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 WorkSpaces Applications, 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 des versions d'Amazon WorkSpaces Secure Browser

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 de plus amples informations, veuillez consulter 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 des espaces de travail Web. Pour de plus amples informations, veuillez consulter the section called "Utilisation des rôles liés à un service".
- Console URLs contenant des espaces de travail Web.
- Documentation URLs contenant workspaces-web. Pour plus d'informations, consultez la documentation Amazon WorkSpaces Secure Browser.
- Rôle ReadOnly géré existant. Pour de plus amples informations, veuillez consulter the section called "AWS politiques gérées".
- Nom de la subvention KMS.
- Préfixe de flux Kinesis UAL (User-Activity Logging).

De plus, le portail existant URLs reste le même. URLs pour les portails créés avant le 20 mai 2024, ils 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 d'Amazon 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.

Cloud privé virtuel (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 VPCs 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 les ajouter ou les modifier PCAs 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.

AWS services liés à Amazon WorkSpaces Secure Browser

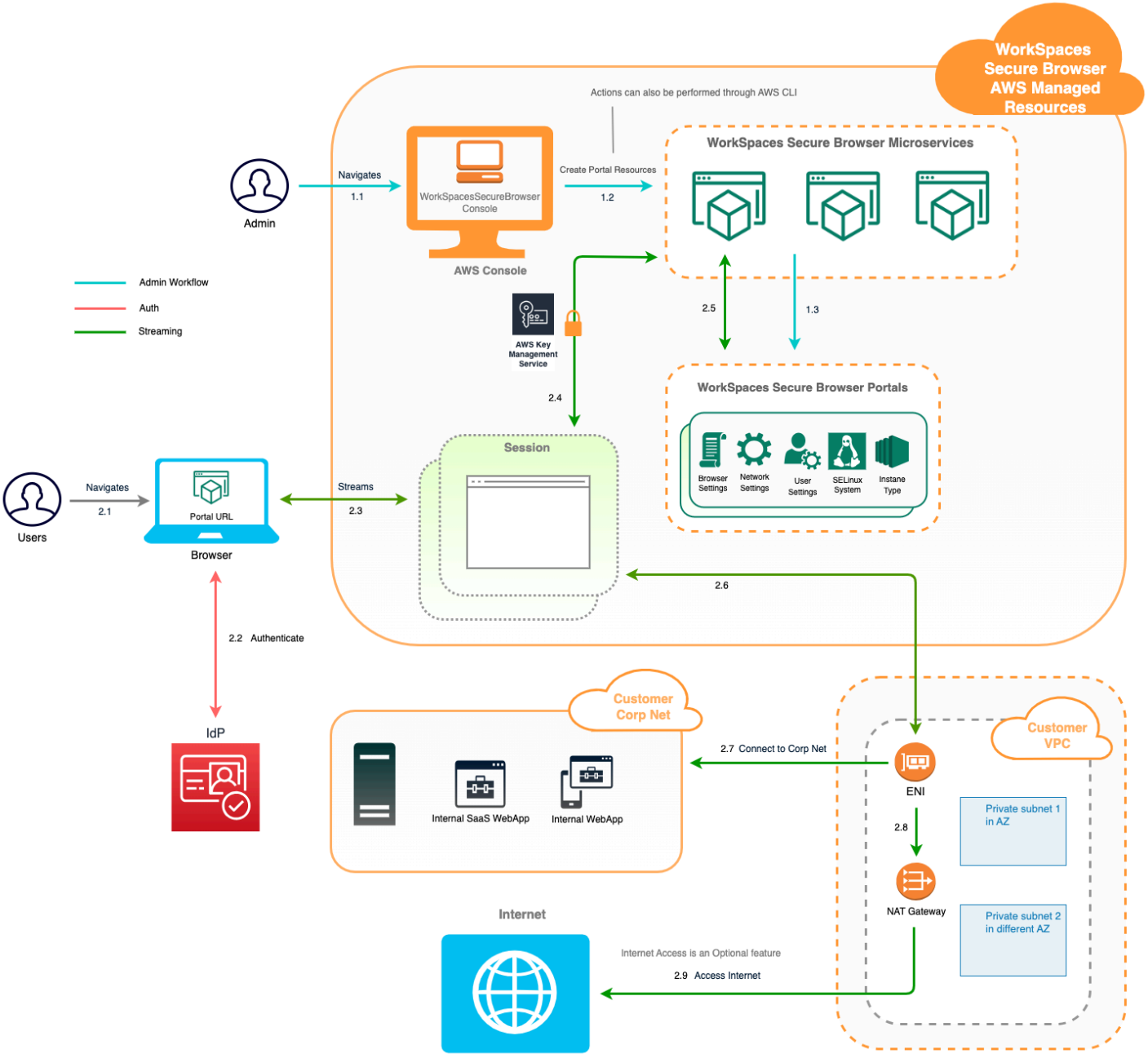
Plusieurs AWS services sont liés à WorkSpaces Secure Browser.

WorkSpaces Secure Browser est une fonctionnalité d'Amazon qui fait WorkSpaces partie du portefeuille informatique pour les utilisateurs AWS finaux. 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 d'Amazon WorkSpaces Secure Browser

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



Accès au navigateur Amazon WorkSpaces Secure

Vous pouvez accéder à WorkSpaces Secure Browser de plusieurs manières.

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 d'Amazon 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 l'https://portal.aws.amazon.com/billing/inscription.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique ou un SMS 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 Services AWS et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

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

Création d'un utilisateur doté d'un accès administratif

Une fois que vous vous êtes inscrit à un utilisateur administratif Compte AWS, que vous Utilisateur racine d'un compte AWS l'avez sécurisé AWS IAM Identity Center, que vous l'avez activé et que vous en avez créé un, 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, octroyez 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.

Connexion en tant qu'utilisateur doté 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.

Attribution d'un accès à d'autres utilisateurs

1. Dans IAM Identity Center, créez un ensemble d'autorisations qui respecte la bonne pratique consistant à appliquer les autorisations de moindre privilège.

   Pour obtenir des instructions, consultez Création d'un ensemble d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .

2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

   Pour obtenir des instructions, consultez Ajout de groupes dans le Guide de l'utilisateur AWS IAM Identity Center .

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 ?	À	Méthode
IAM	(Recommandé) Utilisez les informations d'identification de la console comme informations d'identification temporaires pour signer les demandes programmatiques adressées au AWS CLI AWS SDKs, ou AWS APIs.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour le AWS CLI, voir Connexion pour le développement AWS local dans le guide de AWS Command Line Interface l'utilisateur. • Pour AWS SDKs, voir Connexion pour le développement AWS local

Quel utilisateur a besoin d'un accès programmatique ?	À	Méthode
		dans le guide de référence AWS SDKs and Tools.
Identité de la main-d'œuvre (Utilisateurs gérés dans IAM Identity Center)	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées au AWS CLI AWS SDKs, ou AWS APIs.	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 AWS SDKs, outils, et AWS APIs, voir Authentification IAM Identity Center dans le guide de référence AWS SDKs et Tools.
IAM	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées au AWS CLI AWS SDKs, ou AWS APIs.	Suivez les instructions de la section Utilisation d'informations d'identification temporaires avec AWS les ressources du Guide de l'utilisateur IAM.

Quel utilisateur a besoin d'un accès programmatique ?	À	Méthode
IAM	(Non recommandé) Utilisez des informations d'identification à long terme pour signer des demandes programmatiques adressées au AWS CLI AWS SDKs, ou AWS APIs.	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 outils AWS SDKs et, voir Authentifier à l'aide d'informations d'identif ication à long terme dans le guide de référence des outils AWS SDKs et. • Pour AWS APIs, voir Gestion des clés d'accès pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Mise en réseau pour Amazon WorkSpaces Secure Browser

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

- Configuration d'un VPC pour Amazon Secure Browser WorkSpaces
- Activation des connexions utilisateur pour Amazon WorkSpaces Secure Browser

Configuration d'un VPC pour Amazon Secure Browser WorkSpaces

Pour installer et configurer un VPC pour WorkSpaces Secure Browser, procédez comme suit.

Rubriques

Exigences en matière de VPC pour Amazon Secure Browser WorkSpaces

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 réseaux VPCs , ainsi que les sous-réseaux, doivent répondre aux exigences suivantes :

- Le VPC doit avoir une location par défaut. VPCs avec location dédiée ne sont pas prises 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 de plus amples informations, veuillez consulter Création d'un nouveau VPC pour Amazon Secure Browser WorkSpaces.
- Tous les sous-réseaux doivent disposer d'une connexion stable à tout contenu interne, situé sur site 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 de plus amples informations, veuillez consulter Création d'un nouveau VPC pour Amazon Secure Browser WorkSpaces.

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 illimitée pour Amazon WorkSpaces Secure Browser (recommandé)

Création d'un nouveau VPC pour Amazon Secure Browser WorkSpaces

Cette section décrit comment utiliser l'assistant VPC pour créer rapidement un VPC avec des sous-réseaux publics et privés. L'assistant crée automatiquement une passerelle Internet, une passerelle NAT et configure les tables de routage pour vos sous-réseaux.

Pour en savoir plus sur cette configuration, consultez VPC avec des sous-réseaux publics et privés (NAT).

Rubriques

- Configuration rapide du VPC (1 minute)
- Vérification des tables de routage de votre sous-réseau (facultatif)

Configuration rapide du VPC (1 minute)

Procédez comme suit pour créer rapidement un VPC dédié pour WorkSpaces Secure Browser avec des sous-réseaux publics et privés pour l'accès à Internet. Si vous souhaitez utiliser un VPC existant, vérifiez Exigences en matière de VPC pour Amazon Secure Browser WorkSpaces qu'il répond aux exigences.

> **Note**
>
> Assurez-vous que vous êtes dans la zone souhaitée Région AWS. Vous pouvez modifier la région dans la console si nécessaire.

Pour configurer rapidement un VPC

1. Ouvrez l'assistant de création de VPC : créez un VPC avec des ressources. Conservez tous les paramètres par défaut, sauf indication contraire ci-dessous :

- Pour Resource à créer, sélectionnez VPC et plus encore.
- Dans le champ Name tag, sélectionnez Générer automatiquement et entrez un nom descriptif pour votre VPC (par exemple**WSB-VPC**,).
- Pour le bloc IPv4 CIDR, par défaut, le **10.0.0.0/16** VPC utilise. Vous pouvez spécifier un autre bloc IPv4 CIDR si nécessaire.
- Pour la location, sélectionnez Par défaut (VPCs les locations dédiées ne sont pas prises en charge).
- Pour Nombre de zones de disponibilité (AZs), sélectionnez 2.
  - Développez Personnalisez AZs et sélectionnez 2 zones de disponibilité différentes prises en charge par WorkSpaces Secure Browser. Pour la liste des produits pris en charge AZs, consultezZones de disponibilité prises en charge pour Amazon WorkSpaces Secure Browser.
- Pour Nombre de sous-réseaux publics, sélectionnez 2.
- Pour Nombre de sous-réseaux privés, sélectionnez 2.
- Pour les blocs d'adresse CIDR de sous-réseau, si vous devez personnaliser les blocs d'adresse CIDR de vos sous-réseaux, développez les blocs d'adresse CIDR personnalisés des sous-réseaux. Assurez-vous que chaque sous-réseau possède suffisamment d'adresses IP pour le trafic attendu.
- Pour les passerelles NAT, sélectionnez Régional pour activer l'accès à Internet pour les sous-réseaux privés dans toutes les zones de disponibilité.
- Pour les points de terminaison VPC, sélectionnez Aucun. Si vous avez besoin d'un accès direct à S3 sans passer par la passerelle NAT, sélectionnez S3 Gateway.
- Pour les options DNS, maintenez les options DNS activées (par défaut) pour garantir une résolution de noms correcte au sein de votre VPC.

2. Passez en revue le volet d'aperçu, puis choisissez Create VPC.

> **Note**
>
> Des frais supplémentaires s'appliquent pour les passerelles NAT et les points de terminaison VPC. Pour plus d'informations, consultez la page de tarification des VPC.

Vérification des tables de routage de votre sous-réseau (facultatif)

L'assistant VPC configure automatiquement les tables de routage pour vous. Si vous avez créé votre VPC manuellement ou si vous souhaitez confirmer la configuration, vous pouvez vérifier que les informations suivantes sont correctes 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 Subnets, puis sélectionnez un sous-réseau public. Par exemple, WSB-VPC-Subnet-Public1-US-EAST-1A.
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 IPv4 CIDR du sous-réseau public (par exemple, 10.0.0/20)	Local	Tout le trafic provenant des ressources destinées IPv4 aux adresses du bloc IPv4 CIDR du sous-réseau public. Ce trafic est acheminé localement au sein du VPC.

Destination	Cible	Description
Trafic destiné à toutes les autres IPv4 adresses (par exemple, 0.0.0.0/0)	Sortant (igw-ID)	Le trafic destiné à toutes les autres IPv4 adresses est acheminé vers la passerelle Internet (identifiée par IGW-ID) créée par l'assistant VPC.

5. Dans le panneau de navigation, choisissez Subnets (Sous-réseaux). Sélectionnez ensuite un sous-réseau privé (par exemple,**`WSB-VPC-subnet-private1-us-east-1a`**).
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 **`WSB-VPC-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 IPv4 CIDR du sous-réseau public (par exemple, 10.0.0/20)	Local	Tout le trafic provenant des ressources destinées IPv4 aux adresses du bloc IPv4 CIDR du sous-réseau public est acheminé localement au sein du VPC.
Trafic destiné à toutes les autres IPv4 adresses (par exemple, 0.0.0.0/0)	Sortant (nat-ID)	Le trafic destiné à toutes les autres IPv4 adresses 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 sur Internet pour Amazon WorkSpaces Secure Browser

Vous pouvez choisir d'activer la navigation Internet illimitée (option recommandée) ou la navigation Internet restreinte.

Rubriques

- Activation de la navigation Internet illimitée pour Amazon WorkSpaces Secure Browser (recommandé)
- Activation de la navigation Internet restreinte pour Amazon WorkSpaces Secure Browser
- Ports de connectivité Internet pour Amazon WorkSpaces Secure Browser

Activation de la navigation Internet illimitée pour Amazon WorkSpaces Secure Browser (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 d'un nouveau VPC pour Amazon Secure Browser WorkSpaces.

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 VPC avec des sous-réseaux privés, consultez. the section called "Configuration rapide du VPC"

   > **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.

Activation de la navigation Internet restreinte pour Amazon WorkSpaces Secure Browser

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 de plus amples informations, veuillez consulter the section called "Navigation Internet illimitée". 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 :

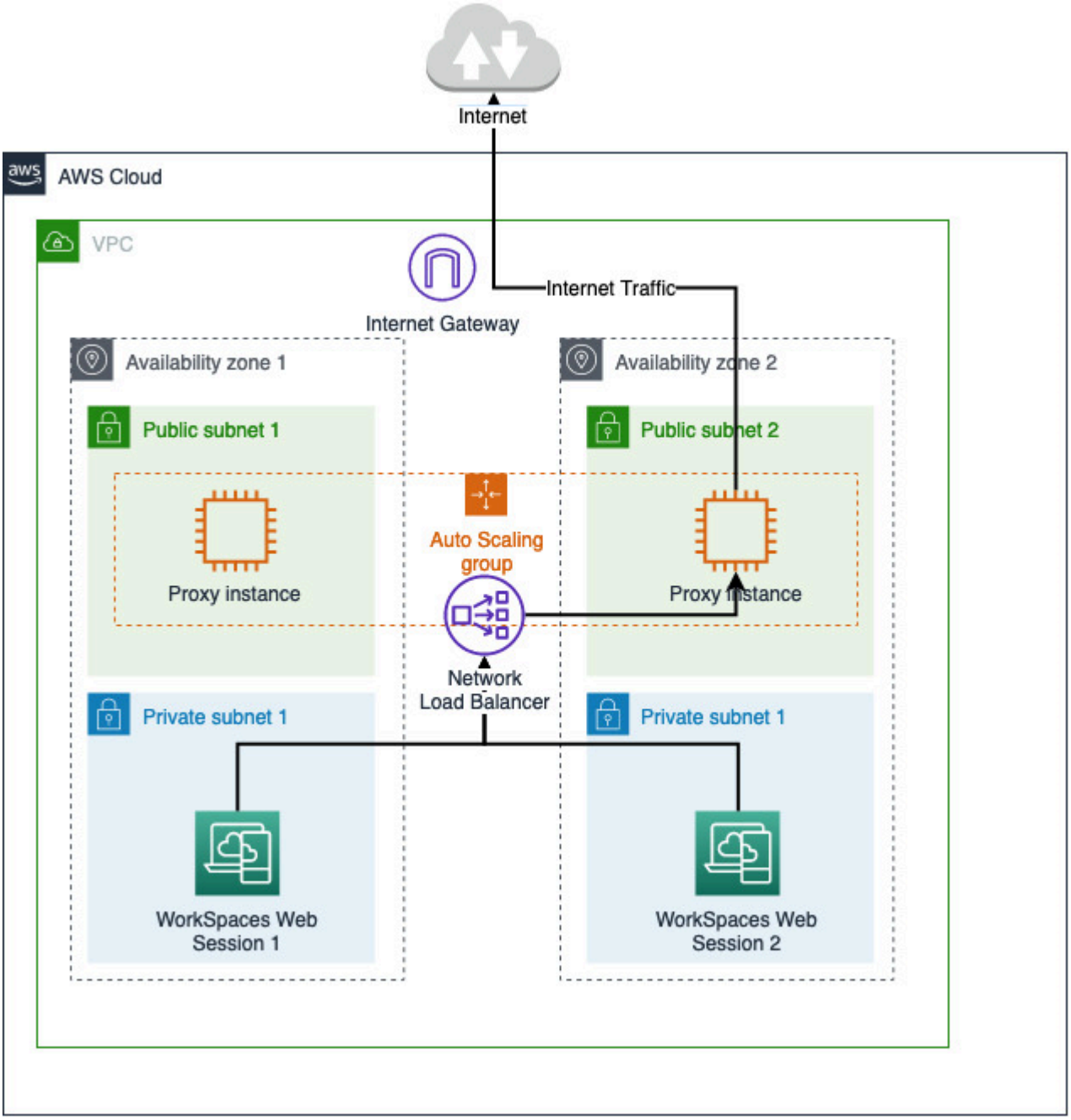
- Un proxy sortant qui inclut un groupe d'instances Amazon EC2 à mise à l'échelle automatique, hébergées par un équilibreur de charge réseau. Les instances de proxy résident dans un sous-réseau public et chacune d'entre elles est associée à une adresse IP élastique, ce qui leur permet d'accéder à Internet.
- 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.

Rubriques

Architecture de navigation Internet restreinte pour Amazon WorkSpaces Secure Browser

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.



Conditions préalables relatives à la navigation Internet restreinte pour Amazon WorkSpaces Secure Browser

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 (). AZs Pour plus d'informations sur la configuration de votre environnement VPC, consultez la section Par défaut. VPCs
- 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.

Proxy sortant HTTP pour Amazon 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 le paramètre CloudFormation de sortie OutboundProxyDomainet 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 liés à la navigation Internet restreinte pour Amazon WorkSpaces Secure Browser

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.

Ports de connectivité Internet pour Amazon WorkSpaces Secure Browser

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

Bonnes pratiques en matière de VPC pour Secure Browser WorkSpaces

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 "Gestion des quotas de service".
- 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 (ENIs) que la capacité maximale souhaitée de votre flotte. Par défaut, la limite ENIs par région est de 5 000. Pour en savoir plus, consultez Interfaces réseau.

Lorsque vous planifiez la capacité pour des déploiements de très grande envergure, par exemple des milliers de sessions de streaming simultanées, tenez compte du nombre de sessions de streaming ENIs qui pourraient être nécessaires en cas de pic d'utilisation. 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 la section 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 de plus amples informations, veuillez consulter the section called "Création d'un nouveau 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 pour Amazon WorkSpaces Secure Browser

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.

La visualisation AZ vous IDs 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 l'AZ IDs que vous pouvez utiliser pour chaque région. Pour voir le mappage entre AZ et IDs les zones de disponibilité de votre compte, consultez la section AZ IDs pour vos ressources dans le guide de AWS RAM l'utilisateur.

Nom de la région	Code région	AZ pris en charge IDs
USA Est (Virginie du Nord)	`us-east-1`	`use1-az1`, `use1-az2`, `use1-az4`, `use1-az5`, `use1-az6`

Nom de la région	Code région	AZ pris en charge IDs
USA Ouest (Oregon)	us-west-2	usw2-az1, usw2-az2, usw2-az3
Asie-Pacifique (Mumbai)	ap-south-1	aps1-az1, aps1-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
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 zones de disponibilité IDs, consultez la section Régions, zones de disponibilité et zones locales dans le guide de l'utilisateur Amazon EC2.

Activation des connexions utilisateur pour Amazon WorkSpaces Secure Browser

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 pour Amazon WorkSpaces Secure Browser.

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

Rubriques

Exigences relatives à l'adresse IP et au port pour Amazon WorkSpaces Secure Browser

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 pour Amazon WorkSpaces Secure Browser.
  - 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 Amazon WorkSpaces Secure Browser

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 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 appstream 2. *{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 identité cognitive. *{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 Amazon 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 tarif 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 d'Amazon WorkSpaces Secure Browser.

Rubriques

Création d'un portail Web pour Amazon WorkSpaces Secure Browser

Pour créer un portail web, procédez comme suit.

Rubriques

Configuration des paramètres réseau pour Amazon WorkSpaces Secure Browser

Pour configurer les paramètres réseau pour WorkSpaces Secure Browser, procédez comme suit.

1. Ouvrez la console WorkSpaces Secure Browser à la https://console.aws.amazon.com/workspaces-web/maison.
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 de plus amples informations, veuillez consulter Mise en réseau pour Amazon WorkSpaces Secure Browser.
        - 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 pour Amazon WorkSpaces Secure Browser

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 de plus amples informations, veuillez consulter the section called "Gestion des quotas de service".

   > **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 Domaine personnalisé, vous pouvez configurer un domaine personnalisé pour votre portail afin de permettre l'accès via votre propre nom de domaine au lieu du point de terminaison du portail par défaut. Pour de plus amples informations, veuillez consulter the section called "Domaine personnalisé". Cette option est facultative.
4. Sous Session Logger, vous pouvez spécifier un compartiment S3 pour stocker les fichiers journaux de session. Pour de plus amples informations, veuillez consulter the section called "Configuration de l'enregistreur de session". Cette option est facultative.
5. Sous Journalisation de l'accès utilisateur, pour l'ID de flux Kinesis, sélectionnez le flux de données Amazon Kinesis auquel vous souhaitez envoyer des fichiers journaux. Pour de plus amples informations, veuillez consulter the section called "Configuration de l'enregistrement des activités des utilisateurs". Cette option est facultative.
6. Sous Contrôle d'accès IP, choisissez si vous souhaitez restreindre l'accès aux réseaux fiables. Pour de plus amples informations, veuillez consulter the section called "Gestion des contrôles d'accès IP". Cette option est facultative.
7. Dans les paramètres de protection des données, vous pouvez créer des politiques pour WorkSpaces Secure Browser afin de supprimer les informations sensibles. Pour de plus amples informations, veuillez consulter the section called "Paramètres de protection des données". Cette option est facultative.
8. Dans le cadre du filtrage des URL, vous pouvez spécifier quels utilisateurs URLs finaux sont autorisés à accéder ou à bloquer des catégories spécifiques URLs ou de domaines afin de restreindre l'accès. Pour de plus amples informations, veuillez consulter the section called "Filtrage du contenu Web". Cette option est facultative.

1. Pour limiter la navigation dans les sessions à quelques domaines sélectionnés, activez le bouton Tout bloquer URLs et cliquez sur Ajouter une URL pour afficher la liste des URLs utilisateurs finaux autorisés à accéder.
2. Pour créer une liste des domaines URLs à bloquer pour les utilisateurs finaux, cliquez sur Ajouter une URL pour répertorier les domaines URLs à bloquer ou cliquez sur Ajouter des catégories pour sélectionner les catégories de domaines bloqués (réseaux sociaux, par exemple).

9. Dans les paramètres de politique, vous pouvez définir n'importe quelle politique de navigateur à l'aide des politiques Chrome disponibles pour la dernière version stable du portail Web. Pour de plus amples informations, veuillez consulter the section called “Gestion de la politique du navigateur”. Cette option est facultative.

   1. Vous pouvez sélectionner rapidement certaines des politiques les plus courantes dans l'éditeur visuel
      - Pour l'URL de démarrage (facultatif), entrez un 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**
        >
        > URLs les visites effectuées pendant une navigation privée, ou avant qu'un utilisateur ne supprime l'historique de son navigateur, ne peuvent pas être enregistrées dans le journal des accès des utilisateurs. Pour de plus amples informations, veuillez consulter the section called “Configuration de l'enregistrement des activités des utilisateurs”.

      - Pour les favoris du navigateur (facultatif), entrez le nom d'affichage, le domaine et le dossier de tous les favoris que vous souhaitez que vos utilisateurs voient 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.

2. Vous pouvez également ajouter ou modifier directement des politiques en utilisant l'éditeur JSON au lieu de l'éditeur visuel. Pour connaître le format spécifique d'une politique, reportez-vous à la liste des règles de Chrome Enterprise.
3. Vous pouvez également importer les politiques Chrome utilisées dans votre organisation en chargeant un fichier JSON sur le portail Web. Pour plus de détails, veuillez consulter the section called "Tutoriel : définition d'une politique de navigateur personnalisée"

   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.

10. Ajoutez des tags 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. Cette option est facultative.
11. Choisissez Next (Suivant) pour continuer.

Configuration des paramètres utilisateur pour Amazon WorkSpaces Secure Browser

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. Dans la section Personnalisation de l'image de marque, vous pouvez personnaliser les écrans de connexion et de chargement qui apparaissent à vos utilisateurs finaux en modifiant les éléments visuels, le contenu textuel et les conditions d'utilisation. Pour de plus amples informations, veuillez consulter the section called "Personnalisation de la marque". Cette option est facultative.
2. Sous Autorisations, indiquez si vous souhaitez activer l'extension pour l'authentification unique. Pour de plus amples informations, veuillez consulter the section called "Gestion de l'extension d'authentification unique".

3. Pour Autoriser les utilisateurs à imprimer sur un appareil local depuis leur portail Web, choisissez Autorisé ou Non autorisé.
4. 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 “Liens profonds”.
5. Pour Autoriser les utilisateurs à utiliser l'authentification locale dans leur session de portail, choisissez Autorisé ou Non autorisé. Pour plus d'informations sur l'authentification Web, consultezthe section called “Redirection de l'authentification Web”.
6. Sous Contrôles de la barre d'outils, choisissez les paramètres souhaités sous Fonctionnalités.
7. Sous Paramètres, gérez l'affichage de la barre d'outils au début de la session, notamment l'état de la barre d'outils (ancrée ou détachée), le thème (mode sombre ou clair), la visibilité des icônes et la résolution d'affichage maximale pour la session. Laissez ces paramètres non configurés pour donner aux utilisateurs finaux le contrôle total de ces options. Pour de plus amples informations, veuillez consulter the section called “Commandes de la barre d’outils”.
8. Pour les délais d'expiration des sessions, spécifiez ce qui suit :

   - 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 de votre fournisseur d'identité pour Amazon WorkSpaces Secure Browser

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

Rubriques

Choix du type de fournisseur d'identité pour Amazon WorkSpaces Secure Browser

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 de plus amples informations, veuillez consulter the section called "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 de plus amples informations, veuillez consulter the section called "Type d'authentification IAM Identity Center".

Rubriques

Configuration du type d'authentification standard pour Amazon WorkSpaces Secure Browser

Le type d'authentification standard est le type d'authentification par défaut. Il peut prendre en charge les flux de connexion initiés par le fournisseur de services (initié par le SP) et par le fournisseur d'identité (initié par l'IdP) avec votre IdP conforme à la norme SAML 2.0. Pour configurer le type d'authentification standard, suivez les étapes ci-dessous pour fédérer votre IdP SAML 2.0 tiers (tel qu'Okta ou Ping) directement avec votre portail.

Rubriques

Configuration de votre fournisseur d'identité sur Amazon 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.

Configuration de votre IdP sur votre propre IdP

Pour configurer votre IdP sur votre propre IdP, procédez comme suit.

1. Ouvrez un nouvel onglet dans votre navigateur.
2. 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.

3. 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.

4. 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 “Configuration de l'IdP sur Secure Browser WorkSpaces ” relais par défaut pour votre application IdP.

5. 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 “Configuration de l'IdP sur Secure Browser WorkSpaces ” 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.

6. 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.

7. Facultatif : configurez une déconnexion unique. Si vous avez choisi Single Logout, suivez les étapes de l'étape 5 the section called “Configuration de l'IdP sur Secure Browser WorkSpaces ” pour télécharger le certificat de signature sur votre IdP, renseigner l'URL de déconnexion unique et activer la déconnexion unique.

8. Accordez l'accès à vos utilisateurs dans votre IdP pour utiliser WorkSpaces Secure Browser.

9. Téléchargez un fichier d'échange de métadonnées auprès de votre IdP. Vous téléchargerez ces métadonnées dans WorkSpaces Secure Browser à l'étape suivante.

Finalisation de la configuration de l'IdP sur Amazon Secure Browser WorkSpaces

Pour terminer la configuration de l'IdP sur WorkSpaces Secure Browser, procédez comme suit.

1. 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.
2. 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.
3. 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.
4. Lorsque vous avez terminé, cliquez sur Next.
5. 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 informations *<Your SP ACS URL>* 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 d'utilisation spécifiques IdPs avec Amazon WorkSpaces Secure Browser

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 : création et attribution d'un compte utilisateur	Activer l'authentification unique pour une application d'entreprise	Vérification de la signature des demandes SAML	Configurer le chiffrement par jeton SAML Microsoft Entra	Protocole SAML de connexion unique
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	Ajouter des utilisateurs OneLogin	Connecteur personnalisé SAML	Connecteur personnalisé SAML	Connecteur personnalisé SAML	Connecteur personnalisé SAML

IdP	Configuration de l'application SAML	Gestion des utilisateurs	Authentification initiée par l'IDP	Signature de la demande	Cryptage des assertions	Déconnexion unique
	(avancé) (4266907)	manuellement	(avancé) (4266907)	(avancé) (4266907)	(avancé) (4266907)	(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 Amazon WorkSpaces Secure Browser

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 de plus amples informations, veuillez consulter the section called "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.

Rubriques

Création d'un portail Web avec IAM Identity Center

Pour créer un portail Web avec IAM Identity Center, procédez comme suit.

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 and/or Groupes d'utilisateurs.
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.

Gestion de votre portail Web avec IAM Identity Center

Pour gérer votre portail Web avec IAM Identity Center, procédez comme suit.

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.

Ajout d'utilisateurs et de groupes supplémentaires à un portail Web

Pour ajouter des utilisateurs et des groupes supplémentaires à un portail Web existant, procédez comme suit.

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 depuis la page d'édition de votre portail WorkSpaces Secure Browser.

Afficher ou supprimer des utilisateurs et des groupes pour votre portail Web

Pour afficher ou supprimer des utilisateurs et des groupes pour votre portail Web, utilisez les actions disponibles dans le tableau Utilisateurs assignés. Pour plus d'informations, voir 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.

Modification du type de fournisseur d'identité pour Amazon WorkSpaces Secure Browser

Vous pouvez modifier le type d'authentification de votre portail à tout moment. Pour ce faire, suivez les étapes suivantes.

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

Lancement d'un portail Web avec Amazon WorkSpaces Secure Browser

Lorsque vous avez terminé de configurer votre portail Web, vous pouvez suivre ces étapes pour le lancer.

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.

Test de votre portail Web dans Amazon WorkSpaces Secure Browser

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'Diffusion de votre portail Web dans Amazon WorkSpaces Secure Browser.

1. Vous voulez ouvrir la console WorkSpaces Secure Browser https://console.aws.amazon.com/workspaces-web/chez vous ? 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 vous voyez la page Votre session est en cours de préparation, 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 URLs en entrant dans la barre d'adresse.

Diffusion de votre portail Web dans Amazon WorkSpaces Secure Browser

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 les assertions SAML initiées par le SP et par l'IdP dans. the section called “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.
- Utilisez un domaine personnalisé si vous en avez configuré un pour votre portail au lieu de l'URL du portail afin d'offrir une expérience de marque plus intégrée à vos utilisateurs. Pour de plus amples informations, veuillez consulter the section called “Domaine personnalisé”.

Gestion de votre portail Web dans Amazon WorkSpaces Secure Browser

Après avoir configuré votre portail Web, vous pouvez effectuer les actions suivantes pour le gérer.

Rubriques

Afficher les détails du portail Web dans Amazon WorkSpaces Secure Browser

Pour consulter les détails du portail Web, 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. Choisissez WorkSpaces Secure Browser, Portails Web, choisissez votre portail Web, puis sélectionnez Afficher les détails.

Modification d'un portail Web dans Amazon WorkSpaces Secure Browser

Pour modifier un portail Web, 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. 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.

Supprimer un portail Web dans Amazon WorkSpaces Secure Browser

Pour supprimer un portail Web, 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. Choisissez WorkSpaces Secure Browser, Portails Web, choisissez votre portail Web, puis sélectionnez Supprimer.

Gestion des quotas de service pour votre portail dans Amazon WorkSpaces Secure Browser

Lorsque vous créez votre Compte AWS, nous définissons automatiquement des quotas de service par défaut (également appelés limites) pour l'utilisation des ressources avec Services AWS. 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	Value
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

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

> **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.

Rubriques

Demande d'augmentation du quota de service dans Amazon WorkSpaces Secure Browser

Pour demander une augmentation du quota de service, procédez comme suit.

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.

Demande d'extension du portail dans Amazon WorkSpaces Secure Browser

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.

Demande d'augmentation du nombre maximum de sessions simultanées dans Amazon WorkSpaces Secure Browser

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 and/or d'utilisation (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 pour Amazon WorkSpaces Secure Browser

Par exemple, supposons 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).

Autres quotas de service dans Amazon WorkSpaces Secure Browser

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 IdP SAML dans Amazon Secure Browser WorkSpaces

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 AWS IAM Identity Center, voir 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 "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 activités des utilisateurs dans Amazon WorkSpaces Secure Browser

WorkSpaces Secure Browser propose deux options pour enregistrer l'activité des utilisateurs et les événements liés à la sécurité :

- Session Logger capture un large éventail d'événements de session. Ces journaux sont envoyés dans un compartiment Amazon S3 de votre compte, ce qui permet une intégration facile à votre plateforme SIEM préférée.
- La journalisation des accès utilisateurs capture les événements de session les plus critiques. Ces journaux sont transmis à un flux Amazon Kinesis pour un traitement et une analyse en temps réel.

Les deux options de journalisation sont configurées au niveau du portail. Vous devez configurer chaque option individuellement pour chaque portail sur lequel vous souhaitez que la journalisation soit active. Vous pouvez activer l'une ou l'autre option ou les deux, en fonction de vos besoins pour chaque portail.

Vous êtes responsable du respect de toutes les exigences applicables à la journalisation ou à la surveillance de l'activité des utilisateurs lorsque vous utilisez cette fonctionnalité, y compris la journalisation ou le suivi de l'activité des employés.

Rubriques

Configuration de l'enregistreur de session pour Amazon WorkSpaces Secure Browser

> **Warning**
>
> L'activation de l'enregistreur de session désactive les fonctionnalités suivantes de Chrome :
>
> - Mode navigation privée
> - Outils pour développeurs
> - Changement de profil Chrome

Pour activer l'enregistreur de session pour un portail WorkSpaces Secure Browser, vous devez d'abord identifier le compartiment Amazon S3 dans lequel les événements de session seront collectés. Vous pouvez utiliser un bucket existant qui stocke déjà des journaux similaires ou en créer un nouveau spécialement à cette fin.

Le compartiment Amazon S3 doit avoir une politique de compartiment qui accorde à WorkSpaces Secure Browser l'autorisation d'y écrire des journaux. Nous vous recommandons de placer le compartiment Amazon S3 dans la même Compte AWS région que votre portail WorkSpaces Secure Browser.

Il n'y a aucune exigence de dénomination pour le compartiment Amazon S3. Pour créer un nouveau compartiment, suivez les étapes ci-dessous ou consultez la section Création d'un compartiment à usage général dans le guide de l'utilisateur d'Amazon Simple Storage Service. Pour obtenir des conseils sur la configuration des autorisations, consultez les politiques relatives aux compartiments pour Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Vous trouverez ci-dessous un exemple de politique pour votre compartiment Amazon S3. Assurez-vous de mettre à jour la politique avec le nom de votre compartiment Amazon S3. Notez que le principal est « workspaces-web.amazonaws.com ».

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "AllowSessionLogger",
          "Effect": "Allow",
          "Principal": {
              "Service": "workspaces-web.amazonaws.com"
          },
          "Action": [
              "s3:PutObject"
          ],
          "Resource": [
              "arn:aws:s3:::bucket-name/*"
          ]
      }
  ]
}
```

L'activation de l'enregistreur de session sur le portail de votre navigateur WorkSpaces sécurisé peut entraîner des frais de la part d'Amazon S3. Pour plus d'informations, consultez Tarification Amazon S3.

Pour plus d'informations sur les événements liés à la session capturés par Session Logger, consultez. the section called "Événements de session dans Session Logger"

Compartiments S3 avec chiffrement KMS (facultatif)

WorkSpaces Secure Browser Session Logger prend entièrement en charge les compartiments Amazon S3 lorsque le AWS KMS chiffrement est activé. Pour garantir une fonctionnalité de journalisation appropriée avec votre compartiment Amazon S3 chiffré, vous devez accorder à Session Logger les autorisations nécessaires pour utiliser votre AWS KMS clé.

Ajoutez la politique suivante à votre configuration de AWS KMS clé :

```
{
  "Sid": "Session Logger",
  "Effect": "Allow",
  "Principal": {
    "Service": "workspaces-web.amazonaws.com"
  },
  "Action": [
    "kms:Encrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*"
},
```

Dans la AWS console, sélectionnez le portail WorkSpaces Secure Browser à partir duquel vous collecterez les événements, puis choisissez l'onglet Session Logger et Modifier.

Entrez les informations suivantes pour configurer l'enregistreur de session pour le portail :

- Emplacement S3 (obligatoire) : nom de votre compartiment Amazon S3 dans lequel les événements seront diffusés.
- Préfixe clé (facultatif) : dossier dans lequel les événements sont transmis. Si le dossier n'existe pas, il sera créé. Si le champ est laissé vide, Session Logger écrira les événements à la racine du compartiment Amazon S3.

Sous Avancé, vous pouvez configurer les champs suivants :

- Filtre d'événements : il s'agit de la liste des événements surveillés par Session Logger.

  - Tous : la sélection de cette option signifie que tous les événements actuels et futurs seront surveillés
  - Inclure : cela vous permet de sélectionner manuellement des événements spécifiques à surveiller. Seuls les événements explicitement sélectionnés seront enregistrés. Les nouveaux événements introduits dans les futures mises à jour ne seront pas surveillés, sauf s'ils sont ajoutés manuellement à la sélection.
- Format de fichier
  - JSON (par défaut) : il s'agit d'un format de fichier dans lequel chaque fichier journal est présenté sous la forme d'un tableau d'événements. Nous recommandons ce format pour la plupart des cas d'utilisation.
  - JSONLines: Il s'agit d'un format de fichier optimisé pour Amazon Athena.
- Structure des dossiers : elle détermine le mode de stockage des fichiers journaux.
  - Plat (par défaut) : tous les fichiers journaux se trouvent dans un seul dossier.
  - Imbriqués par date : les fichiers journaux sont organisés en dossiers par date et heure. Partitionné pour Amazon Athena et optimisé pour les requêtes Amazon Athena.

Vous pouvez tester la configuration de l'enregistreur de session et vous assurer que l'enregistreur de session fonctionne correctement. Une fois la configuration terminée, le système tente d'écrire un fichier de test nommé `_workspaces_secure_browser.tmp` dans le compartiment et le dossier Amazon S3 spécifiés. Cela sert à valider à la fois la fonctionnalité de journalisation et la configuration des autorisations.

Vous pouvez également exécuter une session de test en démarrant une session Secure Browser sur le portail et en utilisant le navigateur comme vous le feriez normalement. L'enregistreur de session écrit des fichiers journaux dans votre compartiment Amazon S3 configuré toutes les 15 minutes pendant une session active ou à la fin de la session.

Après avoir terminé la session ou attendu le prochain intervalle de journalisation, vérifiez le compartiment Amazon S3 pour confirmer que les fichiers journaux de votre session ont été générés et stockés comme prévu.

Configuration de la journalisation des accès utilisateur pour Amazon WorkSpaces Secure Browser

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?.

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?.

Gestion de la politique du navigateur dans Amazon WorkSpaces Secure Browser

Vous pouvez définir n'importe quelle politique de navigateur personnalisée à l'aide des politiques Chrome disponibles pour la dernière version stable de WorkSpaces Secure Browser. Lorsque vous définissez une politique dans le portail WorkSpaces Secure Browser, celle-ci s'applique à toutes les sessions gérées par ce portail Web.

Il existe plus de 300 régles applicables à un portail web. Pour plus d'informations, y compris la liste complète des règles de Chrome, consultez la liste des politiques de Chrome Enterprise.

Vous pouvez définir une politique Chrome de trois manières :

1. Utilisation de l'éditeur visuel dans le portail Web

   En utilisant la vue console pour créer un portail Web, vous pouvez appliquer certaines des règles les plus courantes dans l'éditeur visuel :

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

- Favoris et dossiers de favoris

2. Utilisation de l'éditeur JSON dans le portail Web

   Vous pouvez également ajouter ou modifier directement des politiques en utilisant l'éditeur JSON au lieu de l'éditeur visuel.

   Pour connaître le format spécifique d'une politique, reportez-vous à la liste des règles de Chrome Enterprise.

3. Téléchargement d'un fichier JSON sur le portail Web

   Vous pouvez également importer les politiques Chrome utilisées dans votre organisation en chargeant un fichier JSON sur le portail Web.

   Pour plus de détails, veuillez consulter the section called "Tutoriel : définition d'une politique de navigateur personnalisée"

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 de plus amples informations, veuillez consulter the section called "Modification de la politique de navigation de base".

Rubriques

- Tutoriel : Configuration d'une politique de navigateur personnalisée dans Amazon WorkSpaces Secure Browser
- Modification de la politique de navigation de base dans Amazon WorkSpaces Secure Browser

Tutoriel : Configuration d'une politique de navigateur personnalisée dans Amazon WorkSpaces Secure Browser

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 le didacticiel suivant, vous allez créer un portail Web avec les contrôles de stratégie 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

Pour télécharger votre fichier JSON de politique Chrome, vous devez créer un portail WorkSpaces Secure Browser. Pour de plus amples informations, veuillez consulter the section called "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.
   - RestoreOnStartupURLs— 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 un URLs signet.
   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 le démarrage URLs. 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 définit l'`RestoreOnStartup`action à effectuer pour ouvrir une liste de URLs . Vous pouvez également utiliser d'autres actions lors de votre démarrage URLs. Pour en savoir plus, consultez Liste de règles Chrome Enterprise.
   b. Réglé sur `RestoreOnStartup`URLs 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 navigation de base dans Amazon WorkSpaces Secure Browser

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.

La ligne de base `URLAllowlist` et `URLBlocklist` les politiques ne peuvent pas être remplacées. Notez que le fichier de politique de navigateur JSON associé à votre portail Web ne contiendra pas

ces politiques de base. Pour voir la liste complète de toutes les politiques appliquées et de leurs valeurs, accédez à « chrome : //policy » depuis une session de navigation à distance.

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`.

Configuration de l'éditeur de méthode de saisie pour Amazon WorkSpaces Secure Browser

Un éditeur de méthode de saisie (IME) est un utilitaire qui fournit à l'utilisateur final des options lui permettant de saisir du texte dans des langues utilisant une disposition de clavier autre qu'un clavier QWERTY. IMEs aider les utilisateurs à saisir du texte dans des langues comportant des ensembles linguistiques plus importants et plus complexes, tels que 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 :

- Toutes les langues
  - Pour parcourir les IME (ou passer à la bonne disposition de clavier), appuyez sur Shift+Control+Left Alt.
  - Pour accéder aux paramètres de langue et de saisie, utilisez le sélecteur de langue sur la barre du panneau supérieur. S'il n'est pas visible, activez-le via la barre d'outils → Préférences → Général → Méthode de saisie au clavier.
- Japonais
  - Pour les utilisateurs de macOS : si vous utilisez une source d'entrée américaine, il est possible que vous rencontriez des problèmes de saisie. Pour résoudre ce problème :
    1. Sélectionnez une source d'entrée japonaise (par exemple, japonaise - Kana ou japonaise - Romaji) au lieu de la source d'entrée américaine sur votre macOS.
    2. Dans la session WorkSpaces Secure Browser, accédez à la barre d'outils → Préférences → Clavier → Paramétrage de la touche Option et sélectionnez Utiliser l'option () comme touche Alt de la télécommande (Mac) pour garantir le bon fonctionnement des raccourcis clavier.
  - Conversion des caractères d'entrée
    - Pour convertir des caractères en hiragana, appuyez sur. F6
    - Pour convertir des caractères en Katakana, appuyez sur. F7
    - Pour convertir des caractères en Hankaku Katakana (Katakana demi-largeur), appuyez sur F8
    - Pour convertir les caractères en latin, appuyez surF10.
    - Pour convertir les caractères en Wide Latin, appuyez surF9.
  - Commutation des modes d'entrée
    - Pour passer de Hiragana à Katakana, appuyez sur. Alt/Option+K
    - Pour passer de Katakana à Hankaku Katakana, appuyez sur. Alt/Option+K
    - Pour passer du Hankaku Katakana (Katakana demi-largeur) au Hiragana, appuyez sur. Alt/Option+K
    - Pour passer d'un mode japonais ou d'un mode latin étendu à un mode latin, appuyez surAlt/Option+L.
    - Pour passer du latin au latin large, appuyez surAlt/Option+L.

    - Pour passer de n'importe quel mode à la saisie directe, appuyez surHenkaku/Zenkaku key.
    - Pour revenir de Direct Input à Hiragana, appuyez sur. Henkaku/Zenkaku key
- Coréen
    - Pour sélectionner Hangul, appuyez sur Shift+Space.
    - Pour sélectionner Hanja, appuyez sur F9.

Pour désactiver le clavier virtuel lors de vos sessions WorkSpaces Secure Browser, contactez Support.

Configuration de la localisation en session pour Amazon WorkSpaces Secure Browser

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

1. La ForcedLanguagespolitique dans les paramètres du navigateur du portail Web. Pour de plus amples informations, veuillez consulter 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

Rubriques

Codes de langue pris en charge pour Amazon WorkSpaces Secure Browser

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)

Sélection des langues dans les paramètres du navigateur de l'utilisateur

Pour définir les paramètres du navigateur local d'un utilisateur, suivez les étapes appropriées.

- 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.

Gestion des contrôles d'accès IP dans Amazon WorkSpaces Secure Browser

> **Important**
>
> Les contrôles d'accès IP ne sont pris en charge que IPv4. Les utilisateurs se connectant IPv6 uniquement à partir de réseaux seront bloqués.

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 contrôle 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.

Rubriques

Création d'un groupe de contrôle d'accès IP dans Amazon WorkSpaces Secure Browser

> **Important**
>
> Les contrôles d'accès IP ne sont pris en charge que IPv4. Les utilisateurs se connectant IPv6 uniquement à partir de réseaux seront bloqués.

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.

Associer un paramètre d'accès IP à un portail Web dans Amazon WorkSpaces Secure Browser

> **Important**
>
> Les contrôles d'accès IP ne sont pris en charge que IPv4. Les utilisateurs se connectant IPv6 uniquement à partir de réseaux seront bloqués.

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 "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 contrôle d'accès IP dans Amazon WorkSpaces Secure Browser

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.

Supprimer un groupe de contrôle d'accès IP dans Amazon WorkSpaces Secure Browser

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.

Gestion de l'extension d'authentification unique dans Amazon WorkSpaces Secure Browser

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.

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.

Les utilisateurs sont invités à installer l'extension lorsqu'ils se connectent à un portail. Pour en savoir plus sur l’expérience utilisateur avec l’extension, consultez the section called “Extension d’authentification unique”.

Rubriques

- Identification des domaines pour l'extension d'authentification unique dans Amazon WorkSpaces Secure Browser
- Ajout de l'extension d'authentification unique à un nouveau portail Web dans Amazon WorkSpaces Secure Browser
- Ajout de l'extension d'authentification unique à un portail Web existant dans Amazon WorkSpaces Secure Browser
- Modifier ou supprimer l'extension d'authentification unique dans Amazon WorkSpaces Secure Browser

Identification des domaines pour l'extension d'authentification unique dans Amazon WorkSpaces Secure Browser

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	Domain
Okta	okta.com
Entrez votre identifiant	microsoftonline.com
AWS Identity Center	awsapps.com
Un seul identifiant	onelogin.com

IdP	Domain
Duo	duosecurity.com

Ajout de l'extension d'authentification unique à un nouveau portail Web dans Amazon WorkSpaces Secure Browser

Pour autoriser l'extension lors de la création d'un nouveau portail Web, procédez comme suit.

1. Suivez les étapes décrites dans the section called "Création d'un portail Web" jusqu'à the section called "Paramètres utilisateur".
2. À l'étape 1 de the section called "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 "Paramètres utilisateur" et les sections restantes dans the section called "Création d'un portail Web" pour créer votre portail web.

Ajout de l'extension d'authentification unique à un portail Web existant dans Amazon WorkSpaces Secure Browser

Pour ajouter l'extension à un portail Web existant, procédez comme suit.

1. Ouvrez la console WorkSpaces Secure Browser à la https://console.aws.amazon.com/workspaces-web/maison.
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.

Modifier ou supprimer l'extension d'authentification unique dans Amazon WorkSpaces Secure Browser

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

1. Ouvrez la console WorkSpaces Secure Browser à la https://console.aws.amazon.com/workspaces-web/maison.
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.

Filtrage du contenu Web dans Amazon WorkSpaces Secure Browser

Le filtrage du contenu Web est une fonctionnalité de sécurité et de conformité qui permet à votre entreprise de définir des politiques et de réglementer l'accès au contenu dans WorkSpaces Secure Browser. Avec le filtrage du contenu Web, vous pouvez spécifier quels utilisateurs URLs finaux sont autorisés à accéder ou à bloquer des catégories spécifiques URLs ou de domaines afin de restreindre l'accès, en répondant aux exigences critiques en matière de sécurité et de conformité réglementaire.

> **Note**
>
> Bien que vous puissiez configurer des politiques de filtrage d'URL via les politiques de Chrome pour bloquer ou autoriser des domaines spécifiques, nous ne recommandons pas cette approche car les actions issues des politiques de Chrome ne seront pas capturées dans le cadre des fonctionnalités de journalisation du service. Pour une surveillance complète et des rapports de conformité, utilisez les politiques de filtrage du contenu Web décrites sur cette page.

Rubriques

Restreindre la navigation à des informations spécifiques URLs

Vous pouvez mettre en œuvre une politique de « refus par défaut » dans laquelle seuls les sites Web explicitement approuvés URLs sont accessibles. Il est idéal pour les environnements de haute sécurité où l'accès à Internet doit être étroitement contrôlé et où chaque site autorisé a été approuvé en fonction des besoins commerciaux et de la conformité en matière de sécurité.

Dans la AWS console, sous Filtrage des URL :

- Accédez à la liste de blocage et sélectionnez le bouton Bloquer tout URLs
- Sous Liste d'autorisations, cliquez sur Ajouter une URL pour ajouter une URL qui sera répertoriée comme autorisée pour votre utilisateur final. Ajoutez une entrée par URL.
- Cliquez sur Enregistrer

Blocage spécifique URLs

Vous pouvez trouver un équilibre entre sécurité et productivité en maintenant un accès Internet ouvert tout en bloquant les sites problématiques connus. Il convient aux organisations qui font confiance à leurs utilisateurs mais souhaitent empêcher l'accès à des menaces spécifiques ou à du contenu inapproprié sans trop restreindre les activités commerciales légitimes.

Dans votre AWS console, sous Filtrage d'URL :

- Naviguez vers Bloqué URLs
- Sélectionnez Ajouter une URL, puis entrez l'URL à bloquer. Ajoutez une entrée par URL que vous souhaitez bloquer
- Cliquez sur Enregistrer

Catégories de blocage

En plus de bloquer des groupes spécifiques URLs, vous pouvez également bloquer automatiquement des groupes URLs en fonction de catégories de contenu. Cela est utile pour les entreprises qui ont besoin d'une couverture complète contre différents types de contenus inappropriés ou risqués sans avoir à identifier et à bloquer manuellement des sites individuels.

Dans votre AWS console, sous Filtrage d'URL :

- Accédez aux catégories bloquées et cliquez sur Ajouter des catégories
- Sélectionnez la catégorie que vous souhaitez bloquer
- Vous pouvez faire des exceptions à ces catégories en les ajoutant URLs à la liste d'autorisation. Pour cela, cliquez sur Ajouter une URL et entrez entry/ies celle que URLs vous souhaitez autoriser. Même s'ils figurent dans les catégories, les utilisateurs finaux pourront consulter le URLs.
- Cliquez sur Enregistrer

Les catégories suivantes peuvent être sélectionnées. Vous pouvez sélectionner une, plusieurs ou toutes les catégories.

Catégories de filtrage disponibles

Thème	Catégorie	Description
Contenu réservé aux adultes et inapproprié	Nudité (Nudity)	Sites contenant des images ou des illustrations de nu à caractère non sexuel.
Contenu réservé aux adultes et inapproprié	Pornographie	Sites présentant un contenu sexuel explicite ou du matériel provocateur sur la nudité.
Contenu réservé aux adultes et inapproprié	Éducation sexuelle	Ressources sur la santé et la sexualité adaptées à l'âge et examinées médicalement.
Contenu réservé aux adultes et inapproprié	Insipide	Contenu inapproprié pour les enfants non couverts par d'autres catégories.

Thème	Catégorie	Description
Communication et réseaux sociaux	Chat	Plateformes de messagerie privée et de groupe en temps réel.
Communication et réseaux sociaux	Messagerie instantanée	Services de messagerie privés.
Communication et réseaux sociaux	Réseau professionnel	Plateformes de création de relations axées sur les entreprises.
Communication et réseaux sociaux	Réseautage social	Plateformes d'interaction avec les utilisateurs pour partager du contenu et des expériences personnels.
Communication et réseaux sociaux	E-mail basé sur le Web	Services de messagerie accessibles par navigateur, y compris les cartes électroniques et les systèmes de vœux.
Divertissement	Jeux	Ressources de jeu récréatives, y compris les jeux vidéo, les puzzles et les activités autres que le jeu.
Divertissement	Partage d'images	Plateformes de contenu visuel offrant des fonctionnalités d'hébergement, de recherche et de partage.
Divertissement	De pair à pair	Fournisseurs d'applications de partage de fichiers et outils logiciels associés.
Contenus dangereux et illégaux	Activité criminelle	Des instructions ou du matériel faisant la promotion d'actes illégaux.
Contenus dangereux et illégaux	Piratage	Outils d'accès au système non autorisés et ressources d'exploitation du réseau.

Thème	Catégorie	Description
Contenus dangereux et illégaux	Drogue illégale	Contenu faisant la promotion de la consommation de drogues à des fins récréatives ou de la toxicomanie.
Contenus dangereux et illégaux	Logiciel illégal	Matériel protégé par des droits d'auteur non autorisé et distribution de logiciels malveillants.
Contenus dangereux et illégaux	Violence	Contenu incitant à porter atteinte à l'intégrité physique ou présentant du matériel graphique.
Contenus dangereux et illégaux	Armes	Ressources relatives à l'utilisation légitime d'armes à feu à des fins sportives et récréatives.
Comportements à risque	Cultes	Contenu spirituel et métaphysique non traditionnel.
Comportements à risque	Jeu	Activités et informations liées aux paris.
Comportements à risque	Haine et intolérance	Contenu promouvant un biais à l'encontre des caractéri stiques protégées.
Comportements à risque	Tricherie scolaire	Services d'assistance scolaire et d'achèvement des devoirs non autorisés.
Comportements à risque	Automutilation	Contenu faisant la promotion de comportements autodestructeurs ou évoquant des comportements autodestructeurs
Technologie et IA	Sites de téléchargement	Plateformes d'hébergement de logiciels, d'applications et de ressources numériques.
Technologie et IA	IA générative	Ressources technologiques sur l'IA et l'apprentissage automatique.

Thème	Catégorie	Description
Technologie et IA	Domaines parqués	Nombre minimal de domaines de contenu utilisés pour la publicité ou la vente de domaines.
Technologie et IA	Streaming multimédia et téléchargements	Plateformes de contenu audio/vidéo, y compris la musique, les vidéos et la radio Internet.

Exemple de URLs

Les types suivants URLs peuvent être fournis dans le AllowedUrls ou BlockedUrls

Type	Exemple
Domain	example.com
Sous-domaine	login.exemple.com
Chemin	exemple.com/myvideos
Paramètre de la demande	exemple.com/ ? paramètre=123

Transférer les politiques de Chrome

Si vous avez déjà défini des règles Chrome pour autoriser ou bloquer des domaines spécifiques, nous vous recommandons de les transférer vers la fonctionnalité de filtrage du contenu Web.

La fonctionnalité de filtrage du contenu Web détectera toutes URLAllow URLBlock les politiques qui s'appliquent à une session WorkSpaces Secure Browser et le signalera dans la AWS console.

Pour transférer les politiques de Chrome pour URLAllowlist et/ou/ou URLBlocklist :

- Dans votre AWS console, sous Filtrage d'URL, cliquez sur Consulter les politiques de Chrome (si le bouton Vérifier les politiques de Chrome ne s'affiche pas, cela signifie que les politiques de Chrome ne s'appliquent pas actuellement à l'autorisation d'URL ou URLBlock)
- Sous la superposition, consultez les politiques de Chrome
- Cliquez sur Transférer

Les politiques Chrome seront supprimées de l'éditeur JSON sous Paramètres de stratégie et de nouvelles URLs seront automatiquement ajoutées à la fonctionnalité de filtrage du contenu Web.

Liens profonds dans Amazon WorkSpaces Secure Browser

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.

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.

Rubriques

Configuration de liens profonds dans Amazon WorkSpaces Secure Browser

Pour autoriser les liens profonds, choisissez Autorisé lors de la création 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 %2F%3Fquery %Dtrue. https%3A%2F%2Fwww.example.com

Un lien profond peut en contenir jusqu'à 10 URLs, délimités par une virgule. Par exemple :

https ://<uuid>.workspaces-web.com/ ? https%3A%2F%2Fwww.example.com DeepLinks= %F %3Fquery%Dtrue, %F%3Fquery%Dtrue2, %F%3Fquery%Dtrue3, %F%F%Fquery%Dtrue4. https%3A%2F%2Fwww.example.com https%3A%2F%2Fwww.example.com https%3A%2F %2Fwww.example.com

Pour plus d'informations sur l'autorisation des liens profonds, consultezthe section called “Paramètres utilisateur”.

Utilisation du filtrage d'URL pour les liens profonds dans Amazon WorkSpaces Secure Browser

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. <uuid>Pour ce faire, ajoutez l'URL à une URL de portail répertoriée comme suit, où UUID est l'identifiant du portail : https ://.workspaces-web.com/ ? DeepLinks= %2F%3F%3Fquery%3Dtrue https%3A%2F%2Fwww.example.com

Pour plus d'informations, voir the section called “Filtrage du contenu Web” Autoriser ou bloquer l'accès aux sites Web.

Utilisation du tableau de bord de gestion des sessions dans Amazon WorkSpaces Secure Browser

Utilisez le tableau de bord de gestion des sessions de votre console WorkSpaces Secure Browser pour surveiller et gérer les sessions actives et complètes.

Accès au tableau de bord

Pour accéder au tableau de bord, procédez comme suit.

Pour accéder au tableau de bord

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, puis choisissez votre portail Web.
3. Choisissez l'onglet Session ou choisissez Afficher les sessions pour ouvrir le tableau de bord dans un panneau séparé ci-dessous.

Filtres de tableau de bord

Dans le panneau des sessions, vous pouvez filtrer les sessions en fonction des propriétés ou valeurs suivantes :

- Statut
  - Actif — Indique qu'une session est en cours d'exécution. Pour terminer la session, voir ci-dessous.
  - Terminé — Indique qu'une session n'est plus active.
- Identifiant de session
- Username
- Heure de début de session

Terminer les sessions

Pour mettre fin à une session, procédez comme suit.

Pour mettre fin à une session

1. Sur le tableau de bord des sessions, sélectionnez la session que vous souhaitez arrêter.
2. Sélectionnez Résilier.
3. Les utilisateurs déconnectés perdent tout état de la session. Tous les onglets ouverts, l'historique du navigateur et les fichiers téléchargés sur le navigateur sécurisé sont recyclés.

Historique des sessions

Le tableau de bord contient les sessions des 35 derniers jours. Vous pouvez utiliser la CLI pour répertorier les sessions, avec ou sans filtre. L'historique des sessions est fourni au format JSON, que les administrateurs peuvent traiter, gérer et stocker dans un référentiel distinct.

Vous trouverez ci-dessous des exemples de commandes CLI pour gérer des sessions dans la région US-West-2 (Oregon).

Pour répertorier toutes les sessions d'un portail Web, exécutez la commande suivante :

aws workspaces-web list-sessions --portal-arn arn:aws:workspaces-web:us-west-2:<accountId>:portal/<portalId>

Pour répertorier toutes les sessions d'un utilisateur spécifique d'un portail Web, exécutez la commande suivante :

aws workspaces-web list-sessions --portal-arn arn:aws:workspaces-web:us-west-2:<accountId>:portal/<portalId> --username <username>

Protection des données en transit avec les points de terminaison FIPS et Amazon Secure Browser WorkSpaces

Par défaut, lorsque vous communiquez avec le service WorkSpaces Secure Browser en tant qu'administrateur via la console, l'interface de ligne de AWS commande (AWS CLI) ou un AWS SDK, ou pendant une session utilisateur, toutes les données en transit sont cryptées à l'aide du protocole TLS 1.2.

Si vous avez besoin de modules de chiffrement validés FIPS (Federal Information Processing Standard) 140-3 lorsque vous accédez à AWS via une interface de ligne de commande ou une API (interface de programmation), utilisez un point de terminaison FIPS. Lorsque vous utilisez un point de terminaison FIPS, toutes les données en transit sont cryptées à l'aide de normes cryptographiques conformes à la norme fédérale de traitement de l'information (FIPS) 140-3. Pour plus d'informations sur les points de terminaison FIPS, y compris une liste des points de terminaison WorkSpaces Secure Browser, consultez. https://aws.amazon.com/compliance/fips

Après la création d'un portail avec des points de terminaison FIPS, toutes les sessions utilisateur et les modifications administratives sont automatiquement effectuées à l'aide des points de terminaison FIPS 140-3. Vous pouvez utiliser la variable d'`AWS_USE_FIPS_ENDPOINT=true`environnement pour localiser les points de terminaison FIPS et envoyer des demandes avec le SDK. Voici un exemple.

```
$ export AWS_USE_FIPS_ENDPOINT=true
$ aws workspaces-web list-portal
```

Vous pouvez également utiliser l'`–endpoint-url`option pour envoyer des demandes directement aux points de terminaison FIPS. Voici un exemple de portail de liste d'appels dans la région US-West-2 (Oregon) :

```
$ aws workspaces-web list-portal --endpoint-url https://workspaces-web-fips.us-
west-2.amazonaws.com
```

Gestion des paramètres de protection des données dans Amazon WorkSpaces Secure Browser

Les paramètres de protection des données sont utilisés pour empêcher le partage des données au cours d'une session. Les paramètres peuvent être créés et appliqués à plusieurs portails.

Rubriques

Rédaction de données en ligne dans Amazon Secure Browser WorkSpaces

En ajoutant la rédaction de données en ligne à un portail, vous pouvez automatiquement prévoir et supprimer certaines données à partir d'une chaîne de texte affichée dans les pages Web. Vous pouvez créer des politiques de rédaction en choisissant parmi des modèles intégrés (tels que les numéros de sécurité sociale ou de carte de crédit), ou créer leurs propres types de données personnalisés à l'aide d'expressions régulières et de mots clés. Les politiques incluent des niveaux d'application configurables et des contrôles indiquant URLs où la rédaction doit être appliquée.

Les éléments suivants déterminent le moment où les données sont expurgées :

- Paramètres de protection des données - Les paramètres de protection des données sont le nom de la ressource qui inclut vos types de données et vos critères d'application. Pour utiliser cette ressource, créez d'abord vos paramètres, puis associez-les à un portail. Lorsque les utilisateurs lancent une session, vos paramètres sont appliqués pendant la session.

- Extension de navigateur en cours de session : lorsque vous associez des paramètres de rédaction à votre portail, le navigateur de session démarre avec une extension de navigateur imposée par le système qui applique vos paramètres. Les paramètres de protection des données appliquent la rédaction grâce à la correspondance de modèles (expressions régulières) et à la recherche par mot clé en fonction de votre niveau de confiance et de la configuration d'application des URL. Le contenu est prédit à partir de chaînes de texte et expurgé avant d'être affiché à l'écran. L'extension définit également des politiques de navigateur connexes qui régissent la capacité des utilisateurs à contourner la rédaction (telles que la désactivation de la navigation privée, l'accès aux outils de développement et l'inspection du réseau).

Les modifications de politique du navigateur Chrome suivantes sont appliquées par l'extension de navigateur en cours de session. Pour en savoir plus, consultez Liste de règles Chrome Enterprise.

- Appliquez la politique du navigateur pour empêcher les utilisateurs de consulter la session sans la supprimer :
  - IncognitoModeAvailability = 1
  - DeveloperToolsAvailability = 2
  - BrowserAddPersonEnabled= faux
  - BrowserGuestModeEnabled= faux
- L'extension empêche également les utilisateurs de télécharger des fichiers HTML depuis lesquels URLs les paramètres de protection des données sont appliqués en annulant l'événement de téléchargement.

En général, vous devez utiliser la rédaction pour des sites Web privés et structurés (tels que vos outils de gestion des clients, vos systèmes de billetterie ou vos wikis), et non pour une navigation publique non structurée (comme Facebook ou Google). Vous pouvez choisir parmi les types de données intégrés (voir la liste complète ci-dessous) ou définir des types de données personnalisés à l'aide de vos propres valeurs d'expressions régulières et de vos propres mots clés. Les administrateurs sont chargés de tester et de valider que chaque type de données, chaque niveau de confiance et chaque application des URL fonctionnent comme prévu. AWS ne peut garantir la compatibilité avec les sites Web ou applications personnalisés fournis par des tiers.

WorkSpaces Secure Browser ne prend actuellement pas en charge la rédaction de types de données pris en charge ou personnalisés dans des formats autres que le texte, y compris le texte dans les formats suivants :

- Images, telles que JPEG, PNG ou GIF
- Pages Web permettant aux utilisateurs d'utiliser le traitement ou l'édition de texte dynamiques, telles que Google Docs ou Sheets
- Des flux audio ou vidéo accessibles dans le navigateur, tels que YouTube des vidéos
- PDFs visualisé par le navigateur Chrome

N'utilisez pas la rédaction pour du contenu dans un format non pris en charge. Les administrateurs sont chargés de valider la compatibilité du site et du contenu avant d'accorder aux utilisateurs l'accès au contenu qu'ils ont l'intention de supprimer.

Configuration de rédaction par défaut dans Amazon WorkSpaces Secure Browser

La configuration de rédaction par défaut appliquera automatiquement un niveau de confiance et une application des URL pour tous les types de données intégrés dans les paramètres de protection des données. Vous avez la possibilité de remplacer la configuration par défaut lors de l'ajout d'un type de données intégré.

Les niveaux de confiance vous permettent d'affiner la logique de rédaction pour les types de données intégrés à l'aide d'une combinaison de format, de mots clés et de texte non formaté. Choisissez le niveau de rigueur pour la façon dont la rédaction est appliquée, y compris élevé, moyen ou faible. La valeur par défaut s'applique à tous les types de données, sauf si une dérogation est appliquée au niveau du type de données. En général, commencez par une configuration par défaut Medium, puis affinez en vérifiant que la rédaction est appliquée comme prévu sur vos sites.

Niveau de confiance	Description	Exemple
Élevée	Nécessite un modèle de texte mis en forme correspon dant pour que le contenu soit expurgé.	Le SSN du 123-45-6798 serait expurgé, contrairement au 123456789.
Moyenne	La rédaction prend en compte à la fois le texte formaté et non formaté, et ajoute un mot-clé associé à la logique.	Le numéro SSN du 123-45-67 98 serait supprimé. Le numéro de sécurité sociale 123456789 serait supprimé s'il était

Niveau de confiance	Description	Exemple
		détecté à proximité d'un mot clé (tel que « numéro de sécurité sociale »).
Faible	Rédaction appliquée à la fois pour le modèle formaté et pour le modèle non formaté sans mot-clé.	Les SSN dans les deux formats (123-45-6798 et 123456789) sont expurgés sans nécessiter de mot clé.

Vous devez définir la configuration de rédaction par défaut pour tous les types de données. Choisissez parmi les options suivantes :

- Tout URLs
- Spécifique URLs
- Configuration avancée

La valeur par défaut s'applique à tous les types de données, sauf si une dérogation est appliquée au niveau du type de données. L'application des URL utilise une logique similaire à celle de la politique de Chrome pour gérer les listes d'autorisation et de blocage. Pour obtenir des conseils sur l'utilisation de bloquer et d'autoriser URLs, voir Autoriser ou bloquer l'accès aux sites Web. Pour de meilleurs résultats, ajoutez-les URLs à ces listes en suivant le format de filtre de liste de blocage de Chrome. Pour plus d'informations, voir Format de filtre de liste de blocage d'URL.

Rédaction en ligne de base dans Amazon Secure Browser WorkSpaces

La rédaction de données en ligne prend en charge les modèles intégrés (tels que les numéros de sécurité sociale et les numéros de carte de crédit), que vous trouverez dans la section Rédaction en ligne de base. Choisissez le ou les types de données dans le menu déroulant et spécifiez la valeur de remplacement pour chaque type de données. Tous les types de données suivent le modèle d'application de la configuration par défaut ci-dessus, mais vous pouvez choisir de remplacer le niveau de confiance et d'affiner le modèle d'application du domaine pour chaque type de données.

Pour saisir une autre valeur par rapport à la configuration par défaut, choisissez Confidence level override. Par exemple, lorsque la configuration par défaut est définie sur Medium, vous remarquerez peut-être lors des tests que l'un de vos types de données n'est pas expurgé de manière fiable. Vous

pouvez définir la dérogation sur Faible pour augmenter les chances de rédaction, sans modifier la logique utilisée pour vos autres types de données.

Pour affiner la façon dont la rédaction est appliquée URLs sans modifier la configuration par défaut, appliquez des dérogations à l'application des URL. Par exemple, vous pouvez configurer l'utilisation de remplacements d'URL pour appliquer la suppression des adresses e-mail dans votre système de gestion de la relation client, sans empêcher les utilisateurs d'accéder aux adresses e-mail figurant sur le site Web de l'annuaire de l'entreprise ou aux e-mails basés sur le Web.

Vous trouverez ci-dessous une liste des types de données et le modèle intégré correspondant IDs :

builtInPatternId	Type de données
awsAccessKey:	Clé d'accès AWS
awsSecretKey:	Clé secrète AWS
Numéros de cartes :	Numéros de carte de crédit
cryptomonnaie :	Adresses de crypto-monnaies
Numéro de coussin :	Numéro CUSIP
date :	Date
Dean Num :	Numéros DEA américains
date de naissance :	Date de naissance
Permis de conduire :	Permis de conduire américains
Adresse e-mail :	Adresse e-mail
un :	Numéro d'identification de l'employeur américain
Date d'expiration :	Date d'expiration de la carte de crédit
healthInsuranceNum:	Numéro de réclamation d'assurance maladie Medicare

builtInPatternId	Type de données
Code HIPAA :	Code HIPAA ICD-10
indivTaxId:	Numéro d'identification fiscale individuel américain
Adresse iPad :	Adresse IP
code PIN :	Numéros d'identification internationaux des valeurs mobilières
jet :	Jeton Web JSON
Coord de localisation :	Coordonnées de localisation
Adresse Mac :	Adresse MAC
medicareBeneficiaryId:	Numéro de bénéficiaire de Medicare
NPI :	Numéro d'identification national du fournisseur
et c :	Codes nationaux des médicaments (NDC)
Numéro de passeport :	Numéro de passeport américain
Numéro de téléphone :	Numéro de téléphone
Numéro de routage :	Numéro de routage ABA
ssn :	Numéro de sécurité sociale américain
Code SWIFT :	Code SWIFT
heure :	Heure
vin :	Numéro d'identification du véhicule américain

Rédaction en ligne personnalisée dans Amazon Secure Browser WorkSpaces

Les clients peuvent définir leurs propres modèles à l'aide d'expressions régulières, telles qu'une application interne personnalisée IDs. Pour créer votre modèle de rédaction intégré personnalisé, procédez comme suit :

1. Accédez à vos paramètres de protection des données.
2. Choisissez Rédaction intégrée personnalisée et ajoutez.
3. Entrez un nom pour le type de données personnalisé.
4. Entrez la valeur de votre expression régulière.
   - Les valeurs des expressions régulières doivent correspondre à la syntaxe littérale des expressions JavaScript régulières. Pour plus d'informations, consultez la section Expressions régulières. Un exemple d'expression régulière est`/ex[am]+ple/i`.
   - Assurez-vous de tester vos modèles personnalisés sur les sites Web que vous prévoyez de soutenir. Si les modèles personnalisés sont écrits avec des erreurs, ils peuvent entraîner des problèmes de performances involontaires.
5. Spécifiez la valeur de remplacement.
6. Choisissez Plus d'options pour d'autres personnalisations facultatives, notamment les suivantes :
   - Ajoutez des mots clés pour affiner la logique de rédaction. Les mots clés peuvent améliorer la précision de l'application. Ajoutez des mots clés dans la syntaxe littérale des expressions régulières Javascript. Pour plus d'informations, consultez la section Expressions régulières.

     Par exemple, si vous créez un modèle de rédaction personnalisé pour un client IDs utilisé dans un système interne, vous pouvez l'ajouter `/client name/i` au champ de mot-clé pour informer la logique de numérisation et de détection.
   - Appliquez des dérogations à l'application des URL pour affiner la manière dont la rédaction est appliquée URLs, sans modifier la configuration par défaut.

     Par exemple, vous pouvez configurer l'utilisation de remplacements d'URL pour appliquer la suppression des adresses e-mail dans votre système de gestion de la relation client, sans empêcher les utilisateurs d'accéder aux adresses e-mail du site Web de l'annuaire de l'entreprise ou à la messagerie Web.
   - Entrez une description (facultatif) pour le type de données.

Création de paramètres de protection des données dans Amazon WorkSpaces Secure Browser

Vous pouvez créer des paramètres de protection des données dans WorkSpaces Secure Browser.

Pour créer des paramètres de protection des données

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 de gauche, sélectionnez Paramètres de protection des données.
3. Choisissez Créer des paramètres de protection des données.
4. Entrez un nom d'affichage (obligatoire) et une description (facultatif) pour le paramètre.
5. Sélectionnez les paramètres par défaut pour la rédaction en ligne. Vous pouvez définir les paramètres suivants :
   - Le niveau de rigueur de tous les types de données
   - Les domaines dans lesquels la rédaction doit être appliquée
6. Choisissez vos types de données de rédaction en ligne de base parmi les types pris en charge, ou créez un type de données personnalisé. Vous pouvez définir des dérogations pour chaque type de données, notamment le niveau de rigueur et les exceptions de domaine.
7. Ajoutez des balises (facultatif) pour les rapports.
8. Lorsque vous avez terminé, choisissez Save.

Associer les paramètres de protection des données dans Amazon WorkSpaces Secure Browser

Vous pouvez associer des paramètres de protection des données dans WorkSpaces Secure Browser.

Pour associer un paramètre de protection des données à un portail existant

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 de gauche, sélectionnez Portails Web.
3. Sélectionnez le portail web, puis choisissez Modifier.

4. Sous Paramètres de protection des données, sélectionnez le paramètre de votre portail.
5. Choisissez Enregistrer.

Pour associer un paramètre de protection des données lors de la création d'un nouveau portail, procédez comme suit.

Pour associer un paramètre de protection des données lors de la création d'un nouveau portail

1. Suivez les instructions the section called “Création d'un portail Web” pour créer un portail, jusqu'à ce que vous arriviez au paramètre de protection des données.
2. Choisissez votre paramètre de protection des données dans le menu déroulant.
3. Suivez les étapes décrites the section called “Création d'un portail Web” pour terminer la création de votre portail.

Pour créer un paramètre de protection des données lors de la création d'un nouveau portail, procédez comme suit.

Pour créer un paramètre de protection des données lors de la création d'un nouveau portail

1. Suivez les instructions the section called “Création d'un portail Web” pour créer un portail, jusqu'à ce que vous arriviez au paramètre de protection des données.
2. Choisissez les paramètres de protection des données dans le menu déroulant.
3. Entrez un nom d'affichage (obligatoire) et une description (facultatif) pour le paramètre.
4. Sélectionnez les paramètres par défaut pour la rédaction en ligne. Vous pouvez définir les paramètres suivants :
   - Le niveau de rigueur de tous les types de données
   - Les domaines dans lesquels la rédaction doit être appliquée
5. Choisissez vos types de données de rédaction en ligne de base parmi les types pris en charge, ou créez un type de données personnalisé. Vous pouvez définir des dérogations pour chaque type de données, notamment le niveau de rigueur et les exceptions de domaine.
6. Ajoutez des balises (facultatif) pour les rapports.
7. Lorsque vous avez terminé, choisissez Save.
8. Sélectionnez le bouton d'actualisation dans les paramètres de protection des données, puis choisissez votre paramètre de protection des données dans le menu déroulant.

9. Continuez à suivre les instructions de création de portail pour terminer la création de votre portail.

Modifier les paramètres de protection des données dans Amazon WorkSpaces Secure Browser

Vous pouvez modifier les paramètres de protection des données dans WorkSpaces Secure Browser.

Pour modifier les paramètres de protection des données

1. Ouvrez la console WorkSpaces Secure Browser à l'adressehttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Choisissez les paramètres de protection des données et le paramètre de protection des données que vous souhaitez modifier dans la vue de liste.
3. Vous pouvez mettre à jour le nom, la description, les paramètres par défaut, les types de données (pris en charge ou personnalisés) et appliquer des dérogations au niveau de confiance ou au domaine.
4. Choisissez Enregistrer.

Supprimer les paramètres de protection des données dans Amazon WorkSpaces Secure Browser

Vous pouvez supprimer les paramètres de protection des données dans WorkSpaces Secure Browser.

Pour supprimer les paramètres de protection des données

1. Si un portail est associé à un paramètre de protection des données, vous devez d'abord supprimer l'association avant de supprimer le paramètre de protection des données.
2. Ouvrez la console WorkSpaces Secure Browser à l'adressehttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
3. Choisissez les paramètres de protection des données et le paramètre de protection des données que vous souhaitez supprimer de la liste.
4. Sélectionnez Delete (Supprimer).

Personnalisation de l'image de marque dans Amazon WorkSpaces Secure Browser

Vous pouvez personnaliser les écrans de connexion et de chargement qui apparaissent à vos utilisateurs finaux en modifiant les éléments visuels, le contenu textuel et les conditions d'utilisation. La personnalisation de l'image de marque permet de créer une expérience cohérente qui correspond à l'identité de votre organisation.

Présentation

La personnalisation de l'image de marque vous permet de personnaliser les aspects suivants de l'expérience utilisateur :

- Éléments visuels : importez le logo, le favicon et le fond d'écran, puis sélectionnez des thèmes de couleurs correspondant à l'identité de votre marque.
- Contenu textuel : personnalisez les messages de bienvenue, le titre de l'onglet du navigateur et les autres champs de texte facultatifs pour conserver la voix de votre marque tout au long du processus de connexion. Si vous ne spécifiez pas de texte personnalisé pour certains champs, le texte par défaut sera utilisé. Pour en savoir plus, consultez the section called “Directives de personnalisation”.
- Conditions d'utilisation (facultatif) - Ajoutez les conditions d'utilisation de votre organisation que les utilisateurs doivent accepter avant de démarrer une session.

> **Note**
>
> Vous pouvez également personnaliser le nom de domaine de votre portail. Pour en savoir plus, consultez the section called “Domaine personnalisé”.

Rubriques

Configuration de la personnalisation de l'image de marque pour votre portail

Comment ça marche

Lorsque vous configurez la personnalisation de l'image de marque :

- Les éléments visuels et textuels sont appliqués à la fois à l'écran de connexion et à l'écran de chargement.
- L'onglet du navigateur affiche votre favicon et votre titre personnalisés.
- Les utilisateurs finaux verront vos modifications de personnalisation lorsqu'ils démarreront une nouvelle session. Dans certains cas, quelques minutes peuvent s'écouler avant que vos modifications ne soient visibles.
- Si les conditions d'utilisation sont configurées, les utilisateurs finaux doivent accepter les vôtres avant de démarrer leur session de streaming. Notez qu'ils seront demandés au début de chaque session.

Conditions préalables

Avant de commencer :

- Assurez-vous de disposer des autorisations nécessaires pour modifier les paramètres du portail, voirthe section called “AWS politiques gérées”.
- Préparez vos actifs de marque (logo, favicon, fond d'écran) conformément aux spécifications indiquées dansthe section called “Directives de personnalisation”.

Prise en main

Pour configurer la personnalisation de la marque, 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. Choisissez WorkSpaces Secure Browser, Portails Web, puis choisissez votre portail Web.
3. Sélectionnez votre portail et cliquez sur l'onglet Paramètres utilisateur.
4. Dans la section Personnalisation de l'image de marque, choisissez Modifier.
5. Configurez les sections suivantes selon vos besoins :

- Dans l'éditeur de contenu : téléchargez tous les éléments visuels (le logo de votre entreprise, votre favicon et un fond d'écran optionnel) et sélectionnez le thème de couleur. Vous pouvez télécharger les fichiers depuis votre ordinateur local ou depuis un compartiment S3. Pour plus d'informations sur la configuration des autorisations du compartiment S3, consultezthe section called “Configuration des autorisations du compartiment S3”.
- Dans l'éditeur de texte : personnalisez le texte qui apparaît sur l'écran de connexion.
- Dans l'éditeur des conditions d'utilisation, ajoutez éventuellement des termes que les utilisateurs doivent accepter.

6. Sélectionnez Enregistrer les modifications.

Pour obtenir des instructions détaillées sur chaque option de personnalisation, consultezthe section called “Directives de personnalisation”.

Configuration des autorisations du compartiment S3

Vous pouvez télécharger des fichiers de marque directement depuis votre ordinateur ou sélectionner des objets existants dans vos compartiments S3. Si vous choisissez de télécharger les fichiers des éléments visuels (le logo de votre entreprise, votre favicon et un fond d'écran) à partir d'un compartiment S3, assurez-vous de configurer les autorisations appropriées pour le compartiment S3.

Sélection d'objets S3 dans le même compte

Si votre utilisateur ou votre rôle IAM possède déjà `s3:GetObject` l'autorisation d'accéder au compartiment contenant vos actifs de marque, aucune configuration supplémentaire n'est requise.

Sélection d'objets S3 dans un autre compte

Pour sélectionner un compartiment S3 dans un autre AWS compte, vous devez configurer à la fois la politique de compartiment dans le compte source et la politique IAM dans votre compte administrateur.

Exemple de politique de compartiment (dans le compte source) :

Appliquez cette politique au compartiment S3 du compte source. *123456789012*Remplacez-le par votre identifiant de compte administrateur et *source-account-bucket-name* par le nom réel de votre bucket.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCrossAccountAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      },
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::source-account-bucket-name",
        "arn:aws:s3:::source-account-bucket-name/*"
      ]
    }
  ]
}
```

Exemple de politique IAM (dans votre compte administrateur) :

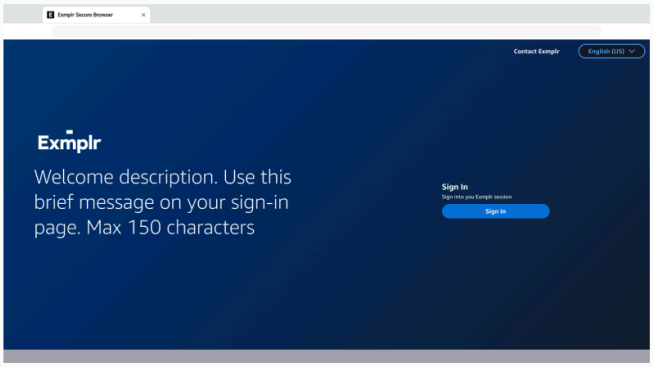
Associez cette politique à l'utilisateur ou au rôle IAM dans votre compte d'administrateur. *source-account-bucket-name*Remplacez-le par le nom réel du compartiment indiqué dans le compte source.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCrossAccountS3Access",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::source-account-bucket-name",
        "arn:aws:s3:::source-account-bucket-name/*"
      ]
    }
  ]
}
```

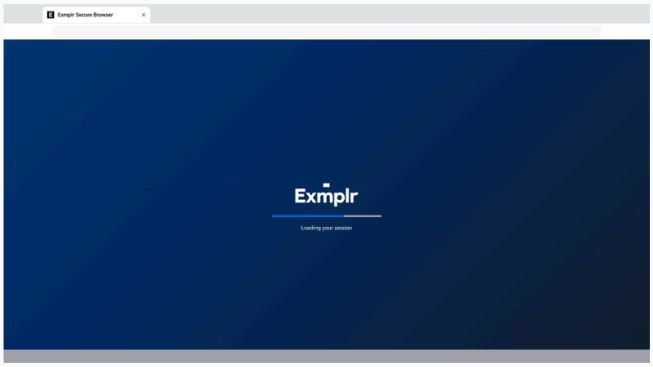
Pour des informations détaillées sur l'accès entre comptes, voir S3 Access accorde un accès entre comptes.

Directives de personnalisation

Personnalisez l'expérience de connexion et de chargement pour vos utilisateurs finaux en mettant à jour les éléments de marque et le texte sur les pages de connexion et de chargement. Vous pouvez modifier les éléments visuels tels que les logos et les fonds d'écran, modifier des éléments de texte tels que les messages de bienvenue et les en-têtes, et éventuellement configurer un accord de conditions d'utilisation que les utilisateurs doivent accepter avant de démarrer leur session.



Sign in Page

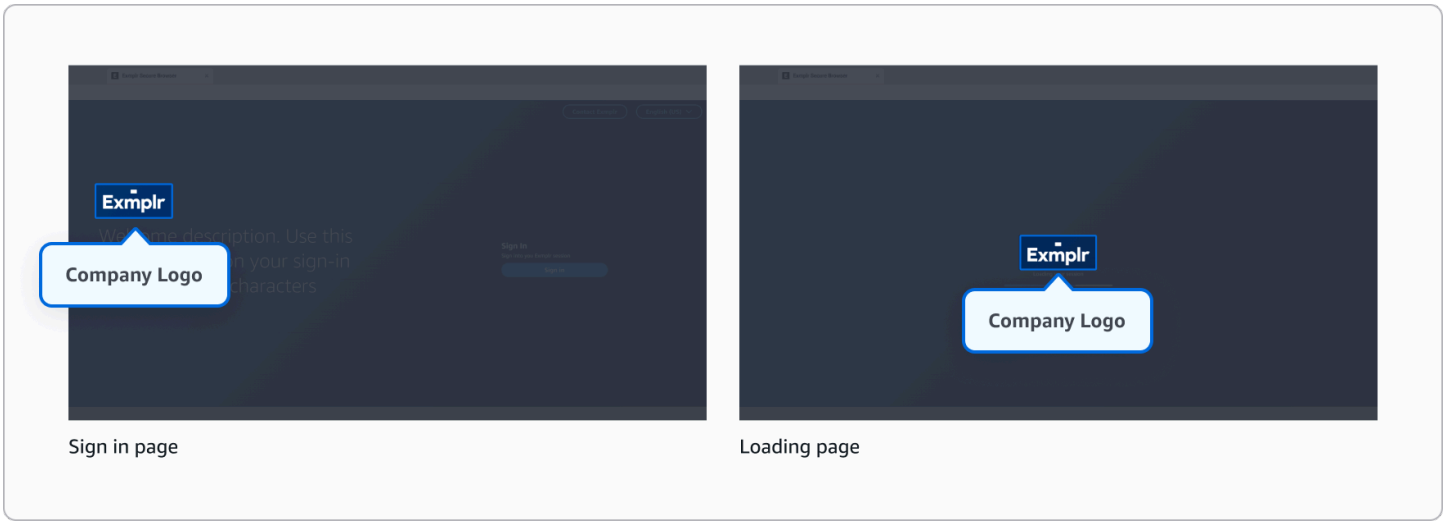


Loading Page

Éditeur de contenu

Logo de l'entreprise

Le logo apparaît sur l'écran de connexion et sur l'écran de chargement, offrant une marque cohérente tout au long de l'expérience utilisateur.

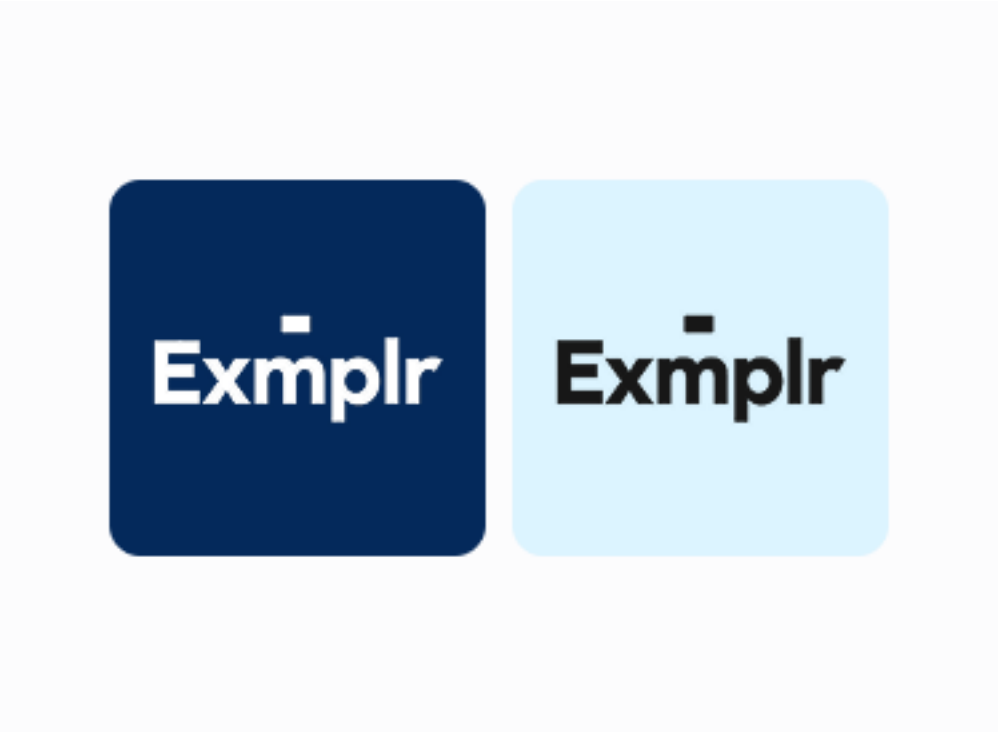


Sign in page

Loading page

- Formats pris en charge : JPG ou ICO ou PNG
- Taille maximale du fichier : 100 Ko

Faire



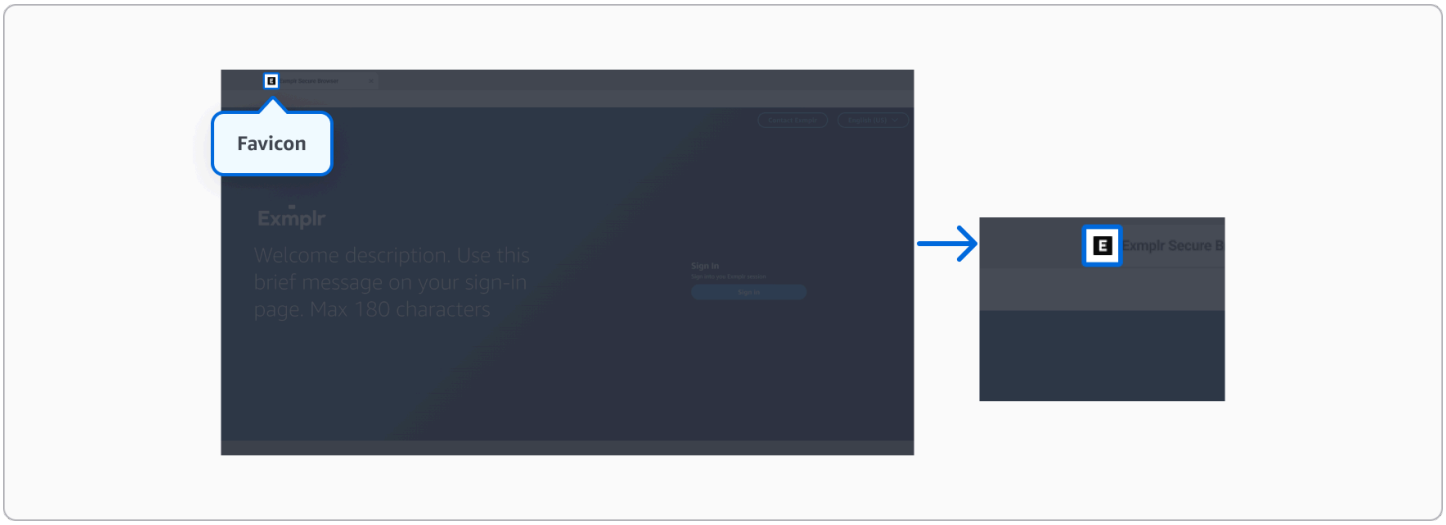
- Si vous avez différentes variantes de logo (telles que des couleurs ou des styles différents), choisissez celui qui offre le meilleur contraste avec le fond d'écran que vous avez sélectionné.

Ne

- N'ignorez pas les proportions lorsque vous redimensionnez votre logo.
- N'utilisez pas de logos mal dimensionnés au préalable car ils peuvent sembler déformés.

Favicon

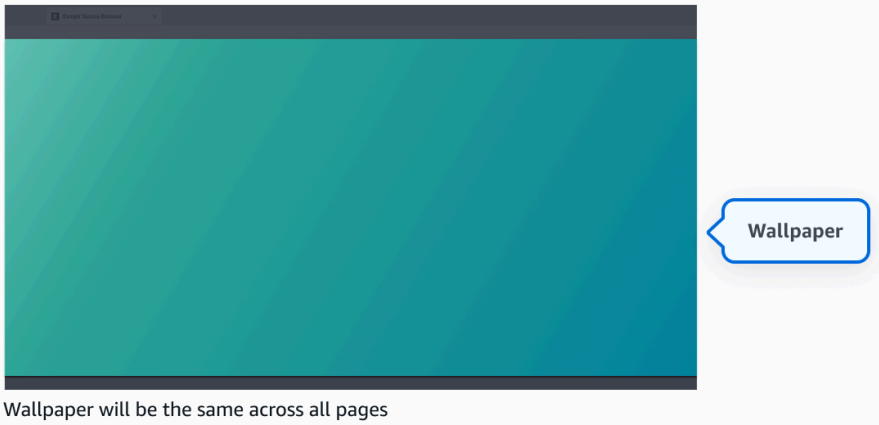
Un favicon est une petite icône qui apparaît dans les onglets du navigateur pour aider les utilisateurs à identifier votre application parmi plusieurs onglets ouverts.



- Formats pris en charge : JPG ou ICO ou PNG
- Taille maximale du fichier : 100 Ko
- Rapport hauteur/largeur recommandé : 1:1

Papier peint - facultatif

Le fond d’écran sert d’image de fond sur tous les écrans, créant ainsi une expérience visuelle cohérente. Si vous ne téléchargez pas de fond d'écran personnalisé, le fond d'écran par défaut illustré ci-dessous sera utilisé. Choisissez une image qui complète votre marque sans nuire à la lisibilité du contenu.



- Formats pris en charge : JPG ou PNG
- Taille de fichier maximale : 5 Mo
- Rapport hauteur/largeur recommandé : 16:9
- Résolution minimale recommandée : 1920 x 1080

Faire

- Utilisez des fonds d'écran subtils à faible contraste ou des images floues qui n'interfèrent pas avec le contenu du premier plan.
- Envisagez un positionnement prédéfini du texte pour éviter les zones encombrées derrière le texte.
- Utilisez les couleurs de la marque et utilisez des superpositions pour créer un meilleur contraste et une meilleure lisibilité.

Ne

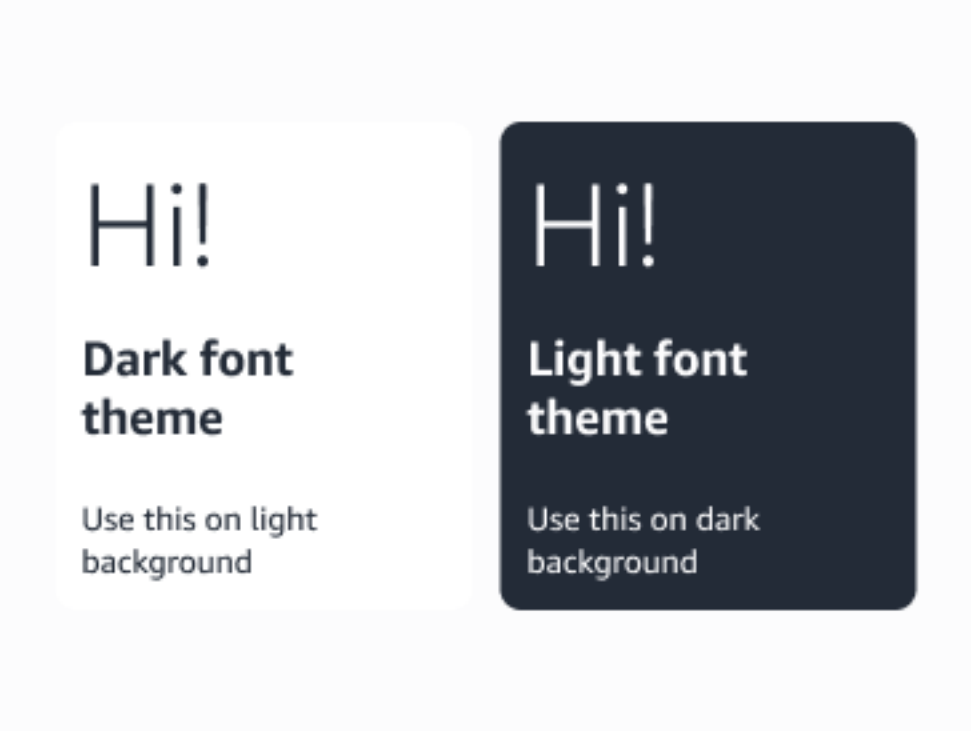
- N'utilisez pas d'images surchargées, saturées ou très détaillées juste derrière un texte important.
- N'utilisez pas d'images visuellement complexes ou d'images présentant des transitions nettes qui limiteraient la lisibilité avec des emplacements de texte prédéfinis.
- Ne vous fiez pas uniquement à la couleur pour séparer le texte de l'arrière-plan sans un contraste suffisant.

Thème de couleurs

Choisissez entre des thèmes clairs ou foncés qui reflètent les polices, les boutons et les modaux.

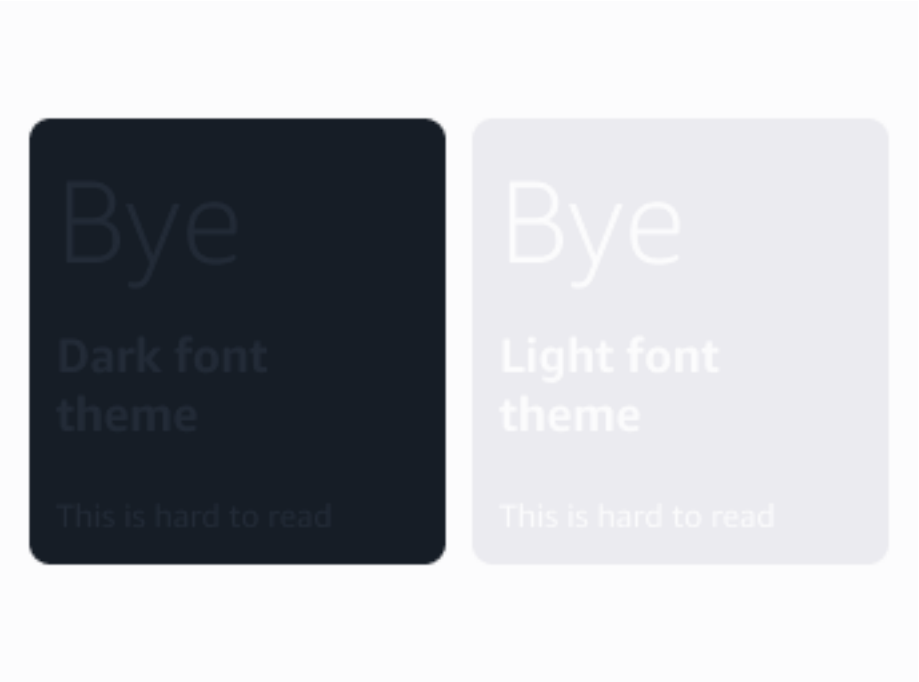
- Thème clair : idéal pour les arrière-plans sombres, offrant un contraste clair et réduisant la fatigue oculaire lorsque vous travaillez dans des environnements peu éclairés.
- Thème foncé : idéal pour les arrière-plans clairs, offrant un affichage confortable et un éblouissement réduit dans les environnements lumineux.

Faire



- Garantissez un fort contraste avec les éléments d'arrière/le papier peint.
- Utilisez un thème de couleur foncée sur des arrière-plans clairs.
- Utilisez un thème de couleur claire sur des arrière-plans sombres.

Ne



- Ne placez pas de polices claires ou foncées sur des images ou des fonds d'écran complexes.

Éditeur de texte

L’éditeur de texte vous permet de personnaliser le texte qui apparaît sur l’écran de connexion de vos utilisateurs finaux. Pour activer la personnalisation de la marque, vous devez ajouter au moins une langue.

Pour les nouveaux utilisateurs : nous détectons la langue préférée de votre navigateur et affichons la page du portail dans cette langue si vous l’avez configurée dans les langues de votre marque. Si la langue de votre navigateur n’est pas dans les langues que vous avez configurées, nous utilisons par défaut l’anglais (en-US) si disponible. Si vous n’avez pas configuré l’anglais, nous utilisons la première langue dans l’ordre alphabétique des langues que vous avez configurées.

Pour les utilisateurs récurrents : nous stockons les préférences linguistiques de votre session précédente dans un cookie de navigateur. Si cette langue figure dans les langues de marque que vous avez configurées, nous l’utilisons. Sinon, nous suivons la même logique de repli : anglais (en-US) si disponible, ou première langue configurée par ordre alphabétique.

Les paramètres régionaux (codes de langue) suivants sont pris en charge :

- Allemand (de-DE)
- Anglais (en-US)

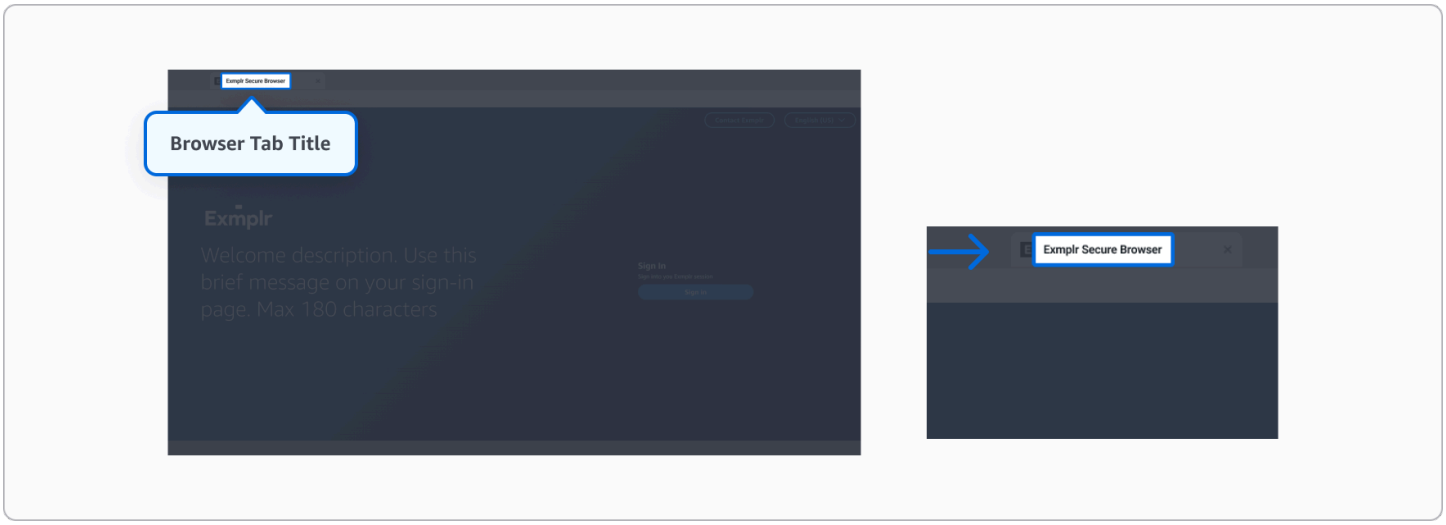
- Espagnol (es-ES)
- Français (fr-FR)
- Indonésien (id-ID)
- Italien (it-IT)
- Japonais (ja-JP)
- Coréen (ko-KR)
- Portugais (pt-PT)
- Chinois simplifié (zh-CN)
- Chinois traditionnel (zh-TW)

Pour des raisons de sécurité, les caractères suivants sont bloqués dans tous les champs de texte :

- < (inférieur à)
- > (supérieur à)
- & (esperluette)
- ' (apostrophe droite)
- ` (guillemet arrière/accent grave)
- ~ (tilde)
- \ (barre oblique inverse)

Titre de l'onglet du navigateur

Texte affiché dans l'onglet du navigateur. 25 caractères maximum.

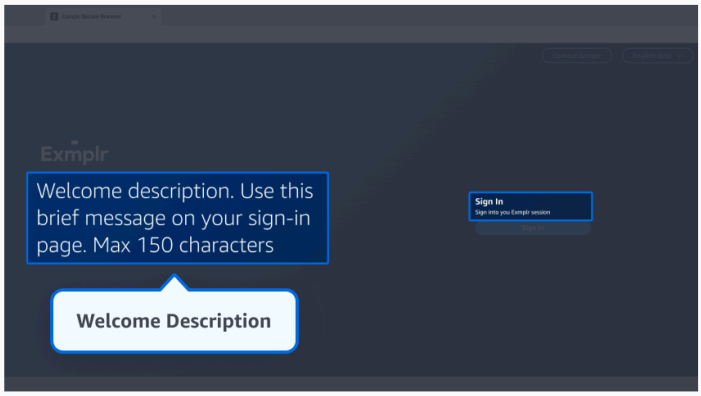


Recommandation

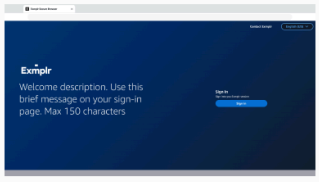
Pensez à utiliser des titres courts et clairs afin qu'ils restent lisibles même lorsque plusieurs onglets sont ouverts.

Description du message de bienvenue

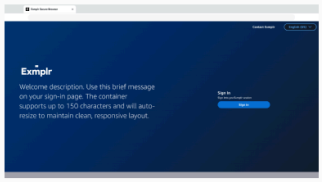
Brève description à côté du logo de votre entreprise sur l'écran de connexion. 150 caractères maximum.



Welcome description



Starting font sizing



Adapted sizing to Max characters

Recommandation

Veillez à ce que le texte soit concis pour une meilleure lisibilité. Notez qu'un texte plus long sera automatiquement redimensionné pour une taille de police plus petite, tandis que les messages plus courts s'afficheront de manière plus visible.

Section de contact

Bouton de contact : facultatif

Texte du bouton de contact sur l'écran de connexion. Si ce champ est laissé vide, « Contactez-nous » s'affichera. 30 caractères maximum.

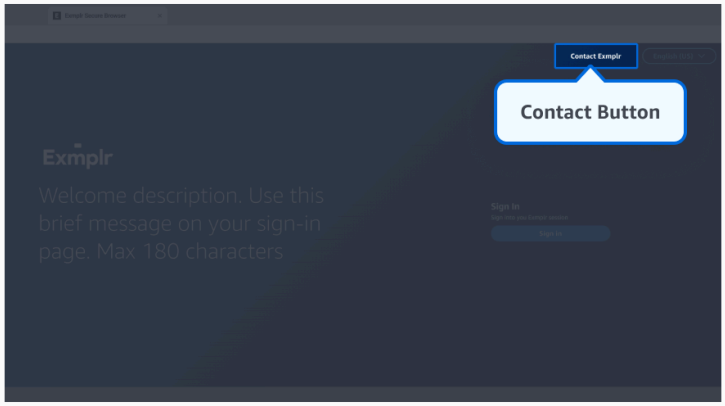
Lien de contact : facultatif

Texte du bouton de contact sur l'écran de connexion. Vous pouvez utiliser :

- URL HTTPS pour diriger les utilisateurs vers une page Web

- Un lien mailto : pour ouvrir le client de messagerie de l'utilisateur

S'il est laissé vide, le bouton de contact est masqué à l'écran.



Recommandation

Faites en sorte que le texte soit court, idéalement 2 à 3 mots.

Section de connexion

En-tête de connexion : facultatif

En-tête de la section de connexion de la page de connexion. Si ce champ est laissé vide, le message « Se connecter » s'affiche. 100 caractères maximum.

Description de connexion : facultatif

Texte de description de la section de connexion. Si ce champ est laissé vide, « Connectez-vous à votre session de navigation WorkSpaces sécurisée » s'affichera. 250 caractères maximum.

Bouton Se connecter : facultatif

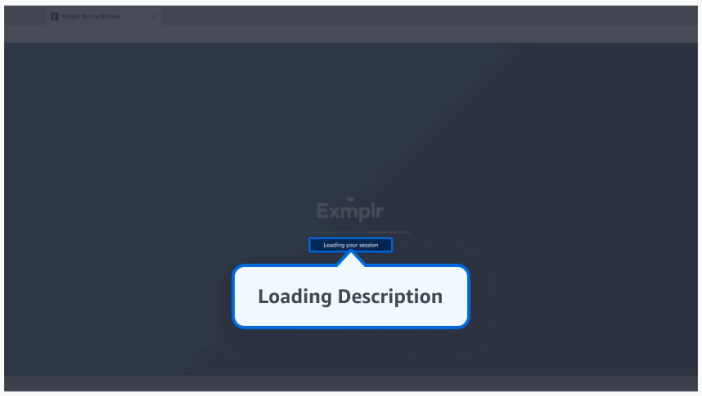
Texte affiché sur le bouton de connexion. Si ce champ est laissé vide, le message « Se connecter » s'affiche. 30 caractères maximum.

Recommandations

- Faites en sorte que le texte soit court.
- Sachez que le bouton de connexion dirige les utilisateurs vers le fournisseur d'identité configuré pour votre portail. Vous pouvez personnaliser le texte du bouton pour qu'il reflète votre fournisseur d'identité spécifique.

Description du chargement

Texte affiché lors de la connexion sur l'écran de chargement. Si ce champ est laissé vide, « Connexion en cours... » s'affiche. 300 caractères maximum.



Loading screen

Recommandation

Ce message n'est affiché que pendant le chargement de la session, de sorte que les utilisateurs finaux n'auront peut-être pas le temps de le lire. Essayez d'éviter de le rendre trop long.

Conditions d’utilisation : facultatif

Vous pouvez personnaliser les conditions d’utilisation que les utilisateurs finaux doivent consulter et accepter avant de démarrer une session de streaming. Ce contenu peut être ajouté en téléchargeant un fichier Markdown ou en utilisant l’éditeur Markdown intégré.

Les conditions d’utilisation sont présentées aux utilisateurs une fois qu’ils se sont connectés avec succès. Ils doivent parcourir le document dans son intégralité et cliquer sur le bouton « Accepter » pour accéder à leur session Secure Browser. Si l’utilisateur clique sur « Refuser », il est redirigé vers la page de connexion.

Notez qu’il s’agit d’un paramètre facultatif. Si vous n’ajoutez pas de conditions d’utilisation, les utilisateurs accèdent directement à leurs sessions après s’être connectés.

Formatage pris en charge :

- Styles de texte de base (gras, italique)
- En-têtes
- Listes ordonnées et non ordonnées
- Citations en blocs
- Règles horizontales
- Paragraphes et sauts de ligne simples

Pour des raisons de sécurité, les éléments suivants sont bloqués :

- Exécution de scripts et de code
- Éléments interactifs tels que des formulaires et des iframes
- Protocoles et chemins de fichiers non sécurisés
- Attributs et style HTML
- Liens externes et tableaux

N’oubliez pas que la taille de votre fichier de conditions d’utilisation ne doit pas dépasser 150 Ko.

Activation de WebAuthn la prise en charge de la redirection dans Amazon WorkSpaces Secure Browser

> **Warning**
>
> WebAuthn la redirection ne fonctionne que dans les sessions de navigateur où l'accès à Internet est activé. Assurez-vous que les paramètres réseau de votre portail autorisent l'accès à Internet pour WebAuthn que les fonctionnalités fonctionnent correctement.

WorkSpaces Secure Browser prend en charge WebAuthn (authentification Web) les sites Web accessibles au cours de la session de navigation à distance. Cela permet aux utilisateurs de s'authentifier sur des sites Web à l'aide de leurs clés de FIDO2 sécurité locales, de leurs authentificateurs biométriques et de leurs authentificateurs de plateforme lorsqu'ils naviguent dans leur session Secure Browser. WorkSpaces

> **Note**
>
> WebAuthn la redirection est disponible pour les utilisateurs finaux utilisant Google Chrome 136 (ou version ultérieure) ou Microsoft Edge 137 (ou version ultérieure). Cette fonctionnalité n'est pas disponible pour les navigateurs autres que Chromium tels que Safari ou Firefox. Pour activer WebAuthn la fonctionnalité de redirection, les administrateurs doivent configurer les deux :
>
> 1. Paramètres utilisateur du portail - Activez WebAuthn la redirection dans les paramètres du portail
> 2. Politiques de navigateur local pour l'utilisateur final : configurez la politique de WebAuthenticationRemoteDesktopAllowedOrigins navigateur sur les appareils des utilisateurs pour autoriser la redirection WebAuthn

Rubriques

Activation WebAuthn de la redirection dans les paramètres du portail

Pour activer WebAuthn la redirection pour les sites Web auxquels vous accédez au cours de la session de navigateur à distance, 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. Choisissez WorkSpaces Secure Browser, Portails Web, choisissez votre portail Web, puis sélectionnez Modifier.
3. Accédez à la section Paramètres utilisateur.
4. Sous Autorisations utilisateur, définissez Autoriser les utilisateurs à utiliser l'authentification locale dans leur session de portail sur Autorisé.
5. Choisissez Enregistrer pour appliquer la configuration.

Configuration de la politique de navigateur locale pour WebAuthn

Outre l'activation de WebAuthn la redirection dans les paramètres de votre portail, la politique du navigateur local doit être configurée pour autoriser la WebAuthn redirection entre l'appareil local de l'utilisateur et la session de navigateur distante et vice versa. Cette configuration est généralement gérée par les administrateurs informatiques pour les environnements d'entreprise ou par des utilisateurs individuels pour les scénarios BYOD.

La politique du navigateur doit inclure le domaine de contenu WorkSpaces Secure Browser de votre région. Ajoutez l'origine suivante à la `WebAuthenticationRemoteDesktopAllowedOrigins` politique en fonction de votre région :

`https://<region>.content.workspaces-web.com`

Par exemple, dans us-west-2 : `https://us-west-2.content.workspaces-web.com`

La méthode de configuration spécifique varie selon que vous gérez des navigateurs dans un environnement d'entreprise ou que vous configurez des appareils individuels pour les utilisateurs du BYOD. Pour plus d'informations sur la politique du navigateur, consultez la documentation relative à la politique de Chrome Enterprise et la documentation relative à la politique de Microsoft Edge.

> **Note**
>
> Le redémarrage du navigateur peut être nécessaire pour que la politique entre en vigueur.

Utilisation de WebAuthn la redirection dans les sessions de navigateur distantes

Une fois que la WebAuthn redirection est activée dans les paramètres du portail et que la politique du navigateur local est configurée, les utilisateurs peuvent utiliser l' WebAuthn authentification sur les sites Web dans le cadre de leurs sessions de navigateur à distance WorkSpaces Secure Browser.

Les utilisateurs peuvent s'authentifier auprès de sites Web en utilisant :

- FIDO2 clés de sécurité connectées à leur appareil local
- Clés d'accès
- Authentificateurs de plateforme tels que Windows Hello ou Touch ID

Le processus WebAuthn d'authentification est transféré de manière fluide de la session de navigateur à distance à l'appareil local de l'utilisateur, ce qui permet une authentification sécurisée sans mot de passe tout en préservant les avantages de sécurité de l'environnement de navigation à distance.

Résolution des problèmes WebAuthn de redirection

Si les utilisateurs rencontrent des problèmes de WebAuthn redirection lors de leurs sessions de navigation à distance, suivez les étapes de dépannage suivantes pour identifier et résoudre les problèmes courants.

Rubriques

WebAuthn la redirection ne fonctionne pas

Si les instructions WebAuthn d'authentification ne s'affichent pas ou ne fonctionnent pas :

1. WebAuthn La vérification est activée dans les paramètres du portail sous Autorisations utilisateur.
2. Vérifiez que la politique du navigateur local est correctement configurée en accédant `chrome://policy` ou en confirmant qu'`edge://policy`elle `WebAuthenticationRemoteDesktopAllowedOrigins` inclut l'URL du contenu de votre région.

3. Assurez-vous que la version du navigateur répond aux exigences : Chrome 136+ ou Edge 137+.
4. Testez avec un autre authentificateur (clé de sécurité ou authentificateur de plateforme).

Messages d'erreur courants

Les messages d'erreur courants et leur résolution sont les suivants :

WebAuthn messages d'erreur et résolutions

Message d’erreur	Résolution
WebAuthn La redirection Amazon DCV n'a pas réussi à terminer la demande d'enregistrement : la redirection Webauthn n'est pas prise en charge par le client	Vérifiez que vous utilisez un navigateur et une version compatibles (Chrome 136+ ou Edge 137+).
L'invite apparaît mais impossible d'interagir avec les authentificateurs locaux	Vérifiez que l'extension de WebAuthn redirecti on Amazon DCV est installée et activée dans votre navigateur distant.
WebAuthn La redirection Amazon DCV n'a pas réussi à traiter la demande d'enregistrement : l'identifiant de la partie utilisatrice n'est pas un suffixe de domaine enregistrable ni un équivalent au domaine actuel. Par la suite, une tentative de récupération de la ressource .well-known/webauthn de l'ID RP revendiqué a échoué.	Cela signifie que la politique du navigateu r WebAuthenticationRemoteDesktopAllowe dOrigins local n'est pas appliquée. Vérifiez la politique et mettez-la à jour pour autoriser le domaine de contenu. Assurez-vous que le navigateur est redémarré. Il se peut que vous deviez démarrer une nouvelle session pour que les modifications s'appliquent.
L'opération a expiré ou n'a pas été autorisée . Voir : https://www.w3. org/TR/webauthn-2/ #sctn-privacy-considerations-client.	Cette erreur peut se produire si : (1) l'extensi on de WebAuthn redirection DCV n'est pas installée ou activée, (2) l'utilisateur annule l'invite d'authentification, (3) l'utilisateur saisit un code PIN incorrect pour sa clé de sécurité, ou (4) l'utilisateur n'interagit pas avec l'invite et la demande expire.

Gestion des commandes de la barre d'outils dans Amazon WorkSpaces Secure Browser

Avec les commandes de barre d'outils, vous pouvez configurer la présentation de la barre d'outils pour les sessions des utilisateurs finaux, notamment les options suivantes :

- Fonctions
  - Presse-papiers : lorsque cette option est activée, permet copy/paste d'utiliser des commandes granulaires (copier uniquement, coller uniquement, ou les deux). Lorsque cette option est désactivée, masque l'icône et empêche son utilisation dans la barre d'outils.
  - Transfert de fichiers : lorsque cette option est activée, elle autorise les opérations sur les fichiers à l'aide de contrôles granulaires (téléchargement uniquement, téléchargement uniquement ou les deux). Lorsque cette option est désactivée, masque l'icône et empêche les transferts.
  - Microphone : lorsque cette option est activée, elle autorise l'utilisation du microphone. Lorsque cette option est désactivée, masque l'icône.
  - Webcam : lorsque cette option est activée, elle autorise l'utilisation de l'appareil photo. Lorsque cette option est désactivée, masque l'icône.
  - Double écran : lorsque cette option est activée, elle permet l'utilisation de deux moniteurs. Lorsque cette option est désactivée, masque l'icône.
  - Plein écran : lorsque cette option est activée, le mode plein écran est activé. Lorsque cette option est désactivée, masque l'icône.
  - Windows : lorsque cette option est activée, elle permet de passer d'une fenêtre à l'autre. Lorsque cette option est désactivée, masque l'icône.
- Paramètres
  - Thème de la barre d'outils : contrôle l'affichage en mode clair ou en mode sombre. La configuration supprime le contrôle du thème de l'utilisateur final.
  - État de la barre d'outils : définit l'état ancré ou détaché de la barre d'outils. La configuration supprime le contrôle de l'utilisateur final sur l'état de la barre d'outils.
  - Résolution maximale : définit la résolution d'affichage maximale autorisée. Les utilisateurs ne peuvent sélectionner que des résolutions allant jusqu'à cette limite définie.

Configuration d'un domaine personnalisé pour votre portail

Vous pouvez configurer un domaine personnalisé pour un portail WorkSpaces Secure Browser afin de permettre l'accès via votre propre nom de domaine au lieu de l'URL du portail par défaut. Cette fonctionnalité vous permet d'offrir aux utilisateurs une expérience plus intégrée en utilisant un domaine qui correspond à l'image de marque de votre entreprise.

Présentation

Le domaine personnalisé vous permet de personnaliser les aspects suivants de l'expérience utilisateur :

- Accès au portail personnalisé : les utilisateurs accèdent à votre portail via le domaine de votre organisation au lieu du point de terminaison AWS par défaut.
- Expérience utilisateur cohérente : maintenez la cohérence de votre marque en utilisant des noms de domaine familiers qui correspondent à ceux de votre entreprise.

> **Note**
>
> Pour personnaliser l'apparence visuelle et les éléments de marque de votre portail, consultezthe section called “Personnalisation de la marque”.

Rubriques

Configuration d'un domaine personnalisé pour votre portail

Comment ça marche

Lorsque vous configurez un domaine personnalisé :

- Vous créez et configurez un proxy inverse avec votre domaine personnalisé pour acheminer le trafic vers le point de terminaison du portail.
- Les utilisateurs accèdent à votre portail via votre domaine personnalisé au lieu du point de terminaison du portail par défaut.

- Les certificats SSL garantissent des connexions sécurisées tout au long du processus.

Conditions préalables

Avant de configurer des domaines personnalisés, assurez-vous de disposer des éléments suivants :

- Nom de domaine que vous gérez par le biais d'un fournisseur de services DNS tel qu'Amazon Route53.
- Un portail WorkSpaces Secure Browser. Pour plus d'informations sur la création d'un portail, consultezthe section called “Création d'un portail Web”.
- Assurez-vous de disposer des autorisations nécessaires pour gérer AWS Certificate Manager et CloudFront les configurations DNS.

> **Important**
>
> Les utilisateurs doivent activer les cookies tiers pour le domaine personnalisé dans leur navigateur afin de garantir le bon fonctionnement du portail.
> Assurez-vous de posséder et de gérer correctement le domaine personnalisé et ses enregistrements DNS afin de garantir la sécurité et les fonctionnalités de votre portail.

> **Note**
>
> Pour activer l'extension d'authentification unique pour les domaines personnalisés, les utilisateurs doivent installer l'extension dans leur navigateur avec une version ultérieure à 1.0.2505.6608.
> Les utilisateurs sont invités à installer l'extension lorsqu'ils se connectent à un portail. Pour en savoir plus sur l’expérience utilisateur avec l’extension, consultez the section called “Extension d’authentification unique”.

Prise en main

Vous pouvez configurer votre domaine personnalisé en tant qu'attribut de paramètres de portail lors de la création d'un nouveau portail ou lors de la modification d'un portail existant. Cela peut être effectué à l'aide des commandes de la AWS console, du SDK CloudFormation ou de la AWS CLI.

Nous vous recommandons de configurer une CloudFront distribution Amazon en tant que proxy inverse qui achemine le trafic de votre domaine personnalisé vers le point de terminaison du portail WorkSpaces Secure Browser.

> **Note**
>
> Bien qu'Amazon CloudFront soit recommandé comme solution de proxy inverse, vous pouvez utiliser d'autres configurations de proxy inverse. Assurez-vous de respecter les paramètres d'origine et de configuration du cache requis, comme indiqué dans les étapes de CloudFront configuration d'Amazon.

Configuration en CloudFront tant que proxy inverse

Pour terminer la configuration d'un proxy inverse, vous devez :

- Un certificat SSL via AWS Certificate Manager (ACM)
- Une CloudFront distribution Amazon
- Enregistrements DNS
- Portail configuré avec votre domaine personnalisé

SSL Certificate (Certificat SSL)

Si vous n'en avez pas déjà un, procédez comme suit pour en faire la demande par le biais d'ACM :

1. Accédez à la console ACM à https://console.aws.amazon.com/acm l'adresse.

   > **Important**
   >
   > Utilisez la région de l'est des États-Unis (Virginie du Nord), CloudFront car les certificats doivent y être stockés.

2. Demandez un certificat :

   - Pour les nouveaux utilisateurs d'ACM : choisissez Get started sous Provisionner des certificats
   - Pour les utilisateurs ACM existants : choisissez Demander un certificat

3. Choisissez Demander un certificat public, puis choisissez Demander un certificat.

> **Note**
>
> Vous pouvez également importer un certificat existant. Pour plus d'informations, consultez la section Importation de certificats dans ACM dans le guide de l'utilisateur d'ACM.

4. Entrez votre nom de domaine principal (par exemple,**`myportal.example.com`**).
5. Choisissez une méthode de validation :
   - Validation DNS (recommandée pour les utilisateurs de Route 53) : permet la création automatique d'ensembles d'enregistrements dans votre zone hébergée. Pour plus d'informations, consultez la section Validation DNS dans le guide de l'utilisateur d'ACM.
   - Validation des e-mails — Pour plus d'informations, consultez la section Validation des e-mails dans le guide de l'utilisateur d'ACM.
6. Vérifiez vos paramètres, puis sélectionnez Confirmer et demander.

CloudFront distribution

Créez une CloudFront distribution pour les demandes de proxy depuis votre domaine personnalisé vers le point de terminaison du portail.

1. Accédez à la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront.
2. Choisissez Create Distribution.
   - Nom de la distribution : entrez le nom de la distribution
   - Type de distribution : site Web ou application unique

> **Note**
>
> Si votre domaine personnalisé est géré dans Route 53 dans le même compte AWS, nous CloudFront pouvons gérer automatiquement votre DNS pour vous. Entrez votre domaine personnalisé et cliquez sur « Vérifier le domaine ». Si vous avez un domaine d'un autre fournisseur DNS, ignorez cette étape et configurez votre domaine ultérieurement.

3. Configurez les paramètres d'origine :

- Type d'origine : Autre
- Origine personnalisée : entrez le point de terminaison du portail *<portalId>* .workspaces-web.com
- Chemin d'origine : laisser le champ vide (par défaut)

4. Personnalisez les paramètres d'origine :

   - Ajout d'en-tête personnalisé

     > **Important**
     >
     > L'accès au portail via un domaine personnalisé ne fonctionnera que si cet en-tête est présent dans les demandes par proxy. Assurez-vous que le nom et la valeur de l'en-tête sont spécifiés exactement comme indiqué.

     - Nom de l'en-tête : workspacessecurebrowser-custom-domain
     - Valeur : votre domaine personnalisé (par exemple,**myportal.example.com**)
   - Protocole : HTTPS uniquement
   - Port HTTPS : 443 (conserver la valeur par défaut)
   - Protocole SSL d'origine minimal : TLSv1 .2 (par défaut)
   - Type d'adresse IP d'origine : IPv4 uniquement (Amazon WorkSpaces Secure Browser n'est pas compatible IPv6 au moment de la rédaction de ce guide d'administration.)

5. Personnalisez les paramètres du cache :

   - Politique de protocole de visualisation : rediriger le HTTP vers HTTPS
   - Méthodes HTTP autorisées : GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE
   - Politique de cache : CachingDisabled
   - Politique de demande d'origine : AllViewerExceptHostHeader

     > **Important**
     >
     > L'accès au portail via un domaine personnalisé ne fonctionnera que si la politique de demande d'origine est définie sur AllViewerExceptHostHeader. Comme son nom

l'indique, cette politique filtre uniquement l'en-tête de l'hôte des en-têtes de demande et transmet tous les en-têtes restants à l'origine.

6. Vous pouvez configurer le WAF si vous le souhaitez, mais cela n'est pas nécessaire aux fins de cette configuration.
7. Dans Obtenir un certificat TLS, sélectionnez le certificat TLS créé à l'étape 1.
8. Vérifiez les paramètres et choisissez Créer une distribution.

Enregistrements DNS

Cloudfront peut mettre à jour vos enregistrements DNS dans Route 53 pour acheminer le trafic des domaines spécifiés vers la distribution créée à l'étape 2, si votre zone hébergée se trouve dans le même compte AWS.

1. Accédez aux CloudFront paramètres
2. Cliquez sur « Router les domaines vers CloudFront »
3. Cliquez sur « Configurer le routage automatiquement »

Si vous avez configuré le DNS pour le domaine personnalisé chez un autre fournisseur de services ou un autre compte AWS, configurez votre fournisseur DNS pour acheminer le trafic de votre domaine vers la distribution. Les étapes suivantes décrivent comment procéder à l'aide de la Route 53.

1. Ouvrez la console Amazon Route 53 à l'adressehttps://console.aws.amazon.com/route53.
2. Gestion des accès DNS :
   - Si vous utilisez Route 53 pour la première fois avec ce AWS compte, la page de présentation d'Amazon Route 53 s'ouvre. Sous Gestion du DNS, choisissez Commencer maintenant.
   - Si vous avez déjà utilisé Route 53 avec ce AWS compte, passez à l'étape suivante.
3. Dans le panneau de navigation, choisissez Zones hébergées.
4. Créez une zone hébergée si vous n'en avez pas déjà une :
   - Pour acheminer le trafic Internet vers vos ressources, consultez la section Création d'une zone hébergée publique dans le guide du développeur Amazon Route 53.
   - Pour acheminer le trafic dans votre VPC, consultez la section Création d'une zone hébergée privée dans le guide du développeur Amazon Route 53.

5. Sur la page Zones hébergées, choisissez le nom de la zone hébergée que vous souhaitez administrer.
6. Choisissez Create Record Set (Créer un ensemble d'enregistrements).
7. Créez une entrée pour votre domaine (par exemple,**`myportal.example.com`**) :

   - Type : A — IPv4 adresse
   - Alias : Oui
   - Alias cible : URL CloudFront de distribution

   Conservez les valeurs par défaut pour tous les autres paramètres.

> **Note**
>
> Si vous n'utilisez pas Route 53 pour gérer le DNS de votre domaine, utilisez votre fournisseur de services DNS et ajoutez les entrées DNS qui pointent vers votre domaine à l'URL de votre CloudFront distribution.

Vous pouvez également utiliser le CloudFormation modèle suivant pour créer votre CloudFront distribution :

Ce CloudFormation modèle crée automatiquement la CloudFront distribution, configure les paramètres du proxy inverse et crée éventuellement des enregistrements DNS Route53 :

Example workspaces-web-custom-domain-modèle.yaml

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'CloudFront Distribution for custom domain configuration with existing AWS
 WorkSpaces Secure Browser Portal'

Parameters:
  PortalEndpoint:
    Type: String
    Description: 'The endpoint of your existing WorkSpaces Web Portal (e.g.,
 abc123.workspaces-web.com)'
    AllowedPattern: '^[a-zA-Z0-9-]+(\.[a-zA-Z0-9-]+)?\.workspaces-web\.com$'
    ConstraintDescription: 'Must be a valid WorkSpaces Web portal endpoint'
```

```
  CustomDomainName:
    Type: String
    Description: 'Custom domain name for the portal (e.g., myportal.example.com)'
    AllowedPattern: '^([a-zA-Z0-9]?((?!-)([A-Za-z0-9-]*[A-Za-z0-9])\.)+[a-zA-Z0-9]+)$'
    ConstraintDescription: 'Must be a valid domain name'

  CertificateArn:
    Type: String
    Description: 'ARN of the validated SSL certificate in ACM (must be in us-east-1
 region for CloudFront)'
    AllowedPattern: 'arn:aws:acm:us-east-1:[0-9]{12}:certificate/[a-f0-9]{8}-[a-f0-9]
{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}'
    ConstraintDescription: 'Must be a valid ACM certificate ARN in us-east-1 region'

  CreateRoute53Record:
    Type: String
    Description: 'Create Route53 record for custom domain (requires existing hosted
 zone)'
    Default: 'No'
    AllowedValues:
      - 'Yes'
      - 'No'

  HostedZoneId:
    Type: String
    Description: 'Route53 Hosted Zone ID for the custom domain (required if creating
 Route53 record)'
    Default: ''

Conditions:
  ShouldCreateRoute53Record: !And
    - !Equals [!Ref CreateRoute53Record, 'Yes']
    - !Not [!Equals [!Ref HostedZoneId, '']]

Resources:
  # CloudFront Distribution
  CloudFrontDistribution:
    Type: AWS::CloudFront::Distribution
    Properties:
      DistributionConfig:
        Aliases:
          - !Ref CustomDomainName
        Comment: !Sub 'CloudFront distribution for WorkSpaces Web Portal -
 ${CustomDomainName}'
```

```
        Enabled: true
        HttpVersion: http2
        IPV6Enabled: false  # WorkSpaces Secure Browser does not support IPv6
        PriceClass: PriceClass_All

        # Origin Configuration
        Origins:
          - Id: WorkSpacesWebOrigin
            DomainName: !Ref PortalEndpoint
            CustomOriginConfig:
              HTTPSPort: 443
              OriginProtocolPolicy: https-only
              OriginSSLProtocols:
                - TLSv1.2
            OriginCustomHeaders:
              - HeaderName: workspacessecurebrowser-custom-domain
                HeaderValue: !Ref CustomDomainName

        # Default Cache Behavior
        DefaultCacheBehavior:
          TargetOriginId: WorkSpacesWebOrigin
          ViewerProtocolPolicy: https-only
          AllowedMethods:
            - GET
            - HEAD
            - OPTIONS
            - PUT
            - POST
            - PATCH
            - DELETE
          Compress: false
          # Cache Policy: CachingDisabled (using predefined managed policy)
          CachePolicyId: 4135ea2d-6df8-44a3-9df3-4b5a84be39ad
          # Origin Request Policy: AllViewerExceptHostHeader (using predefined managed
policy)
          OriginRequestPolicyId: b689b0a8-53d0-40ab-baf2-68738e2966ac

        # SSL Configuration
        ViewerCertificate:
          AcmCertificateArn: !Ref CertificateArn
          SslSupportMethod: sni-only
          MinimumProtocolVersion: TLSv1.2_2021

      Tags:
```

```
        - Key: Name
          Value: !Sub '${AWS::StackName}-cloudfront'

  # Route 53 Record (optional - requires hosted zone to exist)
  Route53Record:
    Type: AWS::Route53::RecordSet
    Condition: ShouldCreateRoute53Record
    Properties:
      HostedZoneId: !Ref HostedZoneId
      Name: !Ref CustomDomainName
      Type: A
      AliasTarget:
        DNSName: !GetAtt CloudFrontDistribution.DomainName
        HostedZoneId: Z2FDTNDATAQYW2  # CloudFront Hosted Zone ID
        EvaluateTargetHealth: false

Outputs:
  PortalEndpoint:
    Description: 'WorkSpaces Web Portal endpoint used as origin'
    Value: !Ref PortalEndpoint
    Export:
      Name: !Sub '${AWS::StackName}-PortalEndpoint'

  CustomDomainEndpoint:
    Description: 'Custom domain endpoint for the portal'
    Value: !Sub 'https://${CustomDomainName}'
    Export:
      Name: !Sub '${AWS::StackName}-CustomDomainEndpoint'

  CloudFrontDistributionId:
    Description: 'CloudFront Distribution ID'
    Value: !Ref CloudFrontDistribution
    Export:
      Name: !Sub '${AWS::StackName}-CloudFrontDistributionId'

  CloudFrontDomainName:
    Description: 'CloudFront Distribution Domain Name'
    Value: !GetAtt CloudFrontDistribution.DomainName
    Export:
      Name: !Sub '${AWS::StackName}-CloudFrontDomainName'

  CertificateArn:
    Description: 'SSL Certificate ARN used by CloudFront'
    Value: !Ref CertificateArn
```

```
    Export:
      Name: !Sub '${AWS::StackName}-CertificateArn'

Metadata:
  AWS::CloudFormation::Interface:
    ParameterGroups:
      - Label:
          default: "Existing Portal Configuration"
        Parameters:
          - PortalEndpoint
      - Label:
          default: "Custom Domain Configuration"
        Parameters:
          - CustomDomainName
          - CertificateArn
          - CreateRoute53Record
          - HostedZoneId
    ParameterLabels:
      PortalEndpoint:
        default: "Portal Endpoint"
      CustomDomainName:
        default: "Custom Domain Name"
      CertificateArn:
        default: "SSL Certificate ARN"
      CreateRoute53Record:
        default: "Create Route53 Record"
      HostedZoneId:
        default: "Hosted Zone ID"
```

Pour utiliser ce modèle :

1. Enregistrez le modèle ci-dessus sous `workspaces-web-custom-domain-template.yaml`
2. Déployez à l'aide de la AWS console, de la AWS CLI ou du AWS SDK avec vos valeurs de paramètres spécifiques
3. Après le déploiement, configurez votre portail avec le domaine personnalisé, comme décrit à l'étape 4 ci-dessous

Configuration du portail

Enregistrez votre domaine personnalisé en tant qu'attribut de paramètres de portail à l'aide de la AWS console, de UpdatePortal l'API ou de la commande update-portal AWS CLI.

1. Ouvrez la console WorkSpaces Secure Browser à l'adressehttps://console.aws.amazon.com/workspaces-web/home.
2. Dans le panneau de navigation, sélectionnez Portails web.
3. Sélectionnez le portail Web que vous souhaitez configurer et choisissez Modifier.
4. Dans les paramètres du portail, ajoutez votre domaine personnalisé.
5. Enregistrez la configuration du portail.

Testez votre configuration

Pour tester votre configuration, procédez comme suit :

1. Ouvrez un navigateur Web et accédez à l'URL de votre domaine personnalisé (par exemple,**`https://myportal.example.com`**).
2. Si tout est correctement configuré, vous devriez voir la page de connexion de votre portail.
3. Ensuite, entrez l'URL du portail dans votre navigateur, vous devriez être redirigé vers le domaine personnalisé après vous être connecté à votre IdP.
4. Enfin, connectez-vous à votre IdP et cliquez sur la vignette de l'application correspondant à votre portail. Vous devriez être redirigé vers un domaine personnalisé.

Résolution des problèmes liés aux domaines personnalisés

Si les utilisateurs rencontrent des problèmes d'accès au portail via un domaine personnalisé lors de leurs sessions de navigation à distance, suivez les étapes de dépannage suivantes pour identifier et résoudre les problèmes courants.

Rubriques

- Messages d'erreur courants

Messages d'erreur courants

Les messages d'erreur courants et leur résolution lors de la configuration de domaines personnalisés sont les suivants :

Erreur de jeton CSRF non valide

Cette erreur se produit lorsque Secure Browser ne reçoit pas correctement votre demande lors de la CloudFront configuration.

Pour résoudre ce problème :

- Vérifiez les paramètres d'origine personnalisés de votre CloudFront distribution.
- Vérifiez que le nom de l'en-tête personnalisé correspond exactement `workspacessecurebrowser-custom-domain` et que la valeur correspond exactement à votre domaine personnalisé (sans https ://ni aucun paramètre de requête).
- Videz le cache de votre navigateur local.
- Invalidez le cache sur. CloudFront

502 Erreur Bad Gateway

Cette erreur indique généralement des problèmes de configuration du cache.

Pour résoudre ce problème :

- Vérifiez les paramètres de cache de votre CloudFront distribution.
- Vérifiez que la politique de cache est définie sur`CachingDisabled`.
- Vérifiez que la politique de demande Origin est définie sur`AllViewerExceptHostHeader`.
- Videz le cache de votre navigateur local.
- Invalidez le cache sur. CloudFront

Erreur d'accès refusé

Cette erreur peut se produire si votre domaine personnalisé n'est pas configuré correctement.

Pour résoudre ce problème :

- Vérifiez les paramètres d'origine de votre CloudFront distribution.
- Vérifiez que l'origine est définie sur l'URL du portail correcte.
- Vérifiez que le portail est configuré avec le domaine personnalisé approprié.
- Videz le cache de votre navigateur local.
- Invalidez le cache sur. CloudFront

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

- Bonnes pratiques de sécurité pour Amazon WorkSpaces Secure Browser

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 Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée d'AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

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

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 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 Nom. Cela inclut lorsque vous travaillez avec WorkSpaces Secure Browser ou autre Services AWS à l'aide de la console, de l'API ou AWS SDKs. AWS CLI Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Rubriques

Chiffrement des données dans Amazon WorkSpaces Secure Browser

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 de politique du navigateur, les préférences des utilisateurs (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 des modèles IAM pour créer un rôle en accès complet ou un rôle 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 pour Amazon WorkSpaces Secure Browser

Le chiffrement au repos est configuré par défaut et toutes les données client (par exemple, les déclarations de politique du navigateur, les noms d'utilisateur, les journaux ou les adresses IP) utilisées dans WorkSpaces Secure Browser sont cryptées à l'aide AWS KMS de. Par défaut, WorkSpaces Secure Browser active le chiffrement à l'aide d'une clé AWS appartenant à l'utilisateur. Vous pouvez également utiliser une clé gérée par le client (CMK) en spécifiant votre clé CMK lors de la création de la ressource. Ceci n'est actuellement pris en charge que via la CLI.

Si vous choisissez de transmettre une clé CMK, la clé fournie doit être une AWS KMS clé de chiffrement symétrique et vous, en tant qu'administrateur, devez disposer des autorisations suivantes :

```
kms:DescribeKey

kms:GenerateDataKey

kms:GenerateDataKeyWithoutPlaintext

kms:Decrypt

kms:ReEncryptTo
kms:ReEncryptFrom
```

Si vous utilisez une clé CMK, vous devez autoriser le principal de service externe de WorkSpaces Secure Browser à accéder à la clé.
Pour plus d'informations, consultez Exemple de politique clé CMK étendue avec aws : SourceAccount

Dans la mesure du possible, WorkSpaces Secure Browser utilisera les informations d'identification FAS (Forward Access Sessions) pour accéder à votre clé. Pour plus d'informations sur le FAS, voir Sessions d'accès transmises.
Dans certains cas, WorkSpaces Secure Browser peut avoir besoin d'accéder à votre clé de manière asynchrone. En autorisant le principal service externe de WorkSpaces Secure Browser dans votre politique de clés, WorkSpaces Secure Browser sera en mesure d'effectuer l'ensemble des opérations cryptographiques autorisées avec votre clé.

Après la création d'une ressource, la clé ne peut plus être supprimée ou modifiée. Si vous avez utilisé une clé CMK, en tant qu'administrateur accédant à la ressource, vous devez disposer des autorisations suivantes :

```
kms:GenerateDataKey
kms:GenerateDataKeyWithoutPlaintext
kms:Decrypt

kms:ReEncryptTo
kms:ReEncryptFrom
```

Si le message d'erreur Accès refusé s'affiche lorsque vous utilisez la console, il est probable que l'utilisateur qui accède à la console ne dispose pas des autorisations requises pour utiliser la clé CMK sur la clé utilisée.

Exemples de politiques clés et de cadrage pour WorkSpaces Secure Browser

CMKs nécessitent la politique clé suivante :

```
{
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
```

```
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      }
    ]
}
```

Les autorisations suivantes sont requises par WorkSpaces Secure Browser :

- `kms:DescribeKey`— Vérifie que la AWS KMS clé fournie est correctement configurée.
- `kms:GenerateDataKeyWithoutPlaintext`et `kms:GenerateDataKey` — Demande la AWS KMS clé pour créer les clés de données utilisées pour chiffrer des objets.
- `kms:Decrypt`— Demande la AWS KMS clé pour déchiffrer les clés de données chiffrées. Ces clés de données sont utilisées pour chiffrer vos données.
- `kms:ReEncryptTo`et `kms:ReEncryptFrom` — Demande la AWS KMS clé pour permettre le rechiffrement depuis ou vers une clé KMS.

Définition des autorisations de WorkSpaces Secure Browser sur votre clé AWS KMS

Lorsque le principal d'une déclaration de politique clé est un principal de AWS service, nous vous recommandons vivement d'utiliser les clés de condition SourceAccount globales aws : SourceArn ou aws :, en plus du contexte de chiffrement.

Le contexte de chiffrement utilisé pour une ressource contiendra toujours une entrée au format `aws:workspaces-web:RESOURCE_TYPE:id` et l'ID de ressource correspondant.

L'ARN source et les valeurs du compte source sont incluses dans le contexte d'autorisation uniquement lorsqu'une demande AWS KMS provient d'un autre AWS service. Cette combinaison de conditions implémente des autorisations de moindre privilège et évite l'éventualité pour un programme d'être manipulé par un autre pour obtenir un accès. Pour plus d'informations, consultez la section Autorisations pour les services AWS dans les politiques clés.

```
   "Condition": {
```

```
        "StringEquals": {
          "aws:SourceAccount": "AccountId",
          "kms:EncryptionContext:aws:workspaces-web:resourceType:id": "resourceId"
        },
        "ArnEquals": {
          "aws:SourceArn": [
            "arn:aws:workspaces-web:Region:AccountId:resourceType/resourceId"
          ]
        },
      }
```

> **Note**
>
> Avant la création de ressources, la politique clé ne doit utiliser que la `aws:SourceAccount` condition, car l'ARN complet de la ressource n'existera pas encore. Après la création de la ressource, la politique clé peut être mise à jour pour inclure les `kms:EncryptionContext` conditions `aws:SourceArn` et.

Exemple de politique clé CMK étendue avec **`aws:SourceAccount`**

```
{
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
```

```
            "aws:SourceAccount": "<AccountId>"
        }
      }
    }
  ]
}
```

Exemple de politique clé CMK étendue avec un caractère générique de **`aws:SourceArn`** ressource

```
{
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:workspaces-web:<Region>:<AccountId>:*/*"
        }
      }
    }
  ]
}
```

Exemple de politique clé CMK étendue avec **`aws:SourceArn`**

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

```
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:workspaces-web:<Region>:<AccountId>:portal/*",
            "arn:aws:workspaces-web:<Region>:<AccountId>:browserSettings/*",
            "arn:aws:workspaces-web:<Region>:<AccountId>:userSettings/*",
            "arn:aws:workspaces-web:<Region>:<AccountId>:ipAccessSettings/*"
          ]
        }
    }
  ]
}
```

> **Note**
>
> Après avoir créé la ressource, vous pouvez mettre à jour le caractère générique `SourceArn` correspondant. Si vous utilisez WorkSpaces Secure Browser pour créer une nouvelle ressource nécessitant un accès CMK, veillez à mettre à jour sa politique clé en conséquence.

Exemple de politique clé CMK étendue avec et spécifique aux ressources **`aws:SourceArn`** **`EncryptionContext`**

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

```
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt portal",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "<AccountId>",
            "kms:EncryptionContext:aws:workspaces-web:portal:id": "<portalId>>"
        }
      }
    },
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt userSettings",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
         "StringEquals": {
            "aws:SourceAccount": "<AccountId>",
            "kms:EncryptionContext:aws:workspaces-web:userSetttings:id":
"<userSetttingsId>"
        }
      }
```

```
    },
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt browserSettings",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
         "StringEquals": {
            "aws:SourceAccount": "<AccountId>",
            "kms:EncryptionContext:aws:workspaces-web:browserSettings:id":
"<browserSettingsId>"
         }
      }
    },
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt ipAccessSettings",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
         "StringEquals": {
            "aws:SourceAccount": "<AccountId>",
            "kms:EncryptionContext:aws:workspaces-web:ipAccessSettings:id":
"<ipAccessSettingsId>"
```

```
        }
      }
    },
  ]
}
```

> **Note**
>
> Assurez-vous de créer des déclarations distinctes lorsque vous incluez une ressource spécifique `EncryptionContext` à la même politique clé. Pour plus d'informations, consultez la section Utilisation de plusieurs paires de contextes de chiffrement sous kms:EncryptionContext: clé de contexte.

Chiffrement en transit pour Amazon WorkSpaces Secure Browser

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

Le chiffrement en transit est configuré par défaut, tout comme les connexions sécurisées (HTTPS, TLS).

Gestion des clés pour Amazon WorkSpaces Secure Browser

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 définir votre clé à l'aide du kit SDK AWS .

Confidentialité du trafic interréseau dans Amazon WorkSpaces Secure Browser

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. La connexion aux applications sur site est configurée dans votre propre VPC et n'est pas contrôlée WorkSpaces par 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 Amazon Secure Browser WorkSpaces.

Accès utilisateur et connexion dans Amazon WorkSpaces Secure Browser

Les administrateurs peuvent enregistrer les événements de session WorkSpaces Secure Browser, notamment le démarrage, l'arrêt et les visites d'URL. 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. Les visites d'URL 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

Gestion des identités et des accès AWS (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources du WorkSpaces Secure Browser. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

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

- Utilisateur du service : demandez des autorisations à votre administrateur si vous ne pouvez pas accéder aux fonctionnalités (voir Résolution des problèmes d'identité et d'accès à Amazon WorkSpaces Secure Browser)
- Administrateur du service : déterminez l'accès des utilisateurs et soumettez les demandes d'autorisation (voir Comment Amazon WorkSpaces Secure Browser fonctionne avec IAM)
- Administrateur IAM : rédigez des politiques pour gérer l'accès (voir 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 en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

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

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

Compte AWS utilisateur root

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

Identité fédérée

Il est recommandé d'obliger les utilisateurs humains à utiliser la fédération avec un fournisseur d'identité pour accéder à Services AWS l'aide d'informations d'identification temporaires.

Une identité fédérée est un utilisateur provenant de l'annuaire de votre entreprise, de votre fournisseur d'identité Web ou Directory Service qui y accède à Services AWS l'aide d'informations d'identification provenant d'une source d'identité. Les identités fédérées 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. Pour plus d'informations, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité qui dispose d'autorisations spécifiques pour une seule personne ou application. Nous vous recommandons d'utiliser ces informations d'identification temporaires au lieu des utilisateurs IAM avec des informations d'identification à long terme. Pour plus d'informations, voir Exiger des utilisateurs humains qu'ils utilisent la fédération avec un fournisseur d'identité pour accéder à AWS l'aide d'informations d'identification temporaires dans le guide de l'utilisateur IAM.

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

Rôles IAM

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

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

Gestion de l'accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique définit les autorisations lorsqu'elles sont associées à une identité ou à une ressource. AWS évalue ces politiques lorsqu'un directeur fait une demande. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations les documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

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

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

Politiques basées sur l'identité

Les stratégies basées sur l'identité sont des documents de stratégie d'autorisations JSON que vous attachez à une identité (utilisateur, groupe ou rôle). Ces politiques contrôlent les actions que peuvent exécuter ces identités, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

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

Politiques basées sur les ressources

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

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

Autres types de politique

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

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

Plusieurs types de politique

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

Comment Amazon WorkSpaces Secure Browser fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à WorkSpaces Secure Browser, découvrez quelles fonctionnalités IAM peuvent être utilisées avec WorkSpaces Secure Browser.

Fonctionnalités IAM que vous pouvez utiliser avec Amazon WorkSpaces Secure Browser

Fonctionnalité IAM	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 de politique	Oui
ACLs	Non
ABAC (identifications dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Rôles du service	Non
Rôles liés à un service	Oui

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

Rubriques

- Politiques basées sur l'identité pour Secure Browser WorkSpaces
- Politiques basées sur les ressources dans Secure Browser WorkSpaces
- Actions politiques pour WorkSpaces Secure Browser
- Ressources relatives aux politiques pour WorkSpaces Secure Browser
- Clés de conditions de politique pour WorkSpaces Secure Browser
- Listes de contrôle d'accès (ACLs) dans WorkSpaces Secure Browser
- Contrôle d'accès basé sur les attributs (ABAC) avec Secure Browser WorkSpaces

- Utilisation d'informations d'identification temporaires avec WorkSpaces Secure Browser
- Autorisations principales interservices pour WorkSpaces Secure Browser
- Rôles de service pour WorkSpaces Secure Browser
- Rôles liés à un service pour Secure Browser WorkSpaces

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 des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

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

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 de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des 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. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Actions politiques pour WorkSpaces Secure Browser

Prend en charge les actions de politique : oui

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

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Intégration d'actions dans une politique 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 les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, 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 caractéristiques ARNs, consultez la section Ressources définies par Amazon WorkSpaces Secure Browser dans le Service Authorization Reference. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, 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

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

L'élément `Condition` indique à quel moment les instructions s'exécutent en fonction de critères définis. 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. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

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. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

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

Prend en charge ABAC (identifications dans les politiques) : partiellement

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs nommés balise. Vous pouvez associer des balises aux entités et aux AWS ressources IAM, puis concevoir des politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de la ressource.

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

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

Pour plus d'informations sur ABAC, consultez Définition d'autorisations avec l'autorisation ABAC dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

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

Prend en charge les informations d'identification temporaires : oui

Les informations d'identification temporaires fournissent un accès à court terme aux AWS ressources et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. AWS recommande de générer dynamiquement des informations d'identification temporaires au

lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM et Services AWS compatibles avec IAM dans le Guide de l'utilisateur IAM.

Autorisations principales interservices pour WorkSpaces Secure Browser

Prend en charge les sessions d'accès direct (FAS) : oui

Les sessions d'accès direct (FAS) utilisent les autorisations du principal appelant et Service AWS, combinées Service AWS à la demande d'envoi de demandes aux services en aval. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez la section Sessions de transmission d'accès.

Rôles de service pour WorkSpaces Secure Browser

Prend en charge les rôles de service : Non

Un rôle de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

> **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 à un service : oui

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

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM. Recherchez un service dans le tableau qui inclut un `Yes` dans la

colonne Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

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. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques IAM (console) dans le Guide de l'utilisateur IAM.

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 basées sur l'identité pour Amazon Secure Browser WorkSpaces
- Utilisation de la console Amazon WorkSpaces Secure Browser
- Permettre aux utilisateurs de consulter leurs propres autorisations pour Amazon WorkSpaces Secure Browser

Bonnes pratiques en matière de politiques basées sur l'identité pour Amazon Secure Browser WorkSpaces

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 politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.

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

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

Utilisation de la console Amazon 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 politique 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 politique.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API 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 Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

Permettre aux utilisateurs de consulter leurs propres autorisations pour Amazon WorkSpaces Secure Browser

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

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

Rubriques

- AWS politique gérée : AmazonWorkSpacesWebServiceRolePolicy
- AWS politique gérée : AmazonWorkSpacesSecureBrowserReadOnly
- AWS politique gérée : AmazonWorkSpacesWebReadOnly
- WorkSpaces Mises à jour des politiques AWS gérées par Secure Browser

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 de plus amples informations, veuillez consulter 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 VPCs les sous-réseaux et les zones de disponibilité ; de créer, étiqueter, décrire et supprimer des interfaces réseau ; d'associer ou de dissocier une adresse ; et de décrire les tables de routage, les groupes de sécurité et les points de terminaison 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 de plus amples informations, veuillez consulter the section called "Configuration de l'enregistrement des activités des utilisateurs".

```
{
    "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 VPCs les sous-réseaux et les groupes de sécurité. Ceci est utilisé dans la console de AWS gestion de WorkSpaces Secure Browser pour afficher vos VPCs 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 VPCs les sous-réseaux et les groupes de sécurité. Ceci est utilisé dans la console de AWS gestion de WorkSpaces Secure Browser pour afficher vos VPCs 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.

Modifier	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 and act on subnet and security group resources, as well as restrict DeleteNetworkInterface to ENIs tagged with 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 de plus amples informations, veuillez consulter the section called "Configuration de l'enregis	2 novembre 2022

Modifier	Description	Date
	trement des activités des utilisateurs".	
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 de plus amples informations, veuillez consulter the section called "Configuration de l'enregistrement des activités des utilisateurs".	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 AWS/Usage noms aux autorisations de l' PutMetricData API.	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

Modifier	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 et d'IAM.

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 quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `workspaces-web:`*`GetWidget`* 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 Services AWS 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, vous devez disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM 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 n'est pas autorisée à transmettre 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 plus d'informations, consultez les éléments suivants :

- Pour savoir si WorkSpaces Secure Browser prend en charge ces fonctionnalités, consultezComment Amazon WorkSpaces Secure Browser fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- 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 l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de rôles liés à un service pour Amazon Secure Browser WorkSpaces

Amazon WorkSpaces Secure Browser utilise des rôles Gestion des identités et des accès AWS 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 vous n'avez pas à 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 à un service, consultez Services AWS qui fonctionnent avec IAM et recherchez les services avec un Oui dans la colonne Rôle lié à un service. Choisissez un Oui ayant un lien permettant de consulter les détails du rôle pour ce service.

Rubriques

- Autorisations de rôle liées au service pour Secure Browser WorkSpaces
- Création d'un rôle lié à un service pour Secure Browser WorkSpaces
- Modification d'un rôle lié à un service pour Secure Browser WorkSpaces
- Supprimer un rôle lié à un service pour Secure Browser WorkSpaces
- Régions prises en charge pour les WorkSpaces rôles liés au service Secure Browser

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 de plus amples informations, veuillez consulter 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 en savoir plus, consultez Service-Linked Role Permissions (autorisations du rôle lié à un service) dans le 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 en savoir plus, 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 AWSService RoleForAmazonWorkSpacesWeb

- 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 au service à l'aide d'IAM

Utilisez la console IAM AWS CLI, le ou l' AWS API pour supprimer le rôle lié au AWSService RoleForAmazonWorkSpacesWeb service. Pour en savoir plus, 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 de plus amples informations, veuillez consulter Surveillance d'Amazon WorkSpaces Secure Browser avec Amazon CloudWatch.

Validation de conformité pour Amazon WorkSpaces Secure Browser

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

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

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. Pour plus d'informations sur votre responsabilité en matière de conformité lors de l'utilisation Services AWS, consultez AWS la documentation de sécurité.

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 dans plusieurs régions AZs ou régions
- Sauvegardes chiffrées
- Chiffrement du contenu en transit entre ou régions AZs
- 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 des appels d'API AWS publiés pour accéder à Amazon WorkSpaces Secure Browser via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

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).

Vous pouvez contrôler l'ensemble de l'accès Internet en configurant les paramètres réseau, tels que le VPC, le sous-réseau ou le groupe de sécurité. Les points de terminaison multitenant et VPC (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.

Accès APIs via un point de terminaison VPC d'interface ()AWS PrivateLink

Vous pouvez appeler directement le point de terminaison de l'API Amazon WorkSpaces Secure Browser depuis un cloud privé (VPC), au lieu de vous connecter via Internet. Vous pouvez le faire sans utiliser de passerelle Internet, de périphérique NAT, de connexion VPN ou de Direct Connect connexion.

Vous établissez cette connexion privée en créant un point de terminaison VPC d'interface alimenté par. AWS PrivateLink Pour chaque sous-réseau que vous spécifiez depuis votre VPC, nous créons une interface réseau de point de terminaison dans le sous-réseau. Une interface réseau de point de terminaison est une interface réseau gérée par le demandeur qui sert de point d'entrée pour le trafic de l'API Amazon WorkSpaces Secure Browser.

Pour plus d'informations, consultez la section Accès aux AWS services via AWS PrivateLink.

Rubriques

Considérations relatives à Amazon WorkSpaces Secure Browser

Avant de configurer un point de terminaison VPC d'interface pour Amazon WorkSpaces Secure Browser APIs, assurez-vous de consulter les « Conditions préalables » dans les services d'accès AWS via. AWS PrivateLink Amazon WorkSpaces Secure Browser permet d'appeler toutes ses actions d'API via le point de terminaison VPC de l'interface.

Par défaut, l'accès complet à Amazon WorkSpaces Secure Browser est autorisé via le point de terminaison. Pour plus d'informations, consultez Contrôle de l'accès aux services avec points de terminaison d'un VPC dans le Guide de l'utilisateur Amazon VPC.

Création d'un point de terminaison VPC d'interface pour Amazon Secure Browser WorkSpaces

Vous pouvez créer un point de terminaison VPC d'interface pour le service Amazon WorkSpaces Secure Browser à l'aide de la console Amazon VPC ou du (). AWS Command Line Interface AWS CLI Pour plus d'informations, consultez Création d'un point de terminaison d'interface dans le Guide de l'utilisateur Amazon VPC.

Créez un point de terminaison VPC d'interface pour Amazon WorkSpaces Secure Browser en utilisant le nom de service suivant :

- com.amazonaws. *region*.espaces de travail-web

Pour les régions prises en charge par FIPS, créez un point de terminaison VPC d'interface pour WorkSpaces Amazon Secure Browser en utilisant le nom de service suivant :

- com.amazonaws. *region*. workspaces-web-fips

Création d'une politique de point de terminaison pour le point de terminaison VPC de votre interface

Une politique de point de terminaison est une ressource IAM que vous pouvez associer à un point de terminaison VPC d'interface. La politique de point de terminaison par défaut vous donne un accès complet à Amazon WorkSpaces Secure Browser APIs via l'interface VPC endpoint. Pour contrôler l'accès accordé à Amazon WorkSpaces Secure Browser depuis votre VPC, associez une politique de point de terminaison personnalisée au point de terminaison VPC de l'interface.

Une politique de point de terminaison spécifie les informations suivantes :

- Les principaux qui peuvent effectuer des actions (Comptes AWS, utilisateurs IAM et rôles IAM).
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles les actions peuvent être exécutées.

Pour plus d'informations, consultez Contrôle de l'accès aux services avec points de terminaison d'un VPC dans le Guide de l'utilisateur Amazon VPC.

Exemple : politique de point de terminaison VPC pour les actions Amazon WorkSpaces Secure Browser

Voici un exemple de politique de point de terminaison personnalisée. Lorsque vous attachez cette politique au point de terminaison VPC de votre interface, elle accorde l'accès aux actions Amazon WorkSpaces Secure Browser répertoriées à tous les principaux sur toutes les ressources.

```
{
     "Statement": [
         {
             "Action": "workspaces-web:*",
             "Effect": "Allow",
             "Resource": "*",
             "Principal": "*"
         }
     ]
}
```

Résolution des problèmes

Si vos appels vers Amazon WorkSpaces Secure Browser APIs sont bloqués, il y a probablement une erreur de configuration dans votre groupe de sécurité VPC Endpoint Service ou dans la configuration du rôle IAM. Pour résoudre ce problème, essayez ce qui suit :

- Lors de la création de votre point de terminaison VPC d'interface, il se peut qu'il se soit automatiquement attaché au groupe de sécurité par défaut Compte AWS de votre interface. Essayez d'utiliser un autre groupe de sécurité et assurez-vous que les autorisations entrantes et sortantes vous permettent de transférer vos données de manière appropriée.
- Assurez-vous que vous utilisez un rôle IAM qui vous permet d'appeler Amazon WorkSpaces Secure Browser APIs.

Pour plus d'informations, voir Qu'est-ce que c'est AWS PrivateLink ? dans le guide de l'utilisateur Amazon VPC.

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 de plus amples informations, veuillez consulter the section called "Configuration de l'enregistrement des activités des utilisateurs".

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 de plus amples informations, veuillez consulter 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 EC2 instances Amazon 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' EC2 instances Amazon 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
`SessionIdleDisconnect`	Nombre de connexions fermées en raison de l'inactivité de l'utilisateur.	`[PortalId]`	Moyenne	Nombre
`ActiveSession`	Le nombre de sessions actives sur un portail.	`[PortalId]`	Moyenne	Nombre
`GlobalCpuPercent`	L'utilisation du processeur de l'instance de session Amazon WorkSpaces Secure Browser.	`[PortalId]` `[PortalId, UserName]`	Moyenne, Somme, Maximum, Minimum	Pourcentage
`GlobalMemoryPercent`	L'utilisation de la mémoire (RAM) de l'instance de session Amazon WorkSpaces Secure Browser.	`[PortalId]` `[PortalId, UserName]`	Moyenne, Somme, Maximum, Minimum	Pourcentage
`DisplayLatency`	Durée moyenne en millisecondes entre la capture de l'image et la présentation.	`[PortalId]` `[PortalId, UserName]`	Moyenne, maximale, minimale	Millisecondes

Métrique	Description	Dimensions	Statistiques	Unités
`InputLatency`	La latence d'entrée entre le client et le serveur. Par exemple, la latence entre le clic de souris du client et le clic de souris du serveur.	`[PortalId]` `[PortalId, UserName]`	Moyenne, maximale, minimale	Millisecondes
`SessionLoggerEventDelivered`	Le nombre d'événements que contient chaque fichier de journalisation de session livré.	`[PortalId]`	Moyenne, Somme, Maximum, Minimum	Nombre
`SessionLoggerTargetNotFoundError`	Le nombre de livraisons de fichiers journaux qui ont abouti à un bucket introuvable.	`[PortalId]`	Moyenne, Somme, Maximum, Minimum	Nombre
`SessionLoggerAccessDeniedError`	Nombre de livraisons de fichiers journaux ayant entraîné le refus d'autorisations.	`[PortalId]`	Moyenne, Somme, Maximum, Minimum	Nombre

> **Note**
>
> Les points de données métriques sont collectés par chaque session une fois par minute et publiés toutes les 5 minutes. CloudWatch Les métriques de l'enregistreur de session sont émises immédiatement, pour chaque livraison de fichier journal.

Dimensions des métriques d'Amazon WorkSpaces Secure Browser

Dimension	Description
PortalId	Filtre les données métriques pour Amazon WorkSpaces Secure Browser pour un portail spécifique.
UserName	Filtre les données métriques pour Amazon WorkSpaces Secure Browser pour un portail et un utilisateur spécifiques.

Vous pouvez utiliser cette SessionLoggerEventDeliveredmétrique pour surveiller le nombre total d'événements provenant de votre portail ou voir le nombre de fichiers journaux fournis en comptant le nombre de points de données plutôt qu'en additionnant les valeurs. Nous vous recommandons de configurer des alarmes sur les SessionLoggerAccessDeniedErrormétriques SessionLoggerTargetNotFoundErroret pour détecter la suppression accidentelle de ressources ou d'autorisations.

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.

Rubriques

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 de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

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"
    }]
}
```

Enregistrement de l'activité des utilisateurs dans Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser permet aux clients d'enregistrer les événements de session liés aux activités des utilisateurs dans les sessions Secure Browser.

WorkSpaces Secure Browser propose deux options pour enregistrer l'activité des utilisateurs et les événements liés à la sécurité :

- Session Logger capture un large éventail d'événements de session. Ces journaux sont envoyés dans un compartiment Amazon S3 de votre compte, ce qui permet une intégration facile à votre plateforme SIEM préférée.
- La journalisation des accès utilisateurs capture les événements de session les plus critiques. Ces journaux sont transmis à un flux Amazon Kinesis pour un traitement et une analyse en temps réel.

Pour plus d'informations sur la configuration de ces options, reportez-vous aux sections the section called “Configuration de l'enregistreur de session” etthe section called “Configuration de la journalisation des accès utilisateurs”.

Rubriques

- Événements de session dans Session Logger pour Amazon WorkSpaces Secure Browser
- Événements de session dans la journalisation de l'accès utilisateur pour Amazon WorkSpaces Secure Browser

Événements de session dans Session Logger pour Amazon WorkSpaces Secure Browser

L'enregistreur de session capture divers événements liés aux sessions à des fins de surveillance et d'audit.

Vous pouvez configurer l'enregistreur de session pour collecter tous les événements de session ou un sous-ensemble sélectionné, en fonction des besoins du portail WorkSpaces Secure Browser. Pour plus d'informations sur la configuration, consultezthe section called "Configuration de l'enregistreur de session".

Pour préserver la confidentialité des utilisateurs, Session Logger n'enregistre aucun contenu sensible, tel que les données du presse-papiers ou le contenu des fichiers chargés ou téléchargés.

Les champs suivants sont inclus dans tous les événements :

- Time (Période)
- Username
- ID du portail
- IP du portail
- IP du client
- Identifiant de session

Name (Nom)	Description	Champs supplémentaires inclus dans l'événement
SessionStart	Une session de navigation sécurisée a été lancée, mais l'utilisateur ne s'est pas encore connecté.	
SessionConnect	L'utilisateur est connecté à la session de navigateur sécurisée.	
TabOpen	Au cours de sa session de navigation sécurisée, l'utilisateur a ouvert un nouvel onglet ou un lien dans un nouvel onglet.	Nom d'hôte, chemin, URL (si l'utilisateur ouvre un lien dans un nouvel onglet), aucun (si l'utilisateur ouvre un nouvel onglet)

Name (Nom)	Description	Champs supplémentaires inclus dans l'événement
UrlVisit	Au cours de sa session de navigation, l'utilisateur a accédé à une URL.	Nom d'hôte, chemin, URL
WebsiteInteract	L'utilisateur a modifié un élément HTML standard sur un site Web (par exemple, clique sur une case à cocher, un bouton radio ou un bouton, ou sélectionne un élément dans le menu déroulant).	Nom d'hôte, chemin, URL
TabClose	Au cours de sa session de navigation, l'utilisateur a fermé un onglet.	Nom d'hôte, chemin, URL (si l'utilisateur ferme un onglet auquel il a accédé), aucun (si l'utilisateur ferme un nouvel onglet)
ContentTransferFro mLocalToRemoteClipboard	L'utilisateur a mis à jour le presse-papiers dans le navigateur sécurisé en utilisant le contenu de son navigateur local (en dehors de l'environnement sécurisé) . Cette mise à jour peut se produire soit en copiant le contenu via la barre d'outils en cours de session, soit en transférant des données via des raccourcis clavier (Ctrl+C/ Ctrl+V).	

Name (Nom)	Description	Champs supplémentaires inclus dans l'événement
ContentCopyFromWebsite	L'utilisateur a mis à jour le presse-papiers dans le navigateur sécurisé en utilisant le contenu du navigateur sécurisé (dans l'environnement sécurisé).	Nom d'hôte, chemin, URL
ContentPasteToWebsite	Le contenu du presse-papiers a été collé sur une page Web du navigateur. (Cet événement ne capture pas les cas où le contenu du presse-papiers est collé dans la barre d'URL du navigateur.)	Nom d'hôte, chemin, URL
PrintJobSubmit	L'utilisateur a soumis une demande de travail à l'imprimante virtuelle du navigateur (« Imprimante DCV »). Le contenu est enregistré au format PDF sur l'ordinateur local de l'utilisateur.	Nom de fichier, taille, extension
FileDownloadFromSecureBrowserToRemoteDisk	Un fichier a été enregistré depuis la session sur le disque local de l'instance distante.	Nom d'hôte, chemin URLfilename, taille, extension
FileTransferFromRemoteToLocalDisk	Un fichier a été téléchargé depuis le disque de l'instance distante vers le périphérique local de l'utilisateur.	Nom de fichier, taille, extension

Name (Nom)	Description	Champs supplémentaires inclus dans l'événement
FileUploadFromRemoteDiskToSecureBrowser	Un fichier stocké sur le disque local de l'instance distante a été chargé sur une plateforme SaaS de partage de fichiers (par exemple, Google Drive, Box ou File.io) via la session du navigateur.	
FileTransferFromLocalToRemoteDisk	Un fichier a été chargé depuis la machine utilisateur vers la session de navigateur sécurisée.	Nom de fichier, taille et extension
SessionDisconnection	L'utilisateur est déconnecté de la session de navigateur sécurisée.	
SessionEnd	La session de navigation sécurisée est terminée. La résiliation peut se produire de trois manières : l'administrateur met fin à la session via le gestionnaire de session utilisateur de la console, l'utilisateur met fin à la session manuellement en utilisant Fin de session dans la barre d'outils, ou la session expire après avoir dépassé une durée définie par l'administrateur.	

Chaque événement suit la norme OCSF et inclut une liste d'attributs communs à tous les événements :

```
{
    activity_name : String | A human readable name of the event | eg. UrlLoad
    activity_id : Integer | OCSF standard value 99 for 'others'
    category_name : "WorkSpacesSecureBrowser" | The category name where the event
 belongs to.
    category_id : 2 | Numerical identifier for category,
    metadata : link | Required {
        product : link {
            vendor_name : "wsb",
            name : "WorkSpacesSecureBrowser"
        }
        version : String | Version of the schema | eg. 1.0.0
    },
    severity_id : 1 | The severity of the event. All events will have a severity of 1,
 meaning 'Informational',
    type_id : class_uid * 100 + activity_id
    time : The time the event happened (RFC3339 format),
    observables : link [
        {
            name : "session_detail.portal_id",
            type_id : 10 //Resource UID
            value : //Generated value
        },
        {
            name : "session_detail.session_id",
            type_id : 10 //Resource UID
            value : //Generated value
        },
        {
            name : "session_detail.client_ip",
            type_id : 2 //IP Address
            value : //Generated value
        },
        {
            name : "session_detail.portal_ip",
            type_id : 2 //IP Address
            value : //Generated value
        },
        {
            name : "session_detail.username",
            type_id : 10 //Resource UID
            value : //Generated value
```

```
        }
    ],

    // New Events
    session_detail : {
        portal_id : String | UUID of the Portal | eg.
 1ebe42de-86bb-4073-88a4-34284bc5bcbb,
        session_id : String | SessionId of the user session | eg. 17be80fa-7bc2-4675-
b17a-791243938cdf
        client_ip : String | IP Address from which user LoggedIn From | eg. 31.65.180.9
        portal_ip : String | IP Address of the AWS AppStream Instance that is running
 the Portal | eg.240.62.100.169
        username : String | The logged-in username | eg. bobross
    }
}
```

Voici un exemple de l' URLVisit événement :

```
{
    activity_id : 99,
    activity_name : "URLVisit",
    ...
    observables : [
        ...
        {
            name : "url",
            type_id : 23 //Unified Resource Locator
        }
    ]
    ...
    url : {
        url_string : String | Full URL path,
        hostname : String | The hostname in the URL
        path : String | Path in the domain
    }
}
```

Voici un exemple de l' PrintJobSubmit événement :

```
{
    activity_id : 99,
    activity_name : "PrintJobSubmitted",
    observable : [
        ...
        {
            name : "file.name",
            type_id : 24 // File
        }
    ]
    ...
    file : {
        name : String | The file name,
        type_id : 1 //Regular file
        size : Long | Size in bytes
        ext : String | File extension
    }
}
```

Statistiques de l'enregistreur de session pour Amazon WorkSpaces Secure Browser

L'enregistreur de session émet les métriques suivantes Amazon CloudWatch .

Vous pouvez utiliser cette SessionLoggerEventDeliveredmétrique pour surveiller le nombre total d'événements provenant de votre portail ou voir le nombre de fichiers journaux fournis en comptant le nombre de points de données plutôt qu'en additionnant les valeurs. Nous vous recommandons de configurer des alarmes sur les SessionLoggerAccessDeniedErrormétriques SessionLoggerTargetNotFoundErroret pour détecter la suppression accidentelle de ressources ou d'autorisations.

> **Note**
>
> Les points de données métriques sont collectés par chaque session une fois par minute et publiés toutes les 5 minutes. Amazon CloudWatch Les métriques de l'enregistreur de session sont émises immédiatement, pour chaque livraison de fichier journal.

Métriques de l'enregistreur de session

Métrique	Description	Dimension	Statistiques	Unit
SessionLoggerEventDelivered	Le nombre d'événements que contient chaque fichier de journalisation de session livré.	[PortalId]	Moyenne, Somme, Maximum, Minimum	Nombre
SessionLoggerTargetNotFoundError	Le nombre de livraisons de fichiers journaux qui ont abouti à un bucket introuvable.	[PortalId]	Moyenne, Somme, Maximum, Minimum	Nombre
SessionLoggerAccessDeniedError	Nombre de livraisons de fichiers journaux ayant entraîné le refus d'autorisations.	[PortalId]	Moyenne, Somme, Maximum, Minimum	Nombre

Événements de session dans la journalisation de l'accès utilisateur pour Amazon WorkSpaces Secure Browser

Les événements de session suivants sont disponibles pour la journalisation de l'accès utilisateur :

- Validation : l'événement est correctement transféré dans le flux de données Kinesis.
- StartSession: L'utilisateur a ouvert une session et est connecté à la session de navigation sécurisée.
- VisitPage: L'utilisateur visite une page de la session.
- EndSession: L'utilisateur a mis fin à la session.

Les journaux de navigation par URL sont enregistrés à partir de l'historique du navigateur. URLs non enregistrées dans l'historique du navigateur (visitées en mode navigation privée ou supprimées 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 conformément à la politique de leur navigateur.

Vous trouverez ci-dessous un exemple de chaque événement disponible. 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"
}
```

Conseils pour les utilisateurs d'Amazon 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 du navigateur et de l'appareil pour Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser est alimenté par le client de navigateur Web Amazon 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 pour Amazon WorkSpaces Secure Browser

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 de session pour Amazon WorkSpaces Secure Browser

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

Rubriques

Démarrage d'une session dans Amazon WorkSpaces Secure Browser

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.

Utilisation de la barre d'outils dans Amazon WorkSpaces Secure Browser

Pour savoir comment utiliser la barre d'outils, procédez comme suit.

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. Use the down arrow to select from a list of available microphones.
	**Webcam**	Activate webcam for the session. Use the down arrow to select from a list of available webcams.
	**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 dans Amazon WorkSpaces Secure Browser

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.

Fin d'une session dans Amazon WorkSpaces Secure Browser

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 liés aux utilisateurs dans Amazon WorkSpaces Secure Browser

Si vous rencontrez l'un des problèmes suivants lors de l'utilisation de WorkSpaces Secure Browser, essayez les solutions suivantes.

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.

Comment savoir quelle and/or webcam avec microphone est utilisée et comment puis-je la modifier ?

Cliquez sur l'icône représentant une flèche vers le bas à côté du microphone ou de la caméra. Le menu affiche les appareils disponibles, avec une coche indiquant votre appareil actuel. Sélectionnez un autre appareil pour changer celui que vous souhaitez utiliser pour votre session.

Mon portail Web ne démarre pas s'il est accessible directement depuis le domaine personnalisé de l'entreprise

Si vous essayez de lancer une session en utilisant un nom de domaine autre que workspaces-web.comacme`.secureportal.mycompany.com`, assurez-vous que les cookies tiers sont activés dans votre navigateur pour le domaine de l'entreprise auquel vous accédez.

Extension d'authentification unique pour Amazon WorkSpaces Secure Browser

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.

Rubriques

Compatibilité de l'extension d'authentification unique pour Amazon WorkSpaces Secure Browser

L'extension d'authentification unique fonctionne avec les appareils et navigateurs suivants :

- Devices
  - Ordinateurs portables
  - Ordinateurs de bureau
- Navigateurs
  - Google Chrome
  - Mozilla Firefox

Installation de l'extension d'authentification unique pour Amazon WorkSpaces Secure Browser

Pour installer l'extension d'authentification unique, procédez comme suit.

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 liés à l'extension d'authentification unique pour Amazon WorkSpaces Secure Browser

Lorsque vous utilisez l'extension d'authentification unique, vous pouvez rencontrer le problème suivant.

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
Enregistreur de session	Configurez l'enregistreur de session pour capturer un large éventail d'événements de session.	1er août 2025
CloudWatch métriques	CloudWatch Métriques mises à jour.	21 juillet 2025
Contrôles de la barre	Avec les commandes de barre d'outils, vous pouvez configure r la présentation de la barre d'outils pour les sessions des utilisateurs finaux.	21 février 2025
Accès APIs via un point de terminaison VPC d'interface ()AWS PrivateLink	Appelez directement le point de terminaison de l'API Amazon WorkSpaces Secure Browser depuis un cloud privé (VPC), au lieu de vous connecter via Internet.	10 janvier 2025
Paramètres de protection des données	Ajoutez des paramètres de protection des données pour empêcher le partage des données pendant une session.	20 novembre 2024
Points de terminaison FIPS	Protégez les données en transit grâce aux points de terminaison FIPS.	7 octobre 2024

Tableau de bord de gestion des sessions	Utilisez le tableau de bord de gestion des sessions pour surveiller et gérer les sessions actives et complètes.	19 septembre 2024
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 politique 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.	1 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 URLs utilisateurs autorisés à accéder à partir de 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 politique 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 politique 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 politique gérée	Politique AmazonWorkSpacesWebReadOnly gérée mise à jour	2 novembre 2022
Mise à jour de politique 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 politique 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 AWS/Usage noms aux autorisations de l' PutMetricData API	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.