails web.
3. Sélectionnez le portail web, puis choisissez Modifier.
4. Sous Groupe de contrôle d'accès IP, sélectionnez les groupes de contrôles d'accès IP pour le portail web.
5. Choisissez Enregistrer.

Pour associer un groupe de contrôles d'accès IP pendant la création d'un portail web, procédez comme suit.

1. Effectuez les étapes 1 à 4 décrites dans the section called "Configuration des paramètres du portail" pour accéder à Contrôle d'accès IP (facultatif).
2. Sélectionnez Créer des contrôles d'accès IP.

3. Dans la boîte de dialogue Créer un groupe IP, saisissez un nom (obligatoire) et une description (facultatif) pour le groupe.
4. Saisissez l'adresse IP ou la plage d'adresses IP CIDR qui sera associée à la Source, ainsi qu'une Description (facultatif).
5. Sous Balises, indiquez si vous souhaitez baliser une paire clé-valeur pour chaque groupe de contrôles d'accès IP.
6. Lorsque vous avez fini d'ajouter des règles et des balises, sélectionnez Créer un contrôle d'accès IP.
7. Votre groupe de contrôles d'accès IP sera associé à ce portail web lors de son lancement.

Modification d'un groupe de contrôles d'accès IP

Vous pouvez à tout moment supprimer une règle d'un paramètre d'accès IP. Si vous supprimez une règle qui a servi à autoriser une connexion à un portail web, les utilisateurs ayant une session active sont alors déconnectés du portail web.

Pour modifier un groupe de contrôles d'accès IP, procédez comme suit.

1. Ouvrez la console WorkSpaces Secure Browser à l'adressehttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Dans le volet de navigation, sélectionnez Contrôles d'accès IP.
3. Sélectionnez le groupe et choisissez Modifier.
4. Modifiez la Source et la Description (facultatif) des règles existantes ou ajoutez des règles supplémentaires.
5. Sous Balises, indiquez si vous souhaitez baliser une paire clé-valeur pour chaque groupe de contrôles d'accès IP.
6. Lorsque vous avez fini d'ajouter des règles et des balises, sélectionnez Enregistrer.
7. Si vous avez mis à jour un paramètre d'accès IP existant, patientez 15 minutes au maximum avant que la règle nouvelle ou modifiée prenne effet.

Suppression d'un groupe de contrôles d'accès IP

Vous pouvez supprimer une règle d'un groupe de contrôles d'accès IP à tout moment. Si vous supprimez une règle qui a servi à autoriser une connexion à un portail web, les utilisateurs ayant une session active sont alors déconnectés du portail web.

Pour supprimer un groupe de contrôles d'accès IP, procédez comme suit.

1. Ouvrez la console WorkSpaces Secure Browser à l'adressehttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Dans le volet de navigation, sélectionnez Groupe de contrôle d'accès IP.
3. Sélectionnez le groupe et choisissez Supprimer.

Activation d'extension pour l'authentification unique (facultatif)

Vous pouvez activer une extension pour faire bénéficier vos utilisateurs finaux d'une meilleure expérience de connexion aux portails. Par exemple, si vous utilisez Okta comme fournisseur d'identité (IdP) SAML 2.0 pour votre portail, et qu'il sert également d'IdP sur les sites web que vous autorisez les utilisateurs à consulter au cours d'une session, vous pouvez transmettre le cookie de connexion Okta à la session à l'aide de l'extension. Ainsi, lorsque les utilisateurs consulteront un site web qui nécessite le cookie du domaine Okta, ils pourront accéder au site web sans avoir à se connecter pendant la session.

L'extension est prise en charge dans les navigateurs Chrome et Firefox. Elle permet la synchronisation des cookies pour les domaines autorisés dès que l'utilisateur se connecte à la session. L'extension dispense l'utilisateur de se connecter, et elle fonctionne en arrière-plan pour permettre la synchronisation des cookies sans que l'utilisateur n'ait besoin d'effectuer une quelconque action après l'installation. Aucune donnée n'est stockée par l'extension.

Les utilisateurs sont invités à installer l'extension lorsqu'ils se connectent à un portail.

Par défaut, les extensions ne sont pas activées dans Chrome dans les fenêtres de navigation privée ou dans les fenêtres de navigation privée de Firefox. Les utilisateurs peuvent les activer manuellement. Pour plus d'informations sur Chrome, consultez la section Extensions en mode navigation privée. Pour plus d'informations sur Firefox, consultez Extensions dans la navigation privée.

Vous pouvez mettre à jour la configuration des paramètres utilisateur existants d'un portail ou lorsque vous créez un portail web pour la première fois. Tout d'abord, identifiez les domaines dont vous avez besoin pour votre IdP SAML et vos sites web. Vous pouvez ajouter jusqu'à 10 domaines.

Il vous incombe de tester et d'identifier le domaine approprié pour la synchronisation des cookies. Vous serez peut-être amené à apporter des modifications au niveau de l'IdP ou de l'authentification de site web pour faire en sorte que l'authentification unique fonctionne comme prévu.

Pour savoir quels domaines utiliser avec l'IdP le plus courant, reportez-vous au tableau suivant :

IdP et domaines

IdP	Domaine
Okta	okta.com
Entrez votre identifiant	microsoftonline.com
AWS Identity Center	awsapps.com
Un seul identifiant	onelogin.com
Duo	duosecurity.com

Accédez ensuite à votre portail Web dans la console. Autorisez l'extension, puis ajoutez les cookies des domaines qui doivent être synchronisés. Suivez les étapes ci-dessous pour créer un portail en ayant l'extension autorisée ou pour mettre à jour un portail existant.

Pour autoriser l'extension pendant la création d'un portail web, procédez comme suit :

1. Suivez les étapes décrites dans the section called "Étape 1 : Création d'un portail web" jusqu'à the section called "Configuration des paramètres utilisateur".
2. À l'étape 1 de the section called "Configuration des paramètres utilisateur", sous Autorisations utilisateur, sélectionnez Autorisé pour activer l'extension pour votre portail web.
3. Indiquez le domaine en vue de la synchronisation des cookies, puis choisissez Ajouter un nouveau domaine.
4. Effectuez les étapes décrites dans the section called "Configuration des paramètres utilisateur" et les sections restantes dans the section called "Étape 1 : Création d'un portail web" pour créer votre portail web.

Pour ajouter l'extension à un portail web existant, procédez comme suit :

1. Ouvrez la console WorkSpaces Secure Browser à l'adresse https://console.aws.amazon.com/workspaces-web/home.
2. Sélectionnez le portail web à modifier.

3. Sélectionnez Paramètres utilisateur, Autorisations utilisateur et Autorisé pour activer l'extension pour votre portail web.
4. Indiquez le domaine en vue de la synchronisation des cookies, puis choisissez Ajouter un nouveau domaine.
5. Enregistrez les modifications apportées au portail. Le portail invite alors les utilisateurs à installer l'extension dans les 15 minutes.

Pour modifier des domaines ou supprimer l'extension, procédez comme suit :

1. Ouvrez la console WorkSpaces Secure Browser à l'adresse https://console.aws.amazon.com/workspaces-web/home.
2. Sélectionnez le portail web à modifier.
3. Sélectionnez Paramètres utilisateur, Autorisations utilisateur et Non autorisé pour supprimer l'extension de votre portail web.
4. Supprimez ou modifiez des domaines individuellement.
5. Une fois les cookies supprimés, les sessions ne synchronisent plus les cookies, même si l'extension WorkSpaces Secure Browser est installée dans le navigateur de l'utilisateur.

Pour en savoir plus sur l'expérience utilisateur avec l'extension, consultez the section called "Extension pour l'authentification unique".

Configurer le filtrage des URL

Vous pouvez utiliser les règles de Chrome pour filtrer les URL auxquelles les utilisateurs peuvent accéder depuis leur navigateur distant. Chrome Policy propose deux mécanismes pour filtrer les URL : URLAllowList et URLBlocklist. Vous pouvez utiliser l'interface de console WorkSpaces Secure Browser pour configurer le filtrage d'URL en tant que paramètre de portail, ou vous pouvez l'ajouter dans le cadre de votre instruction JSON personnalisée (soit dans l'éditeur en ligne, soit sous forme de téléchargement de fichier JSON).

Pour configurer le filtrage des URL à l'aide de la console

1. Ouvrez la console WorkSpaces Secure Browser à l'adressehttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Choisissez WorkSpaces Secure Browser, Portails Web, choisissez votre portail Web, puis sélectionnez Afficher les détails.

3. Pour le filtrage des URL, choisissez l'une des options suivantes :

   - Autoriser l'accès à toutes les URL : par défaut, un portail Web autorise l'accès à toutes les URL. Vous pouvez ajouter des sites Web spécifiques à la liste BlockURL pour empêcher les utilisateurs de visiter ces sites au cours d'une session. Par exemple, l'ajout de www.anycorp.com à la liste des URL de blocage empêchera l'utilisateur d'accéder à www.anycorp.com pendant sa session.
   - Bloquer l'accès à toutes les URL : par défaut, le portail Web bloque l'accès à toutes les URL. Vous pouvez ajouter des sites Web spécifiques à la liste des URL autorisées pour établir une liste des sites Web que les utilisateurs peuvent visiter et bloquer le trafic vers d'autres sites Web. Envisagez d'ajouter chaque URL en tant que signet pour permettre aux utilisateurs d'y accéder en un clic pendant leur session.
   - Configuration avancée : choisissez cette option pour créer des listes AllowURL et BlockURL en parallèle. La liste d'URL autorisée a priorité sur la liste d'URL bloquée. Cette option permet de filtrer les URL par chemin. Par exemple, vous pouvez ajouter www.anycorp.com à la liste de blocage, puis ajouter www.anycorp.com/hr à la liste des autorisations. Cela permet aux utilisateurs de visiter www.anycorp.com/hr, mais ils ne pourront pas accéder à d'autres chemins d'URL, tels que www.anycorp.com/finance.

Pour plus d'informations sur l'utilisation des URL bloquées et autorisées, voir Autoriser ou bloquer l'accès aux sites Web. Ajoutez des URL à ces listes en suivant le format de filtre de liste de blocage de Chrome pour obtenir les meilleurs résultats. Pour plus d'informations, voir Format de filtre de liste de blocage d'URL.

Pour configurer le filtrage des URL à l'aide de l'éditeur JSON ou du téléchargement de fichiers

1. Dans le module des paramètres de politique, choisissez l'éditeur JSON et ignorez le module d'interface utilisateur de la console pour la vue Éditeur ou Téléchargement de fichiers.

   - L'éditeur permet aux clients de créer des déclarations de politique personnalisées en ligne dans la console. L'éditeur met en évidence les erreurs dans l'instruction JSON lors de la création de la politique.
   - Le téléchargement de fichiers permet aux clients d'ajouter un fichier JSON créé en dehors de la console (exporté depuis un navigateur Chrome existant, par exemple).
2. Consultez les détails des règles de Chrome relatives à URLAllowList et URLBlocklist afin de formater correctement une liste Allow/DenyURL pour votre portail Web. Pour plus d'informations, consultez URLAllowList et URLBlocklist.

Autoriser les liens profonds (facultatif)

Lorsqu'un utilisateur se connecte à WorkSpaces Secure Browser, il démarre la session sur une page d'accueil définie par l'administrateur. Vous pouvez également autoriser les portails à recevoir des liens profonds qui connectent les utilisateurs à un site Web spécifique au cours d'une session. Lorsqu'un lien profond est sélectionné, le portail affiche l'URL spécifiée dans le lien profond. Le lien est affiché à côté de la ou des pages d'accueil configurées pour le démarrage de la session, ou seul si une session est déjà en cours. Cette fonctionnalité permet aux administrateurs de créer des expériences utilisateur plus dynamiques avec WorkSpaces Secure Browser. Pour autoriser les liens profonds, choisissez Autorisé lors de la création des paramètres utilisateur. Pour plus d'informations, consultez the section called "Configuration des paramètres utilisateur".

Les liens profonds ouvrent des pages dans une session WorkSpaces Secure Browser. Si une session est déjà en cours, le lien profond s'ouvre dans un nouvel onglet. Si aucune session n'est déjà en cours, elle ouvre l'URL du lien profond dans un nouvel onglet et la page d'accueil par défaut du portail dans un onglet distinct. Si un lien profond contient plusieurs URL, il affichera l'URL du lien profond répertoriée en premier, chaque URL suivante (y compris la page d'accueil par défaut) étant ouverte dans des onglets distincts.

Les liens profonds doivent répondre aux exigences suivantes :

- Les autorisations relatives aux liens profonds du portail doivent être définies sur Autorisé. Pour plus d'informations, consultez the section called "Configuration des paramètres utilisateur".
- Le site vers lequel vous souhaitez créer un lien profond doit être codé en URL. Par exemple, pour lier un utilisateur à « https://www.example.com/?query=true », mettez à jour le lien vers https://A%2F%2Fhttps://www.example.com%F%F%FQuery%DTrue.
- Ajoutez l'URL à une URL de portail répertoriée comme suit, où UUID est l'identifiant du portail :

  https ://<uuid>.workspaces-web.com/ ? DeepLinks=https://A%2F%2F%F%F%FQuery%DTrue
- Un lien profond peut contenir jusqu'à 10 URL, délimitées par une virgule. Par exemple :

  https ://<uuid>.workspaces-web.com/ ? DeepLinks=https://A%2F%3F%F%FQuery%DTrue, https://www.example.com%F%F%FQuery%DTrue2, https://A%2F%Fhttps://www.example.com%F%FQuery%DTrue3, https://A%2F%Fwww.exemple.com%F%F%FQuery%FQuery.com/FQuery%Fquery %DTrue4

Tout utilisateur avec lequel vous partagez ce lien de portail peut manipuler la valeur du lien profond pour visiter un site Web, si ce domaine est accessible depuis le portail et ne figure pas sur la liste d'URL à bloquer. Pour créer une liste d'autorisation ou une liste de blocage restrictive afin d'empêcher les utilisateurs de visiter des domaines non souhaités sur votre portail, utilisez le filtrage d'URL. La liste d'autorisation et la liste de blocage d'un portail peuvent être modifiées à l'aide du filtrage des URL dans les paramètres du navigateur de votre portail. Pour plus d'informations, voir the section called "Configurer le filtrage des URL" Autoriser ou bloquer l'accès aux sites Web.

Sécurité dans Amazon WorkSpaces Secure Browser

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

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

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

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation d'Amazon WorkSpaces Secure Browser. Il vous explique comment configurer Amazon WorkSpaces Secure Browser pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser les ressources de votre Amazon WorkSpaces Secure Browser.

Table des matières

Protection des données dans Amazon WorkSpaces Secure Browser

Le modèle de responsabilité AWS partagée s'applique à la protection des données dans Amazon WorkSpaces Secure Browser. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des AWS services que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez la section Confidentialité des données FAQ. Pour plus d'informations sur la protection des données en Europe, consultez le modèle de responsabilitéAWS partagée et le billet de GDPR blog sur le blog sur la AWS sécurité.

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

- Utilisez l'authentification multifactorielle (MFA) pour chaque compte.
- UtilisezSSL/TLSpour communiquer avec les AWS ressources. Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Configuration API et journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent AWS services.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de FIPS 140 à 3 modules cryptographiques validés pour accéder AWS via une interface de ligne de commande ou unAPI, utilisez un point de terminaison. FIPS Pour plus d'informations sur les FIPS points de terminaison disponibles, voir Federal Information Processing Standard (FIPS) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec WorkSpaces Secure Browser ou autre AWS services à l'aide de la consoleAPI, AWS CLI, ou AWS SDKs. Toutes les données que

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

Chiffrement des données

Amazon WorkSpaces Secure Browser collecte les données de personnalisation du portail, telles que les paramètres du navigateur, les paramètres utilisateur, les paramètres réseau, les informations du fournisseur d'identité, les données du trust store et les données des certificats du trust store. WorkSpaces Secure Browser collecte également les données relatives aux politiques du navigateur, les préférences de l'utilisateur (pour les paramètres du navigateur) et les journaux de session. Les données collectées sont stockées dans Amazon DynamoDB et Amazon S3. WorkSpaces Secure Browser est utilisé AWS Key Management Service pour le chiffrement.

Pour sécuriser votre contenu, suivez ces recommandations :

- Implémentez l'accès avec le moindre privilège et créez des rôles spécifiques à utiliser pour les actions de WorkSpaces Secure Browser. Utilisez IAM des modèles pour créer un rôle en accès complet ou en lecture seule. Pour de plus amples informations, veuillez consulter AWS politiques gérées pour WorkSpaces Secure Browser.
- Protégez les données de bout en bout en fournissant une clé gérée par le client, afin que WorkSpaces Secure Browser puisse chiffrer vos données au repos avec les clés que vous fournissez.
- Faites preuve de prudence lorsque vous partagez des domaines de portail et des informations d'identification utilisateur :
  - Les administrateurs doivent se connecter à la WorkSpaces console Amazon et les utilisateurs doivent se connecter au portail WorkSpaces Secure Browser.
  - Toute personne peut accéder au portail web depuis Internet, mais elle ne peut pas y lancer de session sans disposer d'informations d'identification utilisateur valides.
- Les utilisateurs peuvent explicitement mettre fin à leurs sessions en sélectionnant Terminer la session. L'instance hébergeant la session du navigateur est alors supprimée et le navigateur isolé.

WorkSpaces Secure Browser sécurise le contenu et les métadonnées par défaut en cryptant toutes les données sensibles avec. AWS KMS Il collecte la politique du navigateur et les préférences de l'utilisateur pour appliquer les politiques et les paramètres lors des sessions WorkSpaces Secure

Browser. Si une erreur se produit lors de l'application des paramètres existants, l'utilisateur ne peut ni accéder à de nouvelles sessions ni accéder aux sites internes et aux applications SaaS de l'entreprise.

Chiffrement au repos

Le chiffrement au repos est configuré par défaut. Les données spécifiques au client utilisées dans WorkSpaces Secure Browser sont cryptées à l'aide de. AWS KMS WorkSpaces Secure Browser fournit un chiffrement au repos pour les ressources que vous créez. Le service accepte une clé gérée par le AWS KMS client lors de la création de ressources, et si aucune n'est fournie, une clé AWS détenue sera utilisée pour chiffrer les ressources au repos. Le service chiffre le document Politique de navigateur que vous fournissez éventuellement pour personnaliser vos sessions de navigateur, tout comme la configuration de votre fournisseur d'identité et les noms d'affichage de vos portails. Ces informations resteront cryptées à l'aide de la clé gérée par le client ou de la clé AWS détenue pendant qu'elles sont stockées dans notre backend.

Vous pouvez décider quelle clé sera utilisée lors de la création d'une ressource WorkSpaces Secure Browser. Si les données faisant partie de cette ressource sont cryptées, WorkSpaces Secure Browser accepte le `customerManagedKeyArn` champ comme faisant partie du `create`API. La clé fournie doit être une clé AWS KMS symétrique, et l'administrateur qui crée la ressource en utilisant cette clé doit disposer d'autorisations `kms:Decrypt`, `kms:GenerateDataKey` et `kms:CreateGrant`. Une fois qu'une ressource est créée avec la clé, celle-ci ne peut plus être supprimée ni modifiée. Si vous avez utilisé une clé gérée par le client, l'administrateur qui accède à la ressource doit disposer d'autorisations `kms:Decrypt` et `kms:GenerateDataKey`. Si vous constatez l'existence d'une erreur relative à un accès refusé pendant l'utilisation de la console, vérifiez que l'utilisateur de la console dispose de ces autorisations avec la clé qui a été utilisée.

Vous pouvez résoudre les problèmes et auditer l'utilisation des clés en vérifiant l'état des AWS KMS subventions. Pour en savoir plus, consultez Managing grants. Lors de la création du portail, WorkSpaces Secure Browser crée une autorisation pour permettre au service d'accéder à la clé de manière asynchrone. Vous pouvez vérifier le statut d'utilisation de la clé en vérifiant l'octroi ainsi que le contexte de chiffrement fourni au moment où l'octroi est utilisé. Le contexte de chiffrement contient toujours une entrée avec la clé `aws:workspaces-web:portal:id` et une valeur égale à l'ID de votre portail. Pour les autres ressources, le contexte de chiffrement contient toujours une entrée au format `aws:workspaces-web:`*`RESOURCE_TYPE`*`:id` et l'ID de ressource correspondant.

Chiffrement en transit

WorkSpaces Secure Browser chiffre les données en transit depuis HTTPS et vers la version TLS 1.2. Vous pouvez envoyer une demande à WorkSpaces en utilisant la console ou par des API appels directs. Les données de demande transférées sont cryptées en envoyant le tout via une TLS connexion HTTPS OR. Les données de demande peuvent être transférées depuis la AWS console ou AWS SDK vers WorkSpaces Secure Browser. AWS Command Line Interface

Le chiffrement en transit est configuré par défaut, et les connexions sécurisées (HTTPS,TLS) sont configurées par défaut.

Gestion des clés

Vous pouvez fournir votre propre AWS KMS clé gérée par le client pour chiffrer les informations de vos clients. Si vous n'en fournissez pas, WorkSpaces Secure Browser utilisera une clé AWS détenue. Vous pouvez régler votre clé à l'aide du AWS SDK.

Confidentialité du trafic inter-réseaux

Pour sécuriser les connexions entre WorkSpaces Secure Browser et les applications sur site, vous utilisez WorkSpaces Secure Browser pour lancer des sessions de navigateur au sein de votre propre VPC navigateur. La connexion aux applications sur site est configurée vous-même VPC et n'est pas contrôlée par WorkSpaces Secure Browser.

Pour sécuriser les connexions entre les comptes, WorkSpaces Secure Browser utilise un rôle lié à un service pour se connecter en toute sécurité aux comptes clients et exécuter des opérations pour le compte du client. Pour de plus amples informations, veuillez consulter Utilisation de rôles liés à un service pour Secure Browser WorkSpaces .

Journalisation des accès utilisateur

Les administrateurs peuvent enregistrer les événements de session WorkSpaces Secure Browser, notamment le démarrage, l'arrêt et les URL visites. Ces journaux sont chiffrés et transmis de manière sécurisée aux clients via un flux de données Amazon Kinesis. Les informations de navigation issues de la journalisation des accès des utilisateurs ne sont pas stockées par AWS les sessions où la journalisation n'est pas configurée ou ne sont pas disponibles à partir de ces sessions. URLles visites en mode navigation privée, ou supprimées URLs de l'historique du navigateur, ne sont pas enregistrées dans le journal des accès des utilisateurs.

Identity and Access Management pour Amazon WorkSpaces Secure Browser

AWS Identity and Access Management (IAM) est un outil AWS service qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. IAMles administrateurs contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources du WorkSpaces Secure Browser. IAMest un AWS service outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans WorkSpaces Secure Browser.

Utilisateur du service : si vous utilisez le service WorkSpaces Secure Browser pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités de WorkSpaces Secure Browser pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans WorkSpaces Secure Browser, consultezRésolution des problèmes d'identité et d'accès à Amazon WorkSpaces Secure Browser.

Administrateur du service — Si vous êtes responsable des ressources de WorkSpaces Secure Browser dans votre entreprise, vous avez probablement un accès complet à WorkSpaces Secure

Browser. C'est à vous de déterminer les fonctionnalités et les ressources de WorkSpaces Secure Browser auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite envoyer des demandes à votre IAM administrateur pour modifier les autorisations des utilisateurs de votre service. Consultez les informations de cette page pour comprendre les concepts de base deIAM. Pour en savoir plus sur la façon dont votre entreprise peut utiliser IAM WorkSpaces Secure Browser, consultezComment fonctionne Amazon WorkSpaces Secure Browser avec IAM.

IAMadministrateur — Si vous êtes IAM administrateur, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à WorkSpaces Secure Browser. Pour consulter des exemples de politiques basées sur l'identité WorkSpaces Secure Browser que vous pouvez utiliser dansIAM, consultez. Exemples de politiques basées sur l'identité pour Amazon Secure Browser WorkSpaces

Authentification par des identités

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

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

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

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

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

Compte AWS utilisateur root

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

Identité fédérée

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

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies AWS services par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d’utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour plus d'informations sur IAM Identity Center, consultez Qu'est-ce qu'IAMIdentity Center ? dans le guide de AWS IAM Identity Center l'utilisateur.

Utilisateurs et groupes IAM

Un IAMutilisateur est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des IAM utilisateurs dotés d'informations d'identification à long terme, telles que des mots de passe et des clés d'accès. Toutefois, si vous avez des cas d'utilisation spécifiques qui nécessitent des informations d'identification à long terme auprès des IAM utilisateurs, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, voir Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification à long terme dans le Guide de IAM l'utilisateur.

Un IAMgroupe est une identité qui définit un ensemble d'IAMutilisateurs. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer IAM des ressources.

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

IAMrôles

Un IAMrôle est une identité au sein de Compte AWS vous dotée d'autorisations spécifiques. Il est similaire à un IAM utilisateur, mais n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un IAM rôle dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une AWS API opération AWS CLI or ou en utilisant une option personnaliséeURL. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez la section Utilisation IAM des rôles dans le Guide de IAM l'utilisateur.

IAMles rôles dotés d'informations d'identification temporaires sont utiles dans les situations suivantes :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour plus

d'informations sur les rôles pour la fédération, voir Création d'un rôle pour un fournisseur d'identité tiers dans le guide de IAM l'utilisateur. Si vous utilisez IAM Identity Center, vous configurez un ensemble d'autorisations. Pour contrôler les accès auxquels vos identités peuvent accéder après leur authentification, IAM Identity Center met en corrélation l'ensemble d'autorisations avec un rôle dans. IAM Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .

- Autorisations IAM utilisateur temporaires : un IAM utilisateur ou un rôle peut assumer un IAM rôle afin d'obtenir temporairement différentes autorisations pour une tâche spécifique.
- Accès entre comptes : vous pouvez utiliser un IAM rôle pour autoriser une personne (un mandant fiable) d'un autre compte à accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains AWS services cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, voir Accès aux ressources entre comptes IAM dans le guide de l'IAMutilisateur.
- Accès multiservices — Certains AWS services utilisent des fonctionnalités dans d'autres AWS services. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès transmises (FAS) — Lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FASutilise les autorisations du principal appelant an AWS service, combinées à la demande AWS service pour adresser des demandes aux services en aval. FASles demandes ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes AWS services ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives FAS aux demandes, consultez la section Transférer les sessions d'accès.
  - Rôle de service — Un rôle de service est un IAMrôle qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieurIAM. Pour plus d'informations, consultez la section Création d'un rôle auquel déléguer des autorisations AWS service dans le Guide de IAM l'utilisateur.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. AWS service Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés

au service apparaissent dans votre Compte AWS fichier et appartiennent au service. Un IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un IAM rôle pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui AWS CLI soumettent des AWS API demandes. Cela est préférable au stockage des clés d'accès dans l'EC2instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l'EC2instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez la section Utilisation d'un IAM rôle pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le Guide de IAM l'utilisateur.

Pour savoir s'il faut utiliser IAM des rôles ou des IAM utilisateurs, voir Quand créer un IAM rôle (au lieu d'un utilisateur) dans le guide de IAM l'utilisateur.

Gestion des accès à l'aide de politiques

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

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

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

IAMles politiques définissent les autorisations pour une action, quelle que soit la méthode que vous utilisez pour effectuer l'opération. Par exemple, supposons que vous disposiez d'une politique qui

autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle auprès du AWS Management Console AWS CLI, ou du AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, consultez la section Création de IAM politiques dans le Guide de l'IAMutilisateur.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour savoir comment choisir entre une politique gérée ou une politique intégrée, voir Choisir entre des politiques gérées et des politiques intégrées dans le Guide de l'IAMutilisateur.

Politiques basées sur les ressources

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

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

Listes de contrôle d'accès (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLssont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format du document JSON de stratégie.

Amazon S3 et Amazon VPC sont des exemples de services compatiblesACLs. AWS WAF Pour en savoir plusACLs, consultez la présentation de la liste de contrôle d'accès (ACL) dans le guide du développeur Amazon Simple Storage Service.

Autres types de politique

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

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

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de IAM l'utilisateur.

Comment fonctionne Amazon WorkSpaces Secure Browser avec IAM

Avant de gérer l'IAMaccès à WorkSpaces Secure Browser, découvrez quelles IAM fonctionnalités sont disponibles avec WorkSpaces Secure Browser.

IAMfonctionnalités que vous pouvez utiliser avec Amazon WorkSpaces Secure Browser

IAMfonctionnalité	WorkSpaces Support du navigateur sécurisé
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition d'une politique	Oui
ACLs	Non
ABAC(balises dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Fonctions du service	Non
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble du fonctionnement de WorkSpaces Secure Browser et AWS des autres services avec la plupart des IAM fonctionnalités, consultez la section AWS Services compatibles IAM dans le Guide de IAM l'utilisateur.

Politiques basées sur l'identité pour Secure Browser WorkSpaces

Prend en charge les politiques basées sur l'identité : oui

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, consultez la section Création de IAM politiques dans le Guide de l'IAMutilisateur.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier les actions et les ressources autorisées ou refusées ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour en savoir plus sur tous les éléments que vous pouvez utiliser dans une JSON politique, consultez la référence aux éléments de IAM JSON politique dans le Guide de IAM l'utilisateur.

Exemples de politiques basées sur l'identité pour Secure Browser WorkSpaces

Pour consulter des exemples de politiques basées sur l'identité de WorkSpaces Secure Browser, consultez. Exemples de politiques basées sur l'identité pour Amazon Secure Browser WorkSpaces

Politiques basées sur les ressources dans Secure Browser WorkSpaces

Prend en charge les politiques basées sur les ressources : non

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

Pour activer l'accès entre comptes, vous pouvez spécifier un compte entier ou IAM des entités d'un autre compte comme principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un IAM administrateur du compte de confiance doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, voir Accès aux ressources entre comptes IAM dans le Guide de IAM l'utilisateur.

Actions politiques pour WorkSpaces Secure Browser

Prend en charge les actions de politique : oui

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

L'`Action`élément d'une JSON politique décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès dans une politique. Les actions de stratégie portent généralement le même nom que l' AWS APIopération associée. Il existe certaines exceptions, telles que les actions avec autorisation uniquement qui n'ont pas d'opération correspondante. API Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

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

Pour consulter la liste des actions de WorkSpaces Secure Browser, consultez la section Actions définies par Amazon WorkSpaces Secure Browser dans le Service Authorization Reference.

Les actions de stratégie dans WorkSpaces Secure Browser utilisent le préfixe suivant avant l'action :

```
workspaces-web
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "workspaces-web:action1",
```

```
      "workspaces-web:action2"
         ]
```

Pour consulter des exemples de politiques basées sur l'identité de WorkSpaces Secure Browser, consultez. Exemples de politiques basées sur l'identité pour Amazon Secure Browser WorkSpaces

Ressources relatives aux politiques pour WorkSpaces Secure Browser

Prend en charge les ressources de politique : oui

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

L'élément `Resource` JSON de stratégie indique le ou les objets auxquels s'applique l'action. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de spécifier une ressource en utilisant son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

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

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

Pour consulter la liste des types de ressources WorkSpaces Secure Browser et leurs caractéristiquesARNs, consultez la section Ressources définies par Amazon WorkSpaces Secure Browser dans le Service Authorization Reference. Pour savoir avec quelles actions vous pouvez spécifier pour chaque ressource, consultez la ARN section Actions définies par Amazon WorkSpaces Secure Browser.

Pour consulter des exemples de politiques basées sur l'identité de WorkSpaces Secure Browser, consultez. Exemples de politiques basées sur l'identité pour Amazon Secure Browser WorkSpaces

Clés de conditions de politique pour WorkSpaces Secure Browser

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

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

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

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

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez autoriser un IAM utilisateur à accéder à une ressource uniquement si celle-ci est étiquetée avec son nom IAM d'utilisateur. Pour plus d'informations, consultez IAMla section Éléments de politique : variables et balises dans le Guide de IAM l'utilisateur.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés contextuelles de condition AWS globales dans le guide de IAM l'utilisateur.

Pour consulter la liste des clés de condition de WorkSpaces Secure Browser, consultez la section Clés de condition pour Amazon WorkSpaces Secure Browser dans la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez Actions définies par Amazon WorkSpaces Secure Browser.

Pour consulter des exemples de politiques basées sur l'identité de WorkSpaces Secure Browser, consultez. Exemples de politiques basées sur l'identité pour Amazon Secure Browser WorkSpaces

Listes de contrôle d'accès (ACLs) dans WorkSpaces Secure Browser

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLssont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format du document JSON de stratégie.

Contrôle d'accès basé sur les attributs (ABAC) avec Secure Browser WorkSpaces

Supports ABAC (balises dans les politiques) : Partiel

Le contrôle d'accès basé sur les attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises à IAM des entités (utilisateurs ou rôles) et à de nombreuses AWS ressources. Le balisage des entités et des ressources est la première étape deABAC. Vous concevez ensuite des ABAC politiques pour autoriser les opérations lorsque le tag du principal correspond à celui de la ressource à laquelle il essaie d'accéder.

ABACest utile dans les environnements qui se développent rapidement et aide dans les situations où la gestion des politiques devient fastidieuse.

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

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

Pour plus d'informationsABAC, voir Qu'est-ce que c'est ABAC ? dans le guide de IAM l'utilisateur. Pour consulter un didacticiel présentant les étapes de configurationABAC, voir Utiliser le contrôle d'accès basé sur les attributs (ABAC) dans le guide de l'IAMutilisateur.

Utilisation d'informations d'identification temporaires avec WorkSpaces Secure Browser

Prend en charge les informations d'identification temporaires : oui

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

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous

créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez la section Passage à un rôle (console) dans le guide de IAM l'utilisateur.

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

Autorisations principales interservices pour WorkSpaces Secure Browser

Prend en charge les sessions d'accès transféré (FAS) : Oui

Lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FASutilise les autorisations du principal appelant an AWS service, combinées à la demande AWS service pour adresser des demandes aux services en aval. FASles demandes ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes AWS services ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives FAS aux demandes, consultez la section Transférer les sessions d'accès.

Rôles de service pour WorkSpaces Secure Browser

Supporte les rôles de service : Non

Un rôle de service est un IAMrôle qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieurIAM. Pour plus d'informations, consultez la section Création d'un rôle auquel déléguer des autorisations AWS service dans le Guide de IAM l'utilisateur.

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut perturber les fonctionnalités de WorkSpaces Secure Browser. Modifiez les rôles de service uniquement lorsque WorkSpaces Secure Browser fournit des instructions à cet effet.

Rôles liés à un service pour Secure Browser WorkSpaces

Prend en charge les rôles liés aux services : Oui

Un rôle lié à un service est un type de rôle de service lié à un. AWS service Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés au service apparaissent dans votre Compte AWS fichier et appartiennent au service. Un IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.

Pour plus de détails sur la création ou la gestion des rôles liés à un service, consultez la section AWS Services compatibles avec. IAM Recherchez un service dans le tableau qui inclut un `Yes` dans la colonne Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Exemples de politiques basées sur l'identité pour Amazon Secure Browser WorkSpaces

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources WorkSpaces Secure Browser. Ils ne peuvent pas non plus effectuer de tâches en utilisant le AWS Management Console, AWS Command Line Interface (AWS CLI) ou AWS API. Pour autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

Pour savoir comment créer une politique IAM basée sur l'identité à l'aide de ces exemples de documents de JSON stratégie, consultez la section Création de IAM politiques dans le guide de l'IAMutilisateur.

Pour plus de détails sur les actions et les types de ressources définis par WorkSpaces Secure Browser, y compris le ARNs format de chaque type de ressource, consultez la section Actions, ressources et clés de condition pour Amazon WorkSpaces Secure Browser dans le Service Authorization Reference.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console WorkSpaces Secure Browser
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer les ressources WorkSpaces Secure Browser de votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez les politiques AWS gérées ou les politiques AWS gérées pour les fonctions professionnelles dans le Guide de IAM l'utilisateur.
- Appliquer les autorisations du moindre privilège : lorsque vous définissez des autorisations à IAM l'aide de politiques, accordez uniquement les autorisations nécessaires à l'exécution d'une tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation IAM pour appliquer des autorisations, consultez la section Politiques et autorisations IAM dans le guide de IAM l'utilisateur.
- Utilisez des conditions dans IAM les politiques pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques pour limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez rédiger une condition de politique pour spécifier que toutes les demandes doivent être envoyées en utilisantSSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique AWS service, tel que AWS CloudFormation. Pour plus d'informations, voir Éléments IAM JSON de politique : Condition dans le guide de IAM l'utilisateur.
- Utilisez IAM Access Analyzer pour valider vos IAM politiques afin de garantir des autorisations sécurisées et fonctionnelles. IAM Access Analyzer valide les politiques nouvelles et existantes afin qu'elles soient conformes au langage des IAM politiques (JSON) et IAM aux meilleures pratiques. IAMAccess Analyzer fournit plus de 100 vérifications des politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez la section Validation des politiques d'IAMAccess Analyzer dans le guide de IAM l'utilisateur.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des IAM utilisateurs ou un utilisateur root Compte AWS, activez-le MFA pour une sécurité supplémentaire.

Pour exiger le MFA moment où les API opérations sont appelées, ajoutez MFA des conditions à vos politiques. Pour plus d'informations, consultez la section Configuration de l'APIaccès MFA protégé dans le Guide de l'IAMutilisateur.

Pour plus d'informations sur les meilleures pratiques en matière de sécuritéIAM, consultez la section Bonnes pratiques en matière de sécurité IAM dans le Guide de IAM l'utilisateur.

Utilisation de la console WorkSpaces Secure Browser

Pour accéder à la console Amazon WorkSpaces Secure Browser, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher des informations détaillées sur les ressources WorkSpaces Secure Browser de votre Compte AWS. Si vous créez une stratégie basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette stratégie.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui passent des appels uniquement vers le AWS CLI ou le AWS API. Au lieu de cela, autorisez uniquement l'accès aux actions correspondant à l'APIopération qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la console WorkSpaces Secure Browser, associez également le WorkSpaces Secure Browser `ConsoleAccess` ou la politique `ReadOnly` AWS gérée aux entités. Pour plus d'informations, consultez la section Ajouter des autorisations à un utilisateur dans le Guide de IAM l'utilisateur.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux IAM utilisateurs de consulter les politiques intégrées et gérées associées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide du AWS CLI ou. AWS API

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
```

```
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS politiques gérées pour WorkSpaces Secure Browser

Pour ajouter des autorisations aux utilisateurs, aux groupes et aux rôles, il est plus facile d'utiliser des politiques AWS gérées que de les rédiger vous-même. Il faut du temps et de l'expertise pour créer des politiques gérées par le client IAM qui ne fournissent à votre équipe que les autorisations dont elle a besoin. Pour démarrer rapidement, vous pouvez utiliser nos politiques AWS gérées. Ces politiques couvrent les cas d'utilisation courants et sont disponibles dans votre AWS compte. Pour plus d'informations sur les politiques AWS gérées, voir les politiques AWS gérées dans le guide de l'utilisateur IAM.

AWS les services maintiennent et mettent à jour les politiques AWS gérées. Vous ne pouvez pas modifier les autorisations dans les politiques AWS gérées. Les services peuvent parfois ajouter des autorisations supplémentaires à une politique AWS gérée pour prendre en charge de nouvelles

fonctionnalités. Ce type de mise à jour affecte toutes les identités (utilisateurs, groupes et rôles) auxquelles la politique est attachée. Les services sont très susceptibles de mettre à jour une politique gérée par AWS quand une nouvelle fonctionnalité est lancée ou quand de nouvelles opérations sont disponibles. Les services ne suppriment pas les autorisations d'une politique AWS gérée. Les mises à jour des politiques n'endommageront donc pas vos autorisations existantes.

En outre, AWS prend en charge les politiques gérées pour les fonctions professionnelles qui couvrent plusieurs services. Par exemple, la politique `ReadOnlyAccess` AWS gérée fournit un accès en lecture seule à tous les AWS services et ressources. Lorsqu'un service lance une nouvelle fonctionnalité, il AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour obtenir la liste des politiques de fonctions professionnelles et leurs descriptions, consultez la page politiques gérées par AWS pour les fonctions de tâche dans le Guide de l'utilisateur IAM.

AWS politique gérée : AmazonWorkSpacesWebServiceRolePolicy

Vous ne pouvez pas associer `AmazonWorkSpacesWebServiceRolePolicy` à vos entités IAM. Cette politique est associée à un rôle lié à un service qui permet à WorkSpaces Secure Browser d'effectuer des actions en votre nom. Pour plus d'informations, consultez the section called "Utilisation des rôles liés à un service".

Cette politique accorde des autorisations administratives qui permettent d'accéder aux AWS services et aux ressources utilisés ou gérés par WorkSpaces Secure Browser.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `workspaces-web`— Permet d'accéder aux AWS services et aux ressources utilisés ou gérés par WorkSpaces Secure Browser.
- `ec2` – Permet aux principaux de décrire les VPC, les sous-réseaux et les zones de disponibilité ; de créer, baliser, décrire et supprimer des interfaces réseau ; d'associer ou dissocier une adresse ; et de décrire les tables de routage, les groupes de sécurité et les points de terminaison de VPC.

- `CloudWatch` – Permet aux principaux de placer des données de métriques.
- `Kinesis` – Permet aux principaux de décrire un résumé des flux de données Kinesis et de placer des enregistrements dans les flux de données Kinesis pour la journalisation des accès utilisateur. Pour plus d'informations, consultez the section called "Configuration de la journalisation des accès utilisateur".

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaces",
                "ec2:AssociateAddress",
                "ec2:DisassociateAddress",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcEndpoints"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:security-group/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
```

```
                "StringEquals": {
                    "aws:RequestTag/WorkSpacesWebManaged": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "WorkSpacesWebManaged"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/WorkSpacesWebManaged": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": [
                        "AWS/WorkSpacesWeb",
```

```
                        "AWS/Usage"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "kinesis:PutRecord",
                "kinesis:PutRecords",
                "kinesis:DescribeStreamSummary"
            ],
            "Resource": "arn:aws:kinesis:*:*:stream/amazon-workspaces-web-*"
        }
    ]
}
```

AWS politique gérée : AmazonWorkSpacesSecureBrowserReadOnly

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

Cette politique accorde des autorisations en lecture seule qui permettent d'accéder à WorkSpaces Secure Browser et à ses dépendances via la console de AWS gestion, le SDK et la CLI. Cette politique n'inclut pas les autorisations nécessaires pour interagir avec les portails utilisant le type d'authentification `IAM_Identity_Center`. Pour obtenir ces autorisations, combinez cette politique avec `AWSSSOReadOnly`.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `workspaces-web`— Fournit un accès en lecture seule à WorkSpaces Secure Browser et à ses dépendances via la console de AWS gestion, le SDK et la CLI.
- `ec2` – Permet aux principaux de décrire les VPC, les sous-réseaux et les groupes de sécurité. Ceci est utilisé dans la console AWS de gestion de WorkSpaces Secure Browser pour afficher vos VPC, sous-réseaux et groupes de sécurité disponibles pour une utilisation avec le service.

- `Kinesis` – Permet aux principaux de lister les flux de données Kinesis. Il est utilisé dans la console de AWS gestion de WorkSpaces Secure Browser pour afficher les flux de données Kinesis disponibles avec le service.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "workspaces-web:GetBrowserSettings",
                "workspaces-web:GetIdentityProvider",
                "workspaces-web:GetNetworkSettings",
                "workspaces-web:GetPortal",
                "workspaces-web:GetPortalServiceProviderMetadata",
                "workspaces-web:GetTrustStore",
                "workspaces-web:GetTrustStoreCertificate",
                "workspaces-web:GetUserSettings",
                "workspaces-web:GetUserAccessLoggingSettings",
                "workspaces-web:ListBrowserSettings",
                "workspaces-web:ListIdentityProviders",
                "workspaces-web:ListNetworkSettings",
                "workspaces-web:ListPortals",
                "workspaces-web:ListTagsForResource",
                "workspaces-web:ListTrustStoreCertificates",
                "workspaces-web:ListTrustStores",
                "workspaces-web:ListUserSettings",
                "workspaces-web:ListUserAccessLoggingSettings"
            ],
            "Resource": "arn:aws:workspaces-web:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "kinesis:ListStreams"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

AWS politique gérée : AmazonWorkSpacesWebReadOnly

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

Cette politique accorde des autorisations en lecture seule qui permettent d'accéder à WorkSpaces Secure Browser et à ses dépendances via la console de AWS gestion, le SDK et la CLI. Cette politique n'inclut pas les autorisations nécessaires pour interagir avec les portails utilisant le type d'authentification `IAM_Identity_Center`. Pour obtenir ces autorisations, combinez cette politique avec `AWSSSOReadOnly`.

> **Note**
>
> Si vous utilisez actuellement cette politique, passez à la nouvelle `AmazonWorkSpacesSecureBrowserReadOnly` politique.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `workspaces-web`— Fournit un accès en lecture seule à WorkSpaces Secure Browser et à ses dépendances via la console de AWS gestion, le SDK et la CLI.
- `ec2` – Permet aux principaux de décrire les VPC, les sous-réseaux et les groupes de sécurité. Ceci est utilisé dans la console AWS de gestion de WorkSpaces Secure Browser pour afficher vos VPC, sous-réseaux et groupes de sécurité disponibles pour une utilisation avec le service.
- `Kinesis` – Permet aux principaux de lister les flux de données Kinesis. Il est utilisé dans la console de AWS gestion de WorkSpaces Secure Browser pour afficher les flux de données Kinesis disponibles avec le service.

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

```
        {
            "Effect": "Allow",
            "Action": [
                "workspaces-web:GetBrowserSettings",
                "workspaces-web:GetIdentityProvider",
                "workspaces-web:GetNetworkSettings",
                "workspaces-web:GetPortal",
                "workspaces-web:GetPortalServiceProviderMetadata",
                "workspaces-web:GetTrustStore",
                "workspaces-web:GetTrustStoreCertificate",
                "workspaces-web:GetUserSettings",
                "workspaces-web:GetUserAccessLoggingSettings",
                "workspaces-web:ListBrowserSettings",
                "workspaces-web:ListIdentityProviders",
                "workspaces-web:ListNetworkSettings",
                "workspaces-web:ListPortals",
                "workspaces-web:ListTagsForResource",
                "workspaces-web:ListTrustStoreCertificates",
                "workspaces-web:ListTrustStores",
                "workspaces-web:ListUserSettings",
                "workspaces-web:ListUserAccessLoggingSettings"
            ],
            "Resource": "arn:aws:workspaces-web:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "kinesis:ListStreams"
            ],
            "Resource": "*"
        }
    ]
}
```

WorkSpaces Mises à jour des politiques AWS gérées par Secure Browser

Consultez les détails des mises à jour des politiques AWS gérées pour WorkSpaces Secure Browser depuis que ce service a commencé à suivre ces modifications. Pour obtenir des alertes automatiques

sur les modifications apportées à cette page, abonnez-vous au flux RSS de la page Historique de la documentation.

Modification	Description	Date
AmazonWorkSpacesSecureBrowserReadOnly : nouvelle politique	WorkSpaces Secure Browser a ajouté une nouvelle politique pour fournir un accès en lecture seule à WorkSpaces Secure Browser et à ses dépendances via la console de gestion AWS, le SDK et la CLI.	24 juin 2024
AmazonWorkSpacesWebServiceRolePolicy— Politique mise à jour	WorkSpaces Secure Browser a mis à jour la politique CreateNetworkInterface afin de limiter les balises avec aws :RequestTag/WorkSpacesWebManaged: true et d'agir sur les ressources des sous-réseaux et des groupes de sécurité, ainsi que de se limiter DeleteNetworkInterface aux ENI marqués avec aws :ResourceTag/WorkSpacesWebManaged: true.	15 décembre 2022
AmazonWorkSpacesWebReadOnly— Politique mise à jour	WorkSpaces Secure Browser a mis à jour la politique afin d'inclure des autorisations de lecture pour la journalisation des accès des utilisateurs et de répertorier les flux de données Kinesis. Pour plus d'informations, consultez the section called "Configuration	2 novembre 2022

Modification	Description	Date
	de la journalisation des accès utilisateur".	
AmazonWorkSpacesWebServiceRolePolicy— Politique mise à jour	WorkSpaces Secure Browser a mis à jour la politique afin de décrire un résumé des flux de données Kinesis et de placer des enregistrements dans les flux de données Kinesis pour la journalisation des accès des utilisateurs. Pour plus d'informations, consultez the section called "Configuration de la journalisation des accès utilisateur".	17 octobre 2022
AmazonWorkSpacesWebServiceRolePolicy— Politique mise à jour	WorkSpaces Secure Browser a mis à jour la politique de création de balises lors de la création de l'ENI.	6 septembre 2022
AmazonWorkSpacesWebServiceRolePolicy— Politique mise à jour	WorkSpaces Secure Browser a mis à jour la politique pour ajouter l'espace de noms AWS/Usage aux autorisations d'API. PutMetricData	6 avril 2022
AmazonWorkSpacesWebReadOnly : nouvelle politique	WorkSpaces Secure Browser a ajouté une nouvelle politique pour fournir un accès en lecture seule à WorkSpaces Secure Browser et à ses dépendances via la console de gestion AWS, le SDK et la CLI.	30 novembre 2021

Modification	Description	Date
AmazonWorkSpacesWebServiceRolePolicy : nouvelle politique	WorkSpaces Secure Browser a ajouté une nouvelle politique pour autoriser l'accès aux services et ressources AWS utilisés ou gérés par WorkSpaces Secure Browser.	30 novembre 2021
WorkSpaces Secure Browser a commencé à suivre les modifications	WorkSpaces Secure Browser a commencé à suivre les modifications apportées AWS à ses politiques gérées.	30 novembre 2021

Résolution des problèmes d'identité et d'accès à Amazon WorkSpaces Secure Browser

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lors de l'utilisation de WorkSpaces Secure Browser etIAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans WorkSpaces Secure Browser
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder aux ressources de mon navigateur WorkSpaces sécurisé

Je ne suis pas autorisé à effectuer une action dans WorkSpaces Secure Browser

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

L'exemple d'erreur suivant se produit lorsque l'`mateojacksonIAM`utilisateur essaie d'utiliser la console pour afficher les détails d'une *`my-example-widget`* ressource fictive mais ne dispose pas des `workspaces-web:`*`GetWidget`* autorisations fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 workspaces-web:GetWidget on resource: my-example-widget
```

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

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

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à WorkSpaces Secure Browser.

Certains vous AWS services permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un IAM utilisateur nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans WorkSpaces Secure Browser. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

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

Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder aux ressources de mon navigateur WorkSpaces sécurisé

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez

spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si WorkSpaces Secure Browser prend en charge ces fonctionnalités, consultezComment fonctionne Amazon WorkSpaces Secure Browser avec IAM.
- Pour savoir comment donner accès à vos ressources sur un site Comptes AWS qui vous appartient, consultez la section Fournir l'accès à un IAM utilisateur dans un autre site Compte AWS que vous possédez dans le Guide de IAM l'utilisateur.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le Guide de IAM l'utilisateur.
- Pour savoir comment fournir un accès via la fédération d'identité, consultez la section Fournir un accès aux utilisateurs authentifiés de manière externe (fédération d'identité) dans le guide de l'IAMutilisateur.
- Pour connaître la différence entre l'utilisation de rôles et l'utilisation de politiques basées sur les ressources pour l'accès entre comptes, voir Accès aux ressources entre comptes IAM dans le guide de l'IAMutilisateur.

Utilisation de rôles liés à un service pour Secure Browser WorkSpaces

Amazon WorkSpaces Secure Browser utilise des rôles AWS Identity and Access Management liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à WorkSpaces Secure Browser. Les rôles liés au service sont prédéfinis par WorkSpaces Secure Browser et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration de WorkSpaces Secure Browser car il n'est pas nécessaire d'ajouter manuellement les autorisations nécessaires. WorkSpaces Secure Browser définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul WorkSpaces Secure Browser peut assumer ses rôles. Les autorisations définies comprennent les politiques d'approbation et d'autorisations. La politique d'autorisations ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège les ressources de votre navigateur WorkSpaces sécurisé car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés aux services, consultez Services AWS fonctionnant avec IAM et recherchez les services où Oui figure dans la colonne Rôle lié à un service. Choisissez un Yes (oui) ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées au service pour Secure Browser WorkSpaces

WorkSpaces Secure Browser utilise le rôle lié au service nommé `AWSServiceRoleForAmazonWorkSpacesWeb` — WorkSpaces Secure Browser utilise ce rôle lié au service pour accéder aux ressources Amazon EC2 des comptes clients pour les instances de streaming et les métriques. CloudWatch

Le rôle lié à un service `AWSServiceRoleForAmazonWorkSpacesWeb` approuve les services suivants pour endosser le rôle :

- `workspaces-web.amazonaws.com`

La politique d'autorisation de rôle nommée `AmazonWorkSpacesWebServiceRolePolicy` permet à WorkSpaces Secure Browser d'effectuer les actions suivantes sur les ressources spécifiées. Pour plus d'informations, consultez the section called "AmazonWorkSpacesWebServiceRolePolicy".

- Action : `ec2:DescribeVpcs` sur `all AWS resources`
- Action : `ec2:DescribeSubnets` sur `all AWS resources`
- Action : `ec2:DescribeAvailabilityZones` sur `all AWS resources`
- Action : `ec2:CreateNetworkInterface` avec `aws:RequestTag/WorkSpacesWebManaged: true` sur les ressources de sous-réseau et de groupe de sécurité
- Action : `ec2:DescribeNetworkInterfaces` sur `all AWS resources`
- Action : `ec2:DeleteNetworkInterface` sur les interfaces réseau avec `aws:ResourceTag/WorkSpacesWebManaged: true`
- Action : `ec2:DescribeSubnets` sur `all AWS resources`
- Action : `ec2:AssociateAddress` sur `all AWS resources`
- Action : `ec2:DisassociateAddress` sur `all AWS resources`

- Action : `ec2:DescribeRouteTables` sur `all AWS resources`
- Action : `ec2:DescribeSecurityGroups` sur `all AWS resources`
- Action : `ec2:DescribeVpcEndpoints` sur `all AWS resources`
- Action : `ec2:CreateTags` sur l'opération `ec2:CreateNetworkInterface` avec `aws:TagKeys: ["WorkSpacesWebManaged"]`
- Action : `cloudwatch:PutMetricData` sur `all AWS resources`
- Action : `kinesis:PutRecord` sur les flux de données Kinesis dont le nom commence par `amazon-workspaces-web-`
- Action : `kinesis:PutRecords` sur les flux de données Kinesis dont le nom commence par `amazon-workspaces-web-`
- Action : `kinesis:DescribeStreamSummary` sur les flux de données Kinesis dont le nom commence par `amazon-workspaces-web-`

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Service-Linked Role Permissions (autorisations du rôle lié à un service) dans le IAM User Guide (guide de l'utilisateur IAM).

Création d'un rôle lié à un service pour Secure Browser WorkSpaces

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez votre premier portail dans le AWS Management Console, le ou l' AWS API AWS CLI, WorkSpaces Secure Browser crée le rôle lié au service pour vous.

> **Important**
>
> Ce rôle lié à un service peut apparaître dans votre compte si vous avez effectué une action dans un autre service qui utilise les fonctions prises en charge par ce rôle.

Si vous supprimez ce rôle lié à un service et que vous avez besoin de le recréer par la suite, vous pouvez reprendre cette même procédure pour recréer le rôle dans votre compte. Lorsque vous créez votre premier portail, WorkSpaces Secure Browser crée à nouveau le rôle lié au service pour vous.

Vous pouvez également utiliser la console IAM pour créer un rôle lié à un service avec le cas d'utilisation de WorkSpaces Secure Browser. Dans l'API AWS CLI ou dans l' AWS API, créez

un rôle lié à un service avec le nom du `workspaces-web.amazonaws.com` service. Pour plus d'informations, consultez Création d'un rôle lié à un service dans le Guide de l'utilisateur IAM. Si vous supprimez ce rôle lié à un service, vous pouvez utiliser ce même processus pour créer le rôle à nouveau.

Modification d'un rôle lié à un service pour Secure Browser WorkSpaces

WorkSpaces Secure Browser ne vous permet pas de modifier le rôle `AWSServiceRoleForAmazonWorkSpacesWeb` lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence au rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Supprimer un rôle lié à un service pour Secure Browser WorkSpaces

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

> **Note**
>
> Si le service WorkSpaces Secure Browser utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les ressources WorkSpaces Secure Browser utilisées par le AWSServiceRoleForAmazonWorkSpacesWeb

- Choisissez l'une des solutions suivantes :
  - Si vous utilisez la console, supprimez tous vos portails sur la console.
  - Si vous utilisez l'interface CLI ou l'API, dissociez toutes vos ressources (notamment les paramètres de navigateur, les paramètres réseau, les paramètres utilisateur, les magasins de confiance et les paramètres de journalisation des accès utilisateur) de vos portails, supprimez ces ressources, puis supprimez les portails.

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM AWS CLI, le ou l' AWS API pour supprimer le rôle lié au AWSServiceRoleForAmazonWorkSpacesWeb service. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les WorkSpaces rôles liés au service Secure Browser

WorkSpaces Secure Browser prend en charge l'utilisation de rôles liés à un service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez Régions et Points de terminaison AWS.

Réponse aux incidents dans Amazon WorkSpaces Secure Browser

Vous pouvez détecter les incidents en surveillant la CloudWatch métrique `SessionFailure` Amazon. Pour recevoir des alertes en cas d'incident, utilisez une CloudWatch alarme pour la `SessionFailure` métrique. Pour plus d'informations, voir Surveillance d'Amazon WorkSpaces Secure Browser avec Amazon CloudWatch.

Validation de conformité pour Amazon WorkSpaces Secure Browser

Pour savoir si un programme AWS services de conformité AWS service s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez AWS services la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

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

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

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

> **Note**
>
> Tous ne AWS services sont pas HIPAA éligibles. Pour plus d'informations, consultez la référence des services HIPAA éligibles.

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

Résilience dans Amazon WorkSpaces Secure Browser

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones

de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Les éléments suivants ne sont actuellement pas pris en charge par WorkSpaces Secure Browser :

- Sauvegarde de contenu entre différentes zones géographiques ou régions
- Sauvegardes chiffrées
- Chiffrement du contenu en transit entre différentes zones de disponibilité ou régions
- Sauvegardes par défaut ou automatiques

Pour bénéficier d'une haute disponibilité Internet, vous pouvez ajuster la configuration de votre VPC. Pour une haute disponibilité d'API, vous pouvez demander la quantité de transactions par seconde (TPS) appropriée.

Sécurité de l'infrastructure dans Amazon WorkSpaces Secure Browser

En tant que service géré, Amazon WorkSpaces Secure Browser est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez les API appels AWS publiés pour accéder à Amazon WorkSpaces Secure Browser via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Sécurité de la couche de transport (TLS). Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Des suites de chiffrement parfaitement confidentielles (PFS) telles que (Ephemeral Diffie-Hellman) ou DHE ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

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

WorkSpaces Secure Browser isole le trafic des services en appliquant l'authentification et l'autorisation AWS Sigv4 standard à tous les services. Le point de terminaison de ressource du client (ou point de terminaison de portail web) est protégé par votre fournisseur d'identité. Vous pouvez renforcer l'isolement du trafic en utilisant l'autorisation multifactorielle et un autre mécanisme de sécurité au niveau de votre fournisseur d'identité (IdP).

Tous les accès à Internet peuvent être contrôlés en configurant les paramètres réseau, tels que le VPC sous-réseau ou le groupe de sécurité. La mutualisation et les VPC points de terminaison (PrivateLink) ne sont actuellement pas pris en charge.

Analyse de configuration et de vulnérabilité dans Amazon WorkSpaces Secure Browser

WorkSpaces Secure Browser met à jour et corrige les applications et les plateformes selon vos besoins, notamment Chrome et Linux. Vous n'êtes pas tenu de corriger ou de reconstruire. Cependant, il est de votre responsabilité de configurer WorkSpaces Secure Browser conformément aux spécifications et directives, et de surveiller l'utilisation de WorkSpaces Secure Browser par vos utilisateurs. Toutes les configurations liées au service et les analyses de vulnérabilité relèvent de la responsabilité de WorkSpaces Secure Browser.

Vous pouvez demander une augmentation des limites pour les ressources de WorkSpaces Secure Browser, telles que le nombre de portails Web et le nombre d'utilisateurs. WorkSpaces Secure Browser garantit la disponibilité du service et du SLA.

Bonnes pratiques de sécurité pour Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser fournit un certain nombre de fonctionnalités de sécurité que vous pouvez utiliser lorsque vous développez et mettez en œuvre vos propres politiques de sécurité. Les bonnes pratiques suivantes doivent être considérées comme des instructions générales et ne représentent pas une solution de sécurité complète. Étant donné que ces bonnes pratiques

peuvent ne pas être appropriées ou suffisantes pour votre environnement, considérez-les comme des remarques utiles plutôt que comme des recommandations.

Les meilleures pratiques pour Amazon WorkSpaces Secure Browser sont les suivantes :

- Pour détecter les événements de sécurité potentiels associés à votre utilisation de WorkSpaces Secure Browser, utilisez AWS CloudTrail Amazon CloudWatch pour détecter et suivre l'historique des accès et les journaux de traitement. Pour plus d'informations, consultez Surveillance d'Amazon WorkSpaces Secure Browser avec Amazon CloudWatch et Journalisation des appels d'API WorkSpaces Secure Browser à l'aide de AWS CloudTrail.
- Pour mettre en œuvre des contrôles de détection et identifier les anomalies, utilisez CloudTrail des journaux et CloudWatch des métriques. Pour plus d'informations, consultez Surveillance d'Amazon WorkSpaces Secure Browser avec Amazon CloudWatch et Journalisation des appels d'API WorkSpaces Secure Browser à l'aide de AWS CloudTrail.
- Vous pouvez configurer la journalisation des accès utilisateur pour enregistrer les événements utilisateur. Pour plus d'informations, consultez the section called "Configuration de la journalisation des accès utilisateur".

Pour éviter les événements de sécurité potentiels associés à votre utilisation de WorkSpaces Secure Browser, suivez les meilleures pratiques suivantes :

- Implémentez l'accès avec le moindre privilège et créez des rôles spécifiques à utiliser pour les actions de WorkSpaces Secure Browser. Utilisez des modèles IAM pour créer un rôle en accès complet ou en lecture seule. Pour plus d'informations, consultez AWS politiques gérées pour WorkSpaces Secure Browser.
- Faites preuve de prudence lorsque vous partagez des domaines de portail et des informations d'identification utilisateur. Toute personne sur Internet peut accéder au portail web, mais elle ne peut pas y démarrer une session sans disposer d'informations d'identification utilisateur valides. Faites attention à la façon dont vous partagez les informations d'identification du portail web, au moment et avec qui vous le faites.

Surveillance du navigateur Amazon WorkSpaces Secure

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'Amazon WorkSpaces Secure Browser et de vos autres AWS solutions. AWS fournit les outils de surveillance suivants pour surveiller vos portails WorkSpaces Secure Browser et leurs ressources, signaler tout problème et prendre des mesures automatiques le cas échéant :

- Amazon CloudWatch surveille vos AWS ressources et les applications que vous utilisez AWS en temps réel. Vous pouvez collecter et suivre des métriques, créer des tableaux de bord personnalisés et définir des alarmes qui vous informent ou prennent des mesures lorsqu'une métrique spécifique atteint un seuil déterminé. Par exemple, vous pouvez CloudWatch suivre l'utilisation du processeur ou d'autres indicateurs pour vos instances Amazon EC2 et lancer automatiquement de nouvelles instances en cas de besoin. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.
- Amazon CloudWatch Logs vous permet de surveiller, de stocker et d'accéder à vos fichiers journaux à partir d'instances Amazon EC2 et d'autres sources. CloudTrail CloudWatch Les journaux peuvent surveiller les informations contenues dans les fichiers journaux et vous avertir lorsque certains seuils sont atteints. Vous pouvez également archiver vos données de journaux dans une solution de stockage hautement durable. Pour plus d'informations, consultez le guide de l'utilisateur d'Amazon CloudWatch Logs.
- AWS CloudTrailcapture les appels d'API et les événements associés effectués par ou pour le compte de votre AWS compte et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Pour plus d'informations, consultez le Guide de l'utilisateur AWS CloudTrail.

Rubriques

Surveillance d'Amazon WorkSpaces Secure Browser avec Amazon CloudWatch

Vous pouvez surveiller Amazon WorkSpaces Secure Browser à l'aide de ce dernier CloudWatch, qui collecte les données brutes et les traite en indicateurs lisibles en temps quasi réel. Ces statistiques sont enregistrées pour une durée de 15 mois ; par conséquent, vous pouvez accéder aux informations historiques et acquérir un meilleur point de vue de la façon dont votre service ou application web s'exécute. Vous pouvez également définir des alarmes qui surveillent certains seuils et envoient des notifications ou prennent des mesures lorsque ces seuils sont atteints. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

L'espace de noms `AWS/WorkSpacesWeb` inclut les métriques suivantes.

CloudWatch statistiques pour Amazon WorkSpaces Secure Browser

Métrique	Description	Dimensions	Statistiques	Unités
`SessionAttempt`	Le nombre de tentatives de session Amazon WorkSpaces Secure Browser.	`PortalId`	Moyenne, Somme, Maximum, Minimum	Nombre
`SessionSuccess`	Le nombre de sessions Amazon WorkSpaces Secure Browser démarrées avec succès.	`PortalId`	Moyenne, Somme, Maximum, Minimum	Nombre
`SessionFailure`	Le nombre de démarrages d'une session Amazon WorkSpaces Secure Browser ayant échoué.	`PortalId`	Moyenne, Somme, Maximum, Minimum	Nombre

Métrique	Description	Dimensions	Statistiques	Unités
`GlobalCpuPercent`	L'utilisation du processeur de l'instance de session Amazon WorkSpaces Secure Browser.	`PortalId`	Moyenne, Somme, Maximum, Minimum	Pourcentage
`GlobalMemoryPercent`	L'utilisation de la mémoire (RAM) de l'instance de session Amazon WorkSpaces Secure Browser.	`PortalId`	Moyenne, Somme, Maximum, Minimum	Pourcentage

> **Note**
>
> Vous pouvez consulter la statistique métrique « SampleCount » pour `GlobalCpuPercent` ou `GlobalMemoryPercent` pour déterminer le nombre de sessions simultanées actives sur votre portail. Les points de données sont émis par chaque session une fois par minute.

Journalisation des appels d'API WorkSpaces Secure Browser à l'aide de AWS CloudTrail

WorkSpaces Secure Browser est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions effectuées par un utilisateur, un rôle ou un AWS service dans Amazon WorkSpaces Secure Browser. CloudTrail capture tous les appels d'API pour Amazon WorkSpaces Secure Browser sous forme d'événements. Il s'agit notamment des appels depuis la console Amazon WorkSpaces Secure Browser et des appels de code vers les opérations de l'API Amazon WorkSpaces Secure Browser. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Amazon WorkSpaces Secure Browser. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez identifier la demande envoyée à Amazon WorkSpaces Secure

Browser, l'adresse IP à partir de laquelle la demande a été faite, l'auteur de la demande, la date à laquelle elle a été faite, ainsi que des informations supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

WorkSpaces Informations relatives au navigateur sécurisé dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité se produit dans Amazon WorkSpaces Secure Browser, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Dans l'historique des événements, vous pouvez consulter, rechercher et télécharger les événements récents de votre AWS compte. Pour plus d'informations, consultez la section Affichage des événements à l'aide de l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre AWS compte, y compris des événements relatifs à Amazon WorkSpaces Secure Browser, vous pouvez créer un suivi. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal de suivi dans la console, il s'applique à toutes les régions AWS. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Présentation de la création d'un journal de suivi
- CloudTrail services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes les actions d'Amazon WorkSpaces Secure Browser sont enregistrées CloudTrail et documentées dans le Amazon WorkSpaces API Reference. Par exemple, les appels au `CreatePortal` `DeleteUserSettings` et les `ListBrowserSettings` actions génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été effectuée avec des informations d'identification d'utilisateur root ou IAM.

- Si la demande a été effectuée avec des informations d'identification de sécurité temporaires pour un rôle ou un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour plus d'informations, consultez l'élément CloudTrail UserIdentity.

Comprendre les entrées du fichier journal de WorkSpaces Secure Browser

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande et d'autres détails. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`ListBrowserSettings`action.


```
{
   "Records": [{
       "eventVersion": "1.08",
       "userIdentity": {
           "type": "IAMUser",
           "principalId": "111122223333",
           "arn": "arn:aws:iam::111122223333:user/myUserName",
           "accountId": "111122223333",
           "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
           "userName": "myUserName"
       },
       "eventTime": "2021-11-17T23:44:51Z",
       "eventSource": "workspaces-web.amazonaws.com",
       "eventName": "ListBrowserSettings",
       "awsRegion": "us-west-2",
       "sourceIPAddress": "127.0.0.1",
       "userAgent": "[]",
       "requestParameters": null,
       "responseElements": null,
       "requestID": "159d5c4f-c8c8-41f1-9aee-b5b1b632e8b2",
       "eventID": "d8237248-0090-4c1e-b8f0-a6e8b18d63cb",
       "readOnly": true,
```

```
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "111122223333",
        "eventCategory": "Management"
    },
    {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "111122223333",
            "arn": "arn:aws:iam::111122223333:user/myUserName",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "userName": "myUserName"
        },
        "eventTime": "2021-11-17T23:55:51Z",
        "eventSource": "workspaces-web.amazonaws.com",
        "eventName": "CreateUserSettings",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "5127.0.0.1",
        "userAgent": "[]",
        "requestParameters": {
            "clientToken": "some-token",
            "copyAllowed": "Enabled",
            "downloadAllowed": "Enabled",
            "pasteAllowed": "Enabled",
            "printAllowed": "Enabled",
            "uploadAllowed": "Enabled"
        },
        "responseElements": "arn:aws:workspaces-web:us-
west-2:111122223333:userSettings/04a35a2d-f7f9-4b22-af08-8ec72da9c2e2",
        "requestID": "6a4aa162-7c1b-4cf9-a7ac-e0c8c4622117",
        "eventID": "56f1fbee-6a1d-4fc6-bf35-a3a71f016fcb",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "111122223333",
        "eventCategory": "Management"
    }]
}
```

Journalisation des accès utilisateur

Amazon WorkSpaces Secure Browser permet aux clients d'enregistrer les événements de session, notamment le démarrage, l'arrêt et les visites d'URL. Ces journaux sont transmis à un flux de données Amazon Kinesis que vous spécifiez pour votre portail web. Pour plus d'informations, voir the section called “Configuration de la journalisation des accès utilisateur”.

Conseils pour les utilisateurs de WorkSpaces Secure Browser

Les administrateurs utilisent WorkSpaces Secure Browser pour créer des portails Web qui se connectent aux sites Web de l'entreprise, tels que les sites Web internes, les applications Web software-as-a-service (SAAS) ou Internet. Les utilisateurs finaux se servent alors de leur navigateur web existant pour accéder à ces portails web, lancer une session et accéder à du contenu.

Le contenu suivant aide les utilisateurs finaux qui souhaitent en savoir plus sur l'accès à WorkSpaces Secure Browser, le lancement et la configuration d'une session, ainsi que sur l'utilisation de la barre d'outils et du navigateur Web.

Rubriques

Compatibilité des navigateurs et des appareils

Amazon WorkSpaces Secure Browser est alimenté par le client de navigateur Web NICE DCV, qui s'exécute dans un navigateur Web. Aucune installation n'est donc requise. Le client de navigateur web est pris en charge par les navigateurs web courants, tels que Chrome et Firefox, et par les principaux systèmes d'exploitation de bureau, tels que Windows, macOS et Linux.

Pour plus de up-to-date détails sur la prise en charge des clients de navigateur Web, consultez la section Client de navigateur Web.

> **Note**
>
> Pour l'heure, les webcams sont uniquement prises en charge dans les navigateurs basés sur Chromium, comme Google Chrome et Microsoft Edge. Actuellement, Apple Safari et Mozilla ne prennent FireFox pas en charge la webcam.

Accès au portail web

Votre administrateur dispose des méthodes suivantes pour vous donner accès à votre portail web :

- Vous pouvez sélectionner un lien dans un e-mail ou un site web, puis vous connecter à l'aide de vos informations d'identification SAML.
- Vous pouvez vous connecter à votre fournisseur d'identité SAML (comme Okta, Ping ou Azure) et lancer une session en un clic depuis la page d'accueil de l'application de votre fournisseur SAML (comme Okta End-User Dashboard ou le portail Azure My Apps).

Conseils relatifs aux sessions

Après vous être connecté au portail web, vous pouvez lancer une session et effectuer diverses actions.

Rubriques

Démarrer une session

Après vous être connecté pour lancer une session, le message Lancement de la session s'affiche avec une barre de progression. Cela indique qu'Amazon WorkSpaces Secure Browser est en train de créer une session pour vous. Dans les coulisses, Amazon WorkSpaces Secure Browser crée l'instance, lance le navigateur Web géré et applique les paramètres d'administrateur et les politiques du navigateur.

Si vous vous connectez à votre portail web pour la première fois, des icônes + de couleur bleue figurent dans la barre d'outils. Leur présence indique qu'il existe un tutoriel qui fait le tour des différentes fonctionnalités disponibles dans la barre d'outils. Vous pouvez utiliser ces icônes pour savoir comment :

- Autoriser le navigateur à accéder au micro, à la webcam et au presse-papiers en sélectionnant l'icône de cadenas en regard côté de votre navigateur local et en mettant le commutateur en position Activé en regard du presse-papiers, du micro et de la caméra.

  > **Note**
  >
  > Lorsque vous autorisez la webcam au début de votre première session, la webcam s'active brièvement et un voyant se met à clignoter sur votre ordinateur. Il s'agit de la procédure qui octroie au navigateur local un accès à votre webcam.

- Activez Amazon WorkSpaces Secure Browser pour lancer des fenêtres de surveillance supplémentaires en sélectionnant l'icône représentant un cadenas dans votre navigateur et en configurant Toujours autoriser les fenêtres contextuelles.

Si vous souhaitez relancer un tutoriel, vous pouvez sélectionner Profil dans la barre d'outils, Aide, puis Lancer le tutoriel.

Utiliser la barre d'outils

Pour déplacer la barre d'outils, sélectionnez la barre la plus claire dans la partie supérieure de la barre d'outils, faites-la glisser vers l'emplacement souhaité, puis relâchez-la pour la déposer.

Pour réduire la barre d'outils, passez la souris dessus et sélectionnez le bouton flèche vers le haut, ou double-cliquez sur la barre plus claire dans la section supérieure. La vue réduite vous offre plus d'espace sur l'écran et vous permet d'accéder en un clic aux icônes les plus fréquemment utilisées.

Pour augmenter la taille de l'écran, sélectionnez la fenêtre du navigateur et zoomez. Pour augmenter la taille d'affichage des icônes et du texte de la barre d'outils, sélectionnez la barre d'outils et zoomez.

Pour effectuer un zoom avant ou arrière sur un appareil Windows, procédez comme suit :

1. Sélectionnez la barre d'outils ou le contenu Web.
2. Appuyez sur Ctrl + pour zoomer ou sur Ctrl + - pour effectuer un zoom arrière.

Pour effectuer un zoom avant ou arrière sur un appareil Mac, procédez comme suit :

1. Sélectionnez la barre d'outils ou le contenu Web.
2. Appuyez sur Cmd + + pour zoomer ou sur Cmd + - pour effectuer un zoom arrière.

Pour ancrer la barre d'outils en haut de l'écran, choisissez Préférences, Général et Ancré en mode barre d'outils.

Le tableau suivant décrit toutes les icônes disponibles dans la barre d’outils :

Icon	Title	Description
	**Windows**	Move between windows or launch additional browser windows.
	**Launch additional monitor window**	Launch an additional monitor window with a separate browser window. Then drag to your secondary monitor.
	**Full screen**	Launch a full screen experience view.
	**Microphone**	Activate mic input for the session.
	**Preferences**	Access the **General** and **Keyboard** menus. From the **General** menu, toggle between light and dark mode, activate the keyboard input selector (for changing the keyboard language), and switch between streaming mode or display resolution. From the **Keyboard** menu, change the option and command key settings (on Mac devices), or activate **Functions** (see below).
	**Profile**	End your session, view performance metrics, access **Feedback** and **Help**, and learn about Amazon WorkSpaces Web. **End Session** ends the Amazon WorkSpaces Web session. **Performance metrics** displays the frame rate, network latency, and bandwidth usage graph. This information is useful for administrators when investigating issues with the service. **Feedback** provides you with an email address to share feedback to the Amazon WorkSpaces Web team. **Help** provides you with access to Frequently Asked Questions, such as how to use the clipboard, microphone, and webcam during the session, or how to troubleshoot launching an additional monitor window. From help, you can also launch the tutorial or user guide. **About** provides more information about Amazon WorkSpaces Web.
	**Notifications**	Get one-click access to session notifications.
	**Clipboard**	Access clipboard shortcut descriptions, links to set the command key preference, and troubleshoot clipboard permissions from the local web browser. You can use the content preview text box to test clipboard functionality. This icon only displays if clipboard permission is granted by your administator.
	**Files**	From the files menu, you can upload content to the remote browser. Once uploaded, you can rename, download, or delete, as well as create folders in the temporary file menu. All files and data in **Files** are deleted at the end of the session. This icon only displays if **Files** permission is granted by your administator.

> **Note**
>
> Les icônes Presse-papiers et Fichiers sont masquées par défaut, sauf si votre administrateur accorde ces autorisations. Seuls les administrateurs peuvent activer ou désactiver les icônes Presse-papiers et Fichiers sur un portail web. Si ces icônes sont masquées et que vous avez besoin d'y accéder, contactez votre administrateur.

Utilisation du navigateur

Lorsque vous démarrez votre session, le navigateur affiche l'URL de démarrage, qui est une URL choisie par votre administrateur. Si l'administrateur n'a pas choisi d'URL de démarrage, vous voyez la nouvelle expérience d'onglets par défaut de Google Chrome.

Depuis le navigateur, vous pouvez ouvrir des onglets, lancer des fenêtres de navigation supplémentaires (à partir de l'icône de barre d'outils Windows ou du menu à trois points du navigateur), saisir une URL ou effectuer une recherche dans la barre d'URL, ou encore accéder à des sites web à partir des favoris gérés. Pour accéder aux favoris du portail web, ouvrez le dossier Favoris gérés dans la barre de favoris (en dessous de la barre d'URL) ou ouvrez le gestionnaire de favoris à partir du menu à trois points situé à droite de la barre d'URL.

Pour redimensionner ou déplacer la fenêtre du navigateur, faites glisser la barre d'onglets Chrome vers le bas. Vous disposez ainsi de plus d'espace sur l'écran pour ouvrir plusieurs fenêtres de navigation durant la session.

> **Note**
>
> Il se peut que certaines fonctionnalités du navigateur, comme le mode navigation privée, ne soient pas disponibles au cours de la session si votre administrateur les a désactivées.

Résilier une session

Pour mettre fin à une session, sélectionnez Profil et Terminer la session. À la fin d'une session, Amazon WorkSpaces Secure Browser supprime toutes les données de la session. Les données de navigation, comme les sites web ouverts ou l'historique, et les fichiers ou données de l'Explorateur de fichiers ne sont plus disponibles une fois la session terminée.

Si vous fermez un onglet au cours d'une session active, celle-ci se termine au bout d'un délai défini par votre administrateur. Si vous fermez l'onglet et revenez sur le portail web avant l'expiration de ce délai, vous pouvez reprendre la session en cours et voir toutes vos données de session précédentes, comme les sites web et fichiers ouverts.

Résolution des problèmes

Mon portail Amazon WorkSpaces Secure Browser ne me permet pas de me connecter. J'ai obtenu un message d'erreur indiquant « La configuration de votre portail web est incomplète. Contactez votre administrateur informatique pour obtenir de l'aide. »

Pour que vous puissiez vous connecter, votre administrateur doit finaliser la création du portail avec un fournisseur d'identité SAML 2.0. Contactez votre administrateur pour obtenir de l'aide.

Mon portail refuse de lance une session. J'ai obtenu un message d'erreur indiquant « Impossible de réserver la session. Une erreur interne s'est produite. Veuillez réessayer. »

Un problème de lancement de session s'est produit sur votre portail web. Essayez de relancer la session. Si le problème persiste, contactez votre administrateur pour obtenir de l'aide.

Je ne peux pas utiliser le presse-papiers, le micro ou la webcam.

Pour accorder les autorisations nécessaires au navigateur, sélectionnez l'icône de cadenas en regard de l'URL, puis actionnez le commutateur bleu situé en regard de Presse-papiers, Micro, Caméra et Pop-ups et redirections pour activer ces fonctionnalités.

> **Note**
>
> Si votre navigateur web ne prend pas en charge l'entrée vidéo ou audio, ces options ne figurent pas dans la barre d'outils.

L'audio/vidéo (AV) en temps réel d'Amazon WorkSpaces Secure Browser redirige la vidéo de votre webcam locale et l'entrée audio du microphone vers la session de streaming du navigateur. Ainsi, vous pouvez utiliser vos appareils locaux pour des conférences audio et vidéo dans le cadre de votre session de streaming avec des navigateurs web basés sur Chromium, tels que Google Chrome ou Microsoft Edge. La webcam n'est actuellement pas prise en charge dans les navigateurs non Chromium.

Pour savoir comment configurer Google Chrome, consultez Utiliser votre caméra et votre micro.

Mon portail web refuse de lancer une fenêtre d’écran supplémentaire.

Si vous essayez de lancer un double écran et que vous voyez l’icône Pop-ups bloqués à l’extrémité de la barre d’adresse dans la partie supérieure du navigateur, sélectionnez l’icône et la case d’option en regard de Toujours autoriser les pop-ups et les redirections. Lorsque les pop-ups sont autorisés, sélectionnez l’icône Double écran dans la barre d’outils pour lancer une nouvelle fenêtre, repositionnez la fenêtre sur votre écran, puis faites glisser un onglet du navigateur vers la fenêtre.

Lorsque j’essaie de télécharger des fichiers depuis le volet Fichiers, il ne se passe rien.

Si vous essayez de télécharger des fichiers depuis le volet Fichiers et que vous voyez l’icône Pop-ups bloqués à l’extrémité de la barre d’adresse dans la partie supérieure du navigateur, sélectionnez l’icône et la case d’option en regard de Toujours autoriser les pop-ups et les redirections. Maintenant que les pop-ups sont autorisés, essayer de nouveau de télécharger les fichiers.

Extension pour l’authentification unique

Amazon WorkSpaces Secure Browser propose une extension pour l'authentification unique avec les navigateurs Chrome et Firefox sur les ordinateurs de bureau. Si votre administrateur a activé l’extension, le portail web vous demande de l’installer lorsque vous vous connectez.

Amazon WorkSpaces Secure Browser a créé l'extension pour permettre l'authentification unique aux sites Web pendant votre session. Par exemple, si vous vous connectez à votre portail web via un fournisseur d’identité SAML 2.0 (comme Okta ou Ping) et que, pendant votre session, vous accédez à un site web qui utilise le même fournisseur d’identité, l’extension peut faciliter l’accès au site web sans invites de connexion supplémentaires.

Vous n’êtes pas tenu d’installer l’extension pour accéder à votre portail web, mais elle peut améliorer votre expérience en réduisant le nombre de fois que vous êtes invité à saisir votre nom d’utilisateur et votre mot de passe.

Lorsque vous vous connectez, l’extension localise les cookies que votre administrateur a listés pour votre session. Toutes les données localisées par l’extension sont chiffrées au repos et pendant le transit. À aucun moment ces données ne sont stockées dans votre navigateur local. Lorsque vous mettez fin à votre session, toutes les données associées (onglets ouverts, fichiers téléchargés et cookies transmis ou créés pendant la session) sont supprimées.

Compatibilité

L’extension fonctionne avec les appareils suivants :

- Ordinateurs portables
- Ordinateurs de bureau

L’extension fonctionne avec les navigateurs suivants :

- Chrome
- Firefox

Installation

Lorsque vous vous connectez au portail, suivez les instructions pour installer l'extension pour votre navigateur Chrome ou Firefox. Vous effectuez cette opération une seule fois pour toutes pour chaque navigateur web.

Si vous changez d’appareil, passez à un autre navigateur sur le même appareil ou supprimez l’extension de votre navigateur local, vous êtes invité à installer l’extension au démarrage de la session suivante.

Pour vous assurer que l'extension fonctionne comme prévu, utilisez-la dans une fenêtre de navigation normale, au lieu de la navigation privée (Chrome) ou de la navigation privée (Firefox).

Résolution des problèmes

Si l’extension est installée, mais que vous êtes toujours invité à vous connecter durant la session, procédez comme suit :

1. Assurez-vous que l'extension Amazon WorkSpaces Secure Browser est installée sur votre navigateur. Si vous avez supprimé les données de votre navigateur, il se peut que vous ayez supprimé l’extension sans le vouloir.
2. Assurez-vous que vous n'êtes pas en mode navigation privée (Firefox) ou en mode navigation privée (Chrome). Ces modes peuvent occasionner des problèmes avec les extensions.
3. Si le problème persiste, contactez votre administrateur de portail pour obtenir une aide supplémentaire.

Historique du document pour le guide d'administration d'Amazon WorkSpaces Secure Browser

Le tableau suivant décrit les versions de documentation pour Amazon WorkSpaces Secure Browser.

Modification	Description	Date
Autoriser les liens profonds	Autorisez les portails à recevoir des liens profonds qui connectent les utilisateurs à un site Web spécifique au cours d'une session.	25 juin 2024
Mise à jour de la stratégie gérée	Ajout d'une politique AmazonWorkSpacesSecureBrowserReadOnly gérée	24 juin 2024
Utilisez la barre d'outils pour zoomer	Vous pouvez augmenter la taille de l'affichage, des icônes et du texte à l'aide de la barre d'outils.	1er mai 2024
Nouveaux paramètres du portail Web	Vous pouvez désormais spécifier le type d'instance et le nombre maximal d'utilisateurs simultanés pour votre portail Web.	22 avril 2024
CloudWatch métriques	Ajouté GlobalCpuPercent et GlobalMemoryPercent métriques.	26 février 2024
Configurer le filtrage des URL	Vous pouvez utiliser les règles de Chrome pour filtrer les URL auxquelles les utilisateurs peuvent accéder depuis leur navigateur distant.	21 février 2024

Types d'authentification IdP	Vous pouvez choisir le type d'authentification standard ou le type d'authentification IAM Identity Center.	5 février 2024
Activation d’extension pour l’authentification unique	Vous pouvez activer une extension pour faire bénéficier vos utilisateurs finaux d’une meilleure expérience de connexion aux portails.	28 août 2023
Guide de l'utilisateur pour Amazon WorkSpaces Secure Browser	Du contenu a été ajouté pour aider les utilisateurs finaux qui souhaitent en savoir plus sur l'accès à Amazon WorkSpaces Secure Browser, le lancement et la configuration d'une session, ainsi que l'utilisation de la barre d'outils et du navigateur Web.	17 juillet 2023
Contrôle d’accès IP	WorkSpaces Secure Browser vous permet de contrôler les adresses IP à partir desquelles votre portail Web est accessible.	31 mai 2023
Mise à jour de la stratégie gérée	Politique AmazonWorkSpacesWebReadOnly gérée mise à jour	15 mai 2023
Mise à jour de Configuration du fournisseur d’identité	WorkSpaces Secure Browser propose deux types d'authentification : Standard et AWS IAM Identity Center	15 mars 2023

Mise à jour de la politiques de navigateur	Mise à jour et restructuration de la section Politique de navigateur	31 janvier 2023
Mise à jour de la stratégie gérée	Politique AmazonWorkSpacesWebServiceRolePolicy gérée mise à jour	15 décembre 2022
Allowlist et Blocklist	Spécifiez Allowlist et Blocklist pour spécifier la liste des domaines auxquels vos utilisateurs peuvent ou non accéder.	14 novembre 2022
Mise à jour de la stratégie gérée	Politique AmazonWorkSpacesWebReadOnly gérée mise à jour	2 novembre 2022
Mise à jour de la stratégie gérée	Politique AmazonWorkSpacesWebServiceRolePolicy gérée mise à jour	24 octobre 2022
Journalisation des accès utilisateur	Configuration de la journalisation des accès utilisateur pour enregistrer les événements utilisateur	17 octobre 2022
Mises à jour de Mise en réseau	Diverses mises à jour apportées à la section « Mise en réseau et accès »	22 septembre 2022
Mise à jour de la stratégie gérée	Politique AmazonWorkSpacesWebServiceRolePolicy gérée mise à jour	6 septembre 2022
Configuration des sessions utilisateur	Configuration de l'éditeur de méthode d'entrée (IME) et de la localisation dans la session	28 juillet 2022

Mises à jour de Mise en réseau	Diverses mises à jour apportées à la section « Mise en réseau et accès »	7 juillet 2022
Valeurs de délai d'expiration	Spécifiez le Délai de déconnexion en minutes et le Délai d'inactivité de déconnexion en minutes	16 mai 2022
Mise à jour de la politique gérée	Mise à jour de la politique AmazonWorkSpacesWebServiceRolePolicy gérée pour ajouter l'espace de noms AWS/Usage aux autorisations d'API PutMetricData	6 avril 2022
Rôle lié à un service	Nouveau rôle AWSServiceRoleForAmazonWorkSpacesWeb lié au service	30 novembre 2021
Politique gérée	Nouvelle politique AmazonWorkSpacesWebReadOnly gérée	30 novembre 2021
Politique gérée	Nouvelle politique AmazonWorkSpacesWebServiceRolePolicy gérée	30 novembre 2021
Première version	Publication initiale du guide d'administration de WorkSpaces Secure Browser	30 novembre 2021

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