aws

管理ガイド

Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser: 管理ガイド

Table of Contents

Amazon WorkSpaces Secure Browser とは

> **Note**
>
> Amazon WorkSpaces Secure Browser は、以前は Amazon WorkSpaces Web と呼ばれていました。

Amazon WorkSpaces Secure Browser は、プライベートウェブサイトや software-as-a-service (SaaS) ウェブアプリケーションへの安全なアクセス、オンラインリソースとのやり取り、および、保管コンテナからのインターネットの閲覧に使用される、フルマネージド型のクラウドネイティブのホスト型ブラウザサービスです。 WorkSpaces Secure Browser は、アプライアンス、インフラストラクチャ、特殊なクライアントソフトウェア、仮想プライベートネットワーク (VPN) 接続の管理で IT に負担をかけずに、ユーザーの既存のウェブブラウザと連携します。ウェブコンテンツはユーザーのウェブブラウザにストリーミングされ、実際のブラウザとウェブコンテンツは で分離されます AWS。Amazon WorkSpaces や Amazon AppStream 2.0 などの AWS エンドユーザーコンピューティングサービスを強化するのと同じ基盤となるテクノロジーを使用することで、 WorkSpaces Secure Browser は従来の仮想デスクトップよりもコスト効率が高くなり、企業所有のデバイスに管理ソフトウェアを提供するよりも複雑さを軽減できます。 WorkSpaces Secure Browser は、ウェブコンテンツをストリーミングすることでデータ漏えいのリスクを軽減します。HTML、ドキュメントオブジェクトモデル (DOM)、または会社の機密データはローカルマシンに送信されません。デバイス、企業ネットワーク、インターネットを相互に分離することで、ブラウザのアタックサーフェスは事実上排除されます。

エンタープライズブラウザポリシー (URL 許可/ブロックを含む) をすべてのセッションに適用でき、クリップボード、ファイル転送、プリンターのセッションレベルの制御が含まれます。IP アクセスコントロールを使用して、信頼できるネットワークまたはデバイスへのアクセスを制限することもできます。 WorkSpaces Secure Browser は簡単にセットアップおよび運用できます。各セッションは、会社のポリシーと設定が適用された、新しく完全にパッチが適用されたバージョンの Chrome ブラウザで起動します。

リリース履歴

2024 年 5 月 20 日、Amazon WorkSpaces Web の名前が Amazon WorkSpaces Secure Browser に変更されました。既存の顧客の場合、 サービスでユーザーまたはリソースを管理する方法に変更はありませんでした。次のリストは、この名前変更の結果として発生した該当する更新を示しています。

workspaces-web API 名前空間は、下位互換性のために変更されません。その結果、次のリソースは同じままです。

- CLI コマンド。
- Amazon CloudWatch メトリクス。詳細については、「the section called “によるモニタリング CloudWatch”」を参照してください。
- サービスエンドポイント。詳細については、「Amazon WorkSpaces Secure Browser エンドポイントとクォータ」を参照してください。
- AWS CloudFormation リソース。詳細については、「Amazon WorkSpaces Secure Browser リソースタイプのリファレンス」を参照してください。
- workspaces-web を含むサービスにリンクされたロール。詳細については、「the section called “サービスリンクロールの使用”」を参照してください。
- workspacesURLs。
- workspacesURLs。詳細については、「Amazon WorkSpaces Secure Browser Documentation」を参照してください。
- 既存の ReadOnly マネージドロール。詳細については、「the section called “AWS マネージドポリシー”」を参照してください。
- KMS 許可名。
- UAL(User-Activity Logging) Kinesis ストリームプレフィックス。

さらに、既存のポータル URLs変わりません。2024 年 5 月 20 日より前に作成されたポータルの URLs は、<UUID>.workspaces-web.com. WorkSpaces Secure Browser ポータルの形式を使用し、引き続きこの形式と workspaces-web.com ドメインを使用します。

WorkSpaces Secure Browser を使用する際に知っておくべき用語

WorkSpaces Secure Browser の使用を開始するには、以下の概念を理解しておく必要があります。

ID プロバイダー (IdP)

ID プロバイダーはユーザーの認証情報を検証します。その後、認証アサーションを発行し、サービスプロバイダーへのアクセスを提供します。Secure Browser と連携するように既存の IdP WorkSpaces を設定できます。

ID プロバイダー (IdP) の設定プロセスは、IdP によって異なります。

サービスプロバイダーのメタデータファイルを IdP にアップロードする必要があります。そうしないと、ユーザーはログインできません。また、IdP で WorkSpaces Secure Browser を使用するには、ユーザーにアクセス権を付与する必要があります。

ID プロバイダー (IdP) メタデータドキュメント

WorkSpaces Secure Browser では、信頼を確立するために ID プロバイダー (IdP) からの特定のメタデータが必要です。IdP からダウンロードしたメタデータ交換ファイルをアップロードすることで、このメタデータを WorkSpaces Secure Browser に追加できます。

サービスプロバイダー (SP)

サービスプロバイダーは認証アサーションを受け入れ、ユーザーにサービスを提供します。WorkSpaces Secure Browser は、IdP によって認証されたユーザーのサービスプロバイダーとして機能します。

サービスプロバイダー (SP) メタデータドキュメント

ID プロバイダー (IdP) の設定インターフェースにサービスプロバイダーのメタデータの詳細を追加する必要があります。この設定プロセスの詳細はプロバイダーによって異なります。

SAML 2.0

IdP とサービスプロバイダーの間で認証と認可データを交換するための標準。

仮想プライベートクラウド (VPC)

既存または新規の VPC、対応するサブネット、およびセキュリティグループを使用して、コンテンツを WorkSpaces Secure Browser にリンクできます。

サブネットはインターネットへの安定した接続を備えている必要があり、ユーザーがこれらのリソースにアクセスするには、VPC とサブネットが内部および Software as a Service (SaaS) Web サイトへの安定した接続を備えている必要があります。

リストVPCs、サブネット、およびセキュリティグループは、 WorkSpaces Secure Browser コンソールと同じリージョンから取得されます。

信頼ストア

WorkSpaces Secure Browser を介してウェブサイトにアクセスするユーザーが NET::ERR_CERT_INVALID などのプライバシーエラーを受け取った場合、そのサイトはプライベート認証局 (PCA) によって署名された証明書を使用している可能性があります。信頼ストアの PCA を追加または変更する必要がある場合があります。さらに、ユーザーのデバイスがウェブサイトをロードするために特定の証明書をインストールする必要がある場合は、その証明書を信頼

ストアに追加して、ユーザーが WorkSpaces Secure Browser でそのサイトにアクセスできるようにする必要があります。

一般にアクセス可能なウェブサイトでは、通常、信頼ストアを変更する必要はありません。

ウェブポータル

ウェブポータルは、ユーザーがブラウザから内部および SaaS ウェブサイトにアクセスできるようにします。1 つのアカウントで、サポートされている任意のリージョンに 1 つのウェブポータルを作成できます。複数のポータル制限の引き上げをリクエストするには、サポートにお問い合わせください。

ウェブポータルエンドポイント

ウェブポータルエンドポイントは、ポータルに設定されている ID プロバイダーを使用してユーザーがサインインした後にウェブポータルを起動するアクセスポイントです。

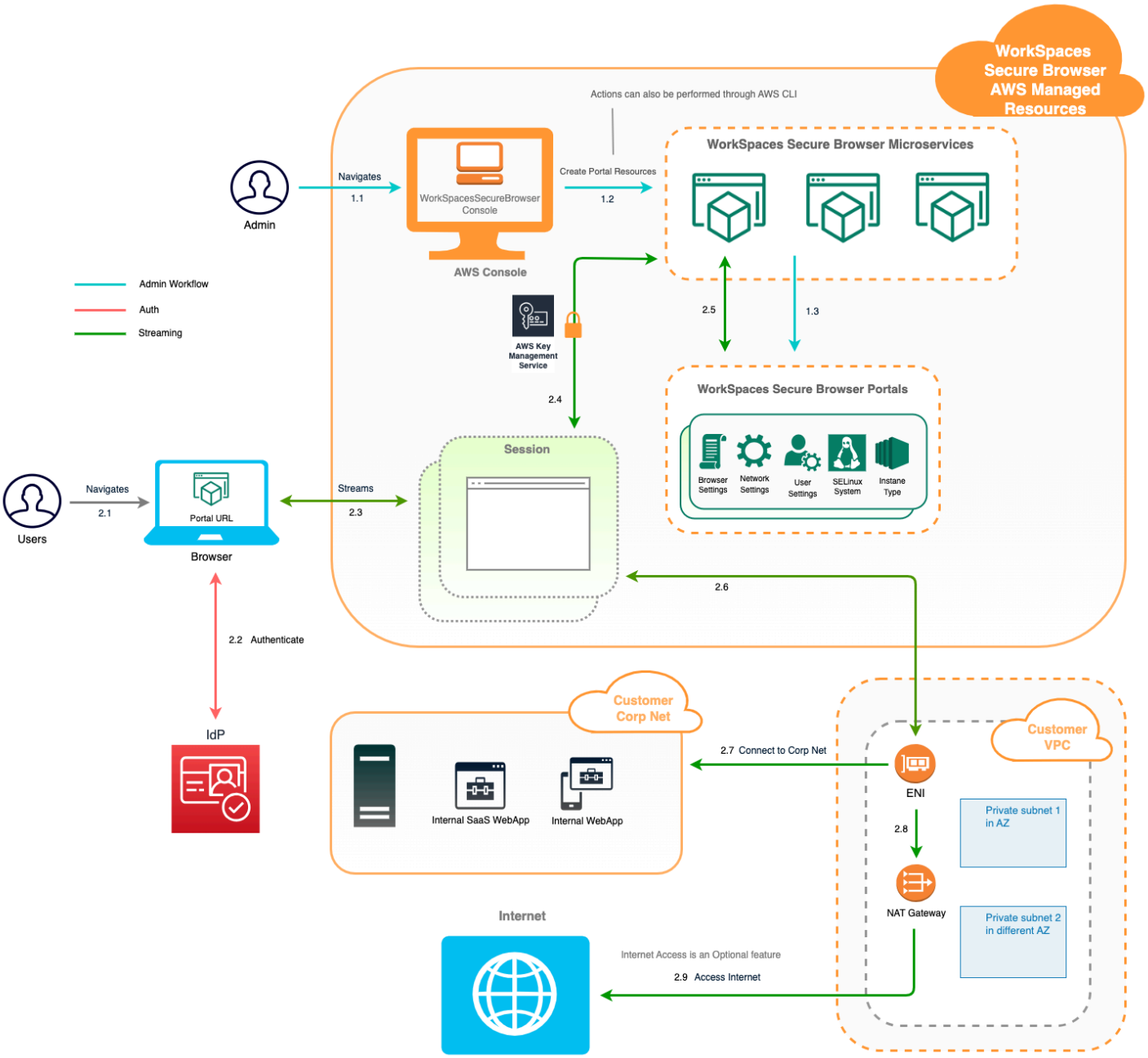
エンドポイントはインターネット上で公開されており、ネットワークに埋め込むことができます。

関連サービス

WorkSpaces Secure Browser は、AWS エンドユーザーコンピューティングポートフォリオ WorkSpaces の Amazon の機能です。 WorkSpaces および AppStream 2.0 と比較すると、WorkSpaces Secure Browser は、安全なウェブベースのワークロードを容易にするために特別に構築されています。 WorkSpaces Secure Browser は自動的に管理され、AWS によってオンデマンドで容量、スケーリング、イメージがプロビジョニングおよび更新されます。例えば、デスクトップリソースへのアクセスを必要とするソフトウェアデベロッパーに永続的な Workspace Desktop を提供し、デスクトップコンピュータ上の少数の内部ウェブサイトと SaaS ウェブサイト (ネットワーク外でホストされているウェブサイトを含む) にのみアクセスする必要があるコンタクトセンターユーザーに WorkSpaces Secure Browser を提供できます。

アーキテクチャ

次の図は、 WorkSpaces Secure Browser のアーキテクチャを示しています。



WorkSpaces Secure Browser へのアクセス

管理者は WorkSpaces 、Secure Browser コンソール、SDK、CLI、または API を介して WorkSpaces Secure Browser にアクセスします。ユーザーは、 WorkSpaces Secure Browser エンドポイントを介してこれにアクセスします。

WorkSpaces Secure Browser のセットアップ

内部ウェブサイトと SaaS アプリケーションにアクセスするように WorkSpaces Secure Browser を設定する前に、次の前提条件を満たす必要があります。

トピック

サインアップしてユーザーを作成する

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

   にサインアップすると AWS アカウント、 AWS アカウントのルートユーザーが作成されます。ルートユーザーには、アカウントのすべての AWS サービス とリソースへのアクセス権があります。セキュリティのベストプラクティスとして、ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用してルートユーザーアクセスが必要なタスクを実行してください。

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ の 「アカウント」 をクリックして、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理することができます。

管理アクセスを持つユーザーを作成する

にサインアップしたら AWS アカウント、 を保護し AWS アカウントのルートユーザー、 を有効にして AWS IAM Identity Center、日常的なタスクにルートユーザーを使用しないように管理ユーザーを作成します。

のセキュリティ保護 AWS アカウントのルートユーザー

1. ルートユーザーを選択し、 AWS アカウント E メールアドレスを入力して、アカウント所有者AWS Management Consoleとして にサインインします。次のページでパスワードを入力します。

   ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドの「ルートユーザーとしてサインインする」を参照してください。
2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、「IAM ユーザーガイド」の AWS アカウント 「ルートユーザーの仮想 MFA デバイスを有効にする (コンソール)」を参照してください。

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「AWS IAM Identity Centerの有効化」を参照してください。
2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

   を ID ソース IAM アイデンティティセンターディレクトリ として使用する方法のチュートリアルについては、「 ユーザーガイド」の「デフォルト でユーザーアクセスを設定する IAM アイデンティティセンターディレクトリAWS IAM Identity Center 」を参照してください。

管理アクセス権を持つユーザーとしてサインインする

- IAM アイデンティティセンターのユーザーとしてサインインするには、IAM アイデンティティセンターのユーザーの作成時に E メールアドレスに送信されたサインイン URL を使用します。

  IAM Identity Center ユーザーを使用してサインインする方法については、「 AWS サインイン ユーザーガイド」の AWS 「 アクセスポータルにサインインする」を参照してください。

追加のユーザーにアクセス権を割り当てる

1. IAM アイデンティティセンターで、最小特権のアクセス許可を適用するというベストプラクティスに従ったアクセス許可セットを作成します。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」を参照してください。
2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「グループの参加」を参照してください。

プログラムによるアクセス権を付与する

ユーザーが の AWS 外部とやり取りする場合は、プログラムによるアクセスが必要です AWS Management Console。プログラムによるアクセスを許可する方法は、 にアクセスするユーザーのタイプによって異なります AWS。

ユーザーにプログラマチックアクセス権を付与するには、以下のいずれかのオプションを選択します。

プログラマチックアクセス権を必要とするユーザー	目的	方法
ワークフォースアイデンティティ (IAM Identity Center で管理されているユーザー)	一時的な認証情報を使用して、、 AWS SDKs AWS CLI、または AWS APIs。	使用するインターフェイス用の手引きに従ってください。 • については AWS CLI、「 ユーザーガイド」の AWS CLI 「 を使用するための の設定 AWS IAM Identity CenterAWS Command Line Interface 」を参照してください。 • AWS SDKs 、ツール、AWS APIs「 SDK とツールのリファレンスガイド」

プログラマチックアクセス権を必要とするユーザー	目的	方法
		の「IAM Identity Center 認証」を参照してください。 AWS SDKs
IAM	一時的な認証情報を使用して、、 AWS SDKs AWS CLI、または AWS APIs。	「IAM ユーザーガイド」の「 AWS リソースでの一時的な認証情報の使用」の手順に従います。
IAM	(非推奨) 長期認証情報を使用して、、 AWS SDKs AWS CLI、または AWS APIs。	使用するインターフェイス用の手引きに従ってください。 • については AWS CLI、「 AWS Command Line Interface ユーザーガイド」の「IAM ユーザー認証情報を使用した認証」を参照してください。 • AWS SDKs「 SDK とツールのリファレンスガイド」の「長期的な認証情報を使用した認証」を参照してください。 AWS SDKs • AWS APIsユーザーガイド」の「IAM ユーザーのアクセスキーの管理」を参照してください。

ネットワークとアクセス

以下のトピックでは、ユーザーが WorkSpaces Secure Browser ストリーミングインスタンスに接続できるようにインスタンスを設定する方法について説明します。また、 WorkSpaces Secure Browser ストリーミングインスタンスが VPC リソースおよびインターネットにアクセスできるようにする方法についても説明します。

トピック

VPC の要件

WorkSpaces Secure Browser ポータルの作成時に、アカウント内の VPC を選択します。また、2 つの異なるアベイラビリティーゾーンで少なくとも 2 つのサブネットを選択します。これらの VPC とサブネットは、次の要件を満たしている必要があります。

- VPC にはデフォルトのテナンシーが必要です。専用テナンシーを備えた VPC はサポートされていません。
- 可用性を考慮して、2 つの異なるアベイラビリティーゾーンで少なくとの 2 つのサブネットを作成する必要があります。サブネットには、予想される WorkSpaces Secure Browser トラフィックをサポートするのに十分な IP アドレスが必要です。各サブネットに、同時セッションの最大数を考慮するのに十分な数のクライアント IP アドレスを許可するサブネットマスクを設定します。詳細については、「新しい VPC の作成と設定」を参照してください。
- すべてのサブネットは、ユーザーが WorkSpaces Secure Browser でアクセスする AWS クラウドまたはオンプレミスの内部コンテンツに安定して接続する必要があります。

アベイラビリティーとスケーリングを考慮して、異なるアベイラビリティーゾーンで 3 つのサブネットを選択することをお勧めします。詳細については、「新しい VPC の作成と設定」を参照してください。

WorkSpaces Secure Browser は、インターネットアクセスを有効にするためにストリーミングインスタンスにパブリック IP アドレスを割り当てません。これにより、ストリーミングインスタンスにインターネットからアクセス可能になります。そのため、パブリックサブネットに接続されたストリーミングインスタンスはインターネットにアクセスできなくなります。 WorkSpaces Secure Browser ポータルでパブリックインターネットコンテンツとプライベート VPC コンテンツの両方にアクセスできるようにするには、「」の手順を実行します無制限のインターネットブラウジングを有効にする (推奨)。

新しい VPC の作成と設定

このセクションでは、VPC ウィザードを使用して、パブリックサブネットと 1 つとプライベートサブネット 1 つを持つ VPC を作成する方法について説明します。このプロセスの一環として、ウィザードはインターネットゲートウェイと NAT ゲートウェイを作成します。また、サブネットに関連付けられているカスタムルートテーブルも作成します。次に、プライベートサブネットに関連付けられているメインルートテーブルを更新します。NAT ゲートウェイは、VPC のパブリックサブネットで自動的に作成されます。

ウィザードを使用して VPC 設定を作成したら、2 つ目のプライベートサブネットを追加します。この設定の詳細については、「パブリックサブネットとプライベートサブネットを持つ VPC (NAT)」を参照してください。

ステップ 1: Elastic IP アドレスを割り当てる

VPC を作成する前に、 WorkSpaces Secure Browser リージョンに Elastic IP アドレスを割り当てる必要があります。割り当てたら、Elastic IP アドレスを NAT ゲートウェイに関連付けることができます。Elastic IP アドレス を使用すると、ストリーミングインスタンスに障害が発生しても、そのアドレスを VPC 内の別のストリーミングインスタンスにすばやく再マッピングすることで、ストリーミングインスタンスの障害を隠すことができます。詳細については、「Elastic IP アドレス」を参照してください。

> **Note**
>
> 使用する Elastic IP アドレスには料金が適用される場合があります。詳細については、「Elastic IP アドレスの料金表ページ」を参照してください。

Elastic IP アドレスをまだ持っていない場合は、以下のステップを実行します。既存の Elastic IP アドレスを使用する場合は、最初にそのアドレスが別のインスタンスやネットワークインターフェイスに現在関連付けられていないことを確認します。

Elastic IP アドレスを割り当てるには

1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
2. ナビゲーションペインの [Network & Security] で、[Elastic IPs] を選択します。
3. [Allocate New Address (新しいアドレスの割り当て)] を選択し、続いて [Allocate (割り当て)] を選択します。

4. コンソールに表示された Elastic IP アドレスをメモします。
5. [Elastic IP] ペインの右上にある [X] アイコンをクリックしてペインを閉じます。

ステップ 2: 新しい VPC を作成する

1 つのパブリックサブネットと 1 つのプライベートサブネットを持つ新しい VPC を作成するには、次のステップを実行します。

新しい VPC を作成するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[VPC ダッシュボード] を選択します。
3. Launch VPC Wizard (VPC ウィザードの起動) を選択します。
4. [Step 1: Select a VPC Configuration (ステップ 1: VPC 設定を選択する)] ページで [VPC with Public and Private Subnets (パブリックサブネットとプライベートサブネットを持つ VPC)] を選択し、[Select (選択)] を選択します。
5. [Step 2: VPC with Public and Private Subnets (ステップ 2: パブリックサブネットとプライベートサブネットを持つ VPC)] で、VPC を次のように設定します。
   - [IPv4 CIDR block (IPv4 CIDR ブロック)] では、VPC 用の IPv4 CIDR ブロックを指定します。
   - [IPv6 CIDR ブロック] は、デフォルト値の、[No IPv6 CIDR Block (IPv6 CIDR ブロックなし)] のままにしておきます。
   - [VPC 名] に VPC の一意の名前を入力します。
   - パブリックサブネットを次のように設定します。
     - [Public subnet's IPv4 CIDR (パブリックサブネットの IPv4 CIDR)] に、サブネットの CIDR ブロックを指定します。
     - [Availability Zone (アベイラビリティーゾーン)] では、デフォルト値の、[No Preference (指定なし)] のままにしておきます。
     - [パブリックサブネット名] に、サブネットの名前を入力します。例えば **`WorkSpaces Secure Browser Public Subnet`** です。
   - 最初のプライベートサブネットを次のように設定します。
     - [Private subnet's IPv4 CIDR (プライベートサブネットの IPv4 CIDR)] に、サブネットの CIDR ブロックを入力します。指定した値を書き留めておきます。
     - [Availability Zone (アベイラビリティーゾーン)] で、特定のゾーンを選択し、選択したゾーンを書き留めます。

  - [プライベートサブネット名] に、サブネットの名前を入力します。例えば **WorkSpaces Secure Browser Private Subnet1** です。
- 残りのフィールドについては、該当する場合はデフォルト値をそのまま使用します。
- [Elastic IP 割り当て ID] で、テキストボックスをクリックし、作成した Elastic IP アドレスに対応する値を選択します。このアドレスは NAT ゲートウェイに割り当てられます。Elastic IP アドレスがない場合は、https://console.aws.amazon.com/vpc/ の Amazon VPC コンソールを使用して作成します。
- [Service endpoints (サービスエンドポイント)] で、環境に Amazon S3 エンドポイントが必要な場合は、エンドポイントを指定します。

  Amazon S3 エンドポイントを指定するには、次の手順を実行します。

  1. [Add Endpoint (エンドポイントの追加)] を選択します。
  2. サービス で、com.amazonaws.***Region*** .s3 エントリを選択します。ここで、*Region* は VPC AWS リージョン を作成する です。
  3. [Subnet (サブネット)] で、[Private subnet (プライベートサブネット)] を選択します。
  4. [Policy (ポリシー)] では、既定値の [Full Access (フルアクセス)] のままにします。
- [Enable DNS hostnames (DNS ホスト名を有効にする)] では、デフォルト値の [Yes (はい)] のままにします。
- [Hardware tenancy (ハードウェアテナンシー)] では、デフォルト値の [Default (デフォルト)] のままにします。
- [Create VPC (VPC の作成)] を選択します。
- VPC の設定には数分かかります。VPC が作成されたら、[OK] を選択します。

ステップ 3: 2 番目のプライベートサブネットを追加する

前のステップで、1 つのパブリックサブネットと 1 つのプライベートサブネットを持つ VPC を作成しました。VPC に 2 つ目のプライベートサブネットを追加するには、以下のステップを実行します。1 つ目のプライベートサブネットとは異なるアベイラビリティーゾーンに 2 つ目のプライベートサブネットを追加することをお勧めします。

2 つ目のプライベートサブネットを追加するには

1. ナビゲーションペインで、[Subnets (サブネット)] を選択します。

2. 前のステップで作成した最初のプライベートサブネットを選択します。サブネットのリストの下にある [Description (説明)] タブで、このサブネットのアベイラビリティーゾーンを書き留めます。
3. サブネットペインの左上にある [Create Subnet (サブネットの作成)] を選択します。
4. [名前タグ] に、プライベートサブネットの名前を入力します。例えば **WorkSpaces Secure Browser Private Subnet2** です。
5. [VPC] では、前のステップで作成した VPC を選択します。
6. [アベイラビリティーゾーン] で、最初のプライベートサブネットに使用しているアベイラビリティーゾーン以外のアベイラビリティーゾーンを選択します。別のアベイラビリティーゾーンを選択すると、耐障害性が向上し、容量不足エラーを防ぐのに役立ちます。
7. [IPv4 CIDR block (IPv4 CIDR ブロック)] の場合は、新しいサブネットの一意の CIDR ブロック範囲を指定します。例えば、最初のプライベートサブネットの IPv4 CIDR ブロック範囲が **10.0.1.0/24** である場合、2 つ目のプライベートサブネットに **10.0.2.0/24** の CIDR ブロック範囲を指定できます。
8. [Create] (作成) を選択します。
9. サブネットが作成されたら、[Close (閉じる)] を選択します。

ステップ 4: サブネットルートテーブルの検証と命名

VPC を作成して設定したら、以下のステップを実行してルートテーブルの名前を指定します。ルートテーブルに関する以下の情報が正しいことを確認する必要があります。

- NAT ゲートウェイが存在するサブネットに関連付けられたルートテーブルには、インターネットゲートウェイへのインターネットトラフィックを指すルートが含まれる必要があります。これにより、NAT ゲートウェイがインターネットにアクセスできるようになります。
- プライベートサブネットに関連付けられたルートテーブルは、インターネットトラフィックを NAT ゲートウェイに向けるように設定される必要があります。これにより、プライベートサブネットのストリーミングインスタンスがインターネットと通信できるようになります。

サブネットルートテーブルを検証および命名するには

1. ナビゲーションペインで [サブネット] を選択し、作成したパブリックサブネットを選択します。例えば、WorkSpaces Secure Browser 2.0 Public Subnet などです。
2. [ルートテーブル] タブで、ルートテーブルの ID を選択します。例えば、rtb-12345678 です。

3. ルートテーブルを選択します。[名前] で、編集 (鉛筆) アイコンを選択し、テーブルの名前を入力します。例えば、名前を **workspacesweb-public-routetable** と入力します。その後、チェックマークをオンにして名前を保存します。
4. パブリックルートテーブルを選択したまま、[ルート] タブで、2 つのルートがあることを確認します。1 つはローカルトラフィック用で、もう 1 つは他のすべてのトラフィックをインターネットゲートウェイに送信する VPC 用です。以下のテーブルでは、これらの 2 つのルートについて説明しています。

送信先	ターゲット	説明
パブリックサブネット IPv4 CIDR ブロック (10.0.0/20 など)	ローカル	パブリックサブネット IPv4 CIDR ブロック内の IPv4 アドレス宛てのリソースからのトラフィック。このトラフィックは VPC 内でローカルにルーティングされます。
その他のすべての IPv4 アドレス宛てのトラフィック (0.0.0.0/0 など)	アウトバウンド (IGW-ID)	その他すべての IPv4 アドレス宛てのトラフィックは、VPC ウィザードで作成されたインターネットゲートウェイ (igw-ID で識別) にルーティングされます。

5. ナビゲーションペインで、[Subnets (サブネット)] を選択します。次に、作成した最初のプライベートサブネットを選択します (例: **WorkSpaces Secure Browser Private Subnet1**)。
6. [ルートテーブル] タブで、ルートテーブルの ID を選択します。
7. ルートテーブルを選択します。[名前] で、編集 (鉛筆) アイコンを選択し、テーブルの名前を入力します。例えば、名前を **workspacesweb-private-routetable** と入力します。名前を保存するには、チェックマークアイコンを選択します。
8. [Routes (ルート)] タブで、ルートテーブルに次のルートが含まれていることを確認します。

送信先	ターゲット	説明
パブリックサブネット IPv4 CIDR ブロック (10.0.0/20 など)	ローカル	パブリックサブネット IPv4 CIDR ブロック内の IPv4 アドレス宛てのリソースからのトラフィックはすべて、VPC 内でローカルにルーティングされます。
その他のすべての IPv4 アドレス宛てのトラフィック (0.0.0.0/0 など)	アウトバウンド (nat-ID)	その他すべての IPv4 アドレス宛てのトラフィックは、NAT ゲートウェイ (nat-ID で識別) にルーティングされます。
S3 バケット宛てのトラフィック (S3 エンドポイントを指定した場合に適用) [pl-ID (com.amazonaws.region.s3)]	ストレージ (vpce-ID)	S3 バケット宛てのトラフィックは、S3 エンドポイント (vpce-ID で識別) にルーティングされます。

9. ナビゲーションペインで、[Subnets (サブネット)] を選択します。次に、作成した 2 つ目のプライベートサブネットを選択します (例:**`WorkSpaces Secure Browser Private Subnet2`**)。
10. [ルートテーブル] タブで、選択したルートテーブルがプライベートルートテーブルであることを確認します (例: **`workspacesweb-private-routetable`**)。ルートテーブルが異なる場合は、[編集] を選択して、代わりにプライベートルートテーブルを選択します。

無制限のインターネットブラウジングを有効にする (推奨)

次の手順に従って、NAT ゲートウェイを含む VPC を設定して、無制限のインターネットブラウジングを可能にします。これにより、パブリックインターネット上のサイト、および でホストされている、または VPC への接続が可能なプライベートサイトへの WorkSpaces Secure Browser アクセスが付与されます。

NAT ゲートウェイを含む VPC を設定して、無制限のインターネットブラウジングを可能にするには

WorkSpaces Secure Browser ポータルでパブリックインターネットコンテンツとプライベート VPC コンテンツの両方にアクセスできるようにするには、次の手順に従います。

> **Note**
>
> すでに VPC を設定している場合は、次のステップを実行して NAT ゲートウェイを VPC に追加します。新しい VPC を作成する必要がある場合は、「新しい VPC の作成と設定」を参照してください。

1. NAT ゲートウェイを作成するには、「NAT ゲートウェイを作成する」の手順を完了します。この NAT ゲートウェイがパブリックに接続され、VPC のパブリックサブネットにあることを確認します。
2. 異なるアベイラビリティーゾーンから少なくとも 2 つのサブネットを指定する必要があります。サブネットを異なるアベイラビリティーゾーンに割り当てると、可用性と耐障害性が向上します。2 番目のプライベートサブネットを作成する方法については、「the section called “ステップ 3: 2 番目のプライベートサブネットを追加する”」を参照してください。

   > **Note**
   >
   > すべてのストリーミングインスタンスがインターネットにアクセスできるように、WorkSpaces Secure Browser ポータルにパブリックサブネットをアタッチしないでください。

3. プライベートサブネットに関連付けられたルートテーブルを更新して、インターネットバウンドトラフィックを NAT ゲートウェイに向かわせます。これにより、プライベートサブネットのストリーミングインスタンスがインターネットと通信できるようになります。ルートテーブルをプライベートサブネットに関連付ける方法については、「ルートテーブルを設定する」の手順を実行してください。

制限されたインターネットブラウジングを有効にする (アウトバウンド HTTP プロキシを使用)

WorkSpaces Secure Browser ポータルの推奨されるネットワーク設定は、NAT ゲートウェイでプライベートサブネットを使用することです。これにより、ポータルはパブリックインターネットとプライベートコンテンツの両方を参照できます。詳細については、「the section called “無制限のイン

ターネットブラウジングを有効にする (推奨)"」を参照してください。ただし、ウェブプロキシを使用して、 WorkSpaces Secure Browser ポータルからインターネットへのアウトバウンド通信を制御する必要がある場合があります。例えば、ウェブプロキシをインターネットへのゲートウェイとして使用する場合は、ドメインの許可リストやコンテンツフィルタリングなどの予防セキュリティコントロールを実装できます。また、ウェブページやソフトウェア更新など、頻繁にアクセスされるリソースをローカルにキャッシュすることで、帯域幅の使用量を減らし、ネットワークパフォーマンスを向上させることもできます。ユースケースによっては、ウェブプロキシを使用してのみアクセスできるプライベートコンテンツがある場合があります。

マネージドデバイスまたは仮想環境のイメージでのプロキシ設定の構成に既に慣れているかもしれません。ただし、デバイスを管理していない場合 (例えば、ユーザーがエンタープライズによって所有または管理されていないデバイス上にある場合) 、または仮想環境のイメージを管理する必要がある場合、これは課題となります。 WorkSpaces Secure Browser を使用すると、ウェブブラウザに組み込まれている Chrome のポリシーを使用してプロキシ設定を行うことができます。これを行うには、 WorkSpaces Secure Browser の HTTP アウトバウンドプロキシを設定します。

このソリューションは、推奨されるアウトバウンド VPC プロキシの設定に基づいています。プロキシソリューションは、オープンソースの HTTP プロキシ Squid に基づいています。次に、WorkSpaces Secure Browser ブラウザ設定を使用して、プロキシエンドポイントに接続するように WorkSpaces Secure Browser ポータルを設定します。詳細については、「ドメインのホワイトリスト登録とコンテンツフィルタリングを使用してアウトバウンド VPC プロキシを設定する方法」を参照してください。

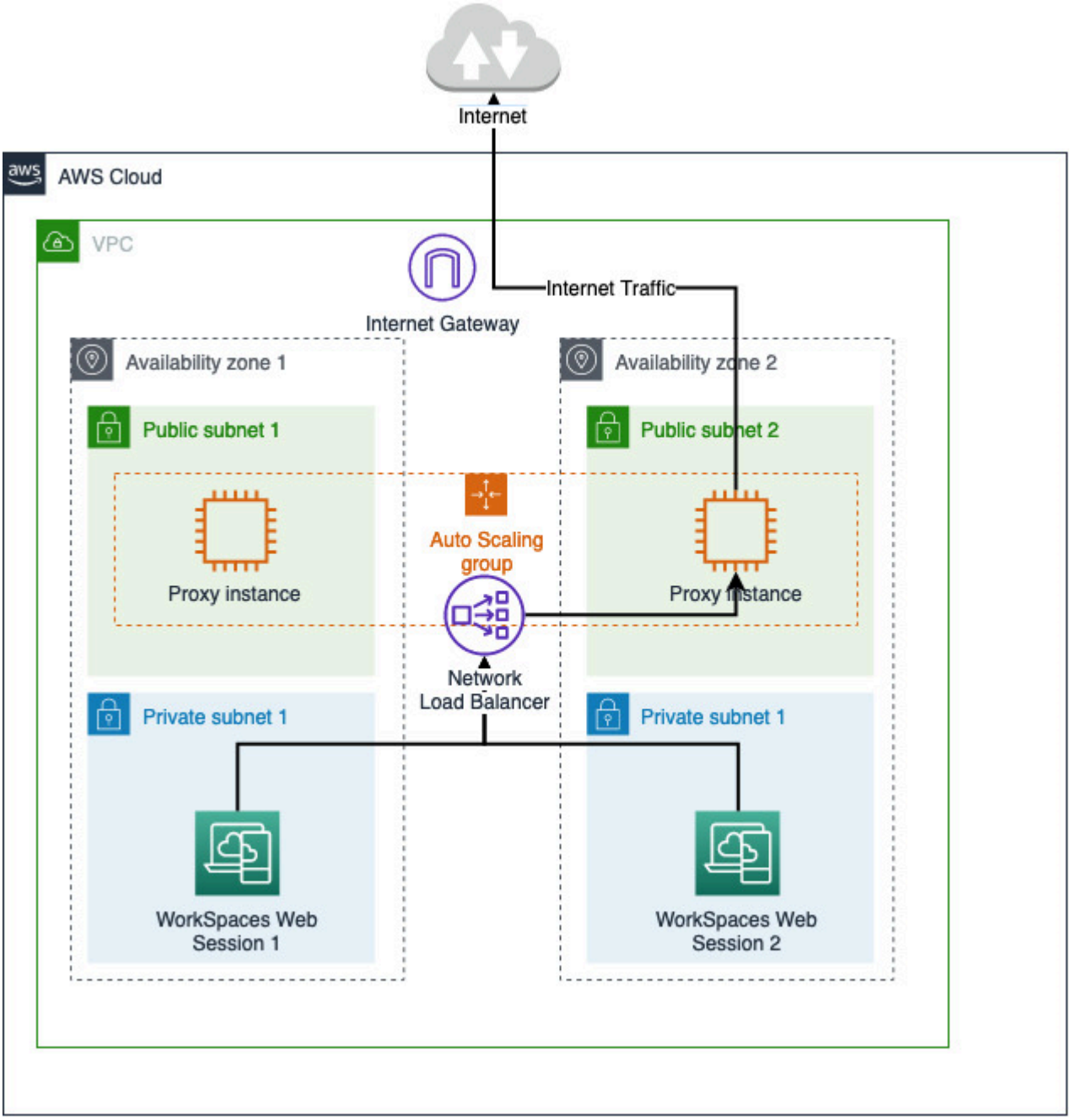
このソリューションには、次の利点があります。

- Network Load Balancer によってホストされる、自動スケーリング Amazon EC2 インスタンスのグループを含むアウトバウンドプロキシ。プロキシインスタンスはパブリックサブネット内にあり、それぞれに Elastic IP がアタッチされているため、インターネットにアクセスできます。
- プライベートサブネットにデプロイされた WorkSpaces Secure Browser ポータル。インターネットアクセスを有効にするために NAT ゲートウェイを設定する必要はありません。代わりに、すべてのインターネットトラフィックがアウトバウンドプロキシを通過するようにブラウザポリシーを設定します。独自のプロキシを使用する場合、 WorkSpaces Secure Browser ポータルの設定は似ています。

アーキテクチャ

VPC での一般的なプロキシ設定の例を次に示します。プロキシ Amazon EC2 インスタンスはパブリックサブネットにあり、Elastic IP に関連付けられているため、インターネットにアクセスできま

す。Network Load Balancer は、プロキシインスタンスの Auto Scaling グループをホストします。これにより、プロキシインスタンスは自動的にスケールアップでき、Network Load Balancer は単一のプロキシエンドポイントであり、Secure Browser WorkSpaces セッションで使用できます。



前提条件

開始する前に、次の前提条件を満たしていることを確認してください。

- パブリックサブネットとプライベートサブネットが複数のアベイラビリティーゾーン (AZsが必要です。VPC 環境の設定方法の詳細については、「デフォルト VPCs」を参照してください。

- プライベートサブネットからアクセス可能な単一のプロキシエンドポイントが必要です。WorkSpaces Secure Browser セッションはライブです (例えば、Network Load Balancer DNS 名) 。既存のプロキシを使用する場合は、プライベートサブネットからアクセス可能なエンドポイントが 1 つあることを確認してください。

WorkSpaces Secure Browser 用の HTTP アウトバウンドプロキシを設定する

WorkSpaces Secure Browser の HTTP アウトバウンドプロキシを設定するには、次の手順に従います。

1. アウトバウンドプロキシの例を VPC にデプロイするには、「ドメインのホワイトリスト登録とコンテンツフィルタリングを使用してアウトバウンド VPC プロキシを設定する方法」のステップに従います。
   a. 「インストール (ワンタイムセットアップ) 」の手順に従って、テンプレートを CloudFormationアカウントにデプロイします。テンプレート CloudFormation パラメータとして、必ず適切な VPC とサブネットを選択してください。
   b. デプロイ後、 CloudFormation 出力パラメータOutboundProxyドメイン とOutboundProxyポート を見つけます。これはプロキシの DNS 名とポートです。
   c. 既に独自のプロキシがある場合は、このステップをスキップし、プロキシの DNS 名とポートを使用します。
2. WorkSpaces Secure Browser コンソールで、ポータルを選択し、編集を選択します。
   a. ネットワーク接続の詳細 で、プロキシにアクセスできる VPC とプライベートサブネットを選択します。
   b. ポリシー設定 で、JSON エディタを使用して次の ProxySettingsポリシーを追加します。`ProxyServer` フィールドはプロキシの DNS 名とポートである必要があります。ProxySettings ポリシーの詳細については、「」を参照してください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. WorkSpaces Secure Browser セッションでは、Chrome が管理者 からのプロキシ設定を使用している Chrome 設定にプロキシが適用されていることがわかります。
4. chrome://policy に移動し、Chrome ポリシータブに移動して、ポリシーが適用されていることを確認します。
5. WorkSpaces Secure Browser セッションが NAT ゲートウェイなしでインターネットコンテンツを正常に参照できることを確認します。 CloudWatch ログで、Squid プロキシアクセスログが記録されていることを確認します。

トラブルシューティング

Chrome ポリシーが適用された後でも WorkSpaces Secure Browser セッションがインターネットにアクセスできない場合は、以下の手順に従って問題を解決してください。

- Secure WorkSpaces Browser ポータルが存在するプライベートサブネットからプロキシエンドポイントにアクセスできることを確認します。これを行うには、プライベートサブネットに EC2 インスタンスを作成し、プライベート EC2 インスタンスからプロキシエンドポイントへの接続をテストします。
- プロキシがインターネットにアクセスできることを確認します。
- Chrome ポリシーが正しいことを確認します。
  - ポリシーの `ProxyServer`フィールドの次の形式を確認します: `<Proxy DNS name>:<Proxy port>`。プレフィックス`https://`に `http://`または を含める必要があります。
  - WorkSpaces Secure Browser セッションで、Chrome を使用して chrome://policy に移動し、ProxySettings ポリシーが正常に適用されていることを確認します。

VPC セットアップの推奨事項

以下の推奨事項は、VPC をより効果的かつ安全に設定するのに役立ちます。

VPC 全体の設定

- VPC 設定が、スケーリングのニーズをサポートできることを確認します。

- WorkSpaces Secure Browser サービスクォータ (制限とも呼ばれます) が、予想される需要をサポートするのに十分であることを確認してください。クォータの引き上げをリクエストするには、https://console.aws.amazon.com/servicequotas/ の [Service Quotas] コンソールを使用します。デフォルトの WorkSpaces Secure Browser クォータについては、「」を参照してくださいthe section called “ポータルのサービスクォータを管理する”。
- ストリーミングセッションにインターネットへのアクセスを提供する場合は、パブリックサブネットに NAT ゲートウェイを持つ VPC を設定することをお勧めします。

弾性ネットワークインターフェース

- 各 WorkSpaces Secure Browser セッションには、ストリーミング期間中に独自の Elastic Network Interface が必要です。 WorkSpaces Secure Browser は、フリートの最大希望容量と同じ数の Elastic Network Interface (ENIsを作成します。デフォルトでは、リージョンごとの ENI の上限は 5000 です。詳細については、「ネットワークインターフェイス」を参照してください。

  何千もの同時ストリーミングセッションなど、非常に大規模なデプロイの容量を計画する場合は、ピーク時の使用量に必要な ENI の数を考慮してください。ENI の上限は、ウェブポータルに設定した同時使用量の上限またはそれ以上に維持することをお勧めします。

サブネット

- ユーザーをスケールアップする計画を立てるときは、Secure Browser WorkSpaces セッションごとに、設定されたサブネットからの一意のクライアント IP アドレスが必要であることに注意してください。したがって、サブネットに設定されるクライアント IP アドレス空間のサイズによって、同時にストリーミングできるユーザーの数が決まります。
- プライベートサブネットに、予想される同時ユーザーの最大数を考慮するのに十分な数のクライアント IP アドレスを許可するサブネットマスクを設定します。また、予想される増加に対応するために、追加される IP アドレスについても考慮しておきます。詳細については、VPC and Subnet Sizing for IPv4 を参照してください。
- 可用性とスケーリングを考慮して、 WorkSpaces Secure Browser が目的のリージョンでサポートする一意のアベイラビリティーゾーンごとにサブネットを設定することをお勧めします。詳細については、「the section called “新しい VPC の作成と設定”」を参照してください。
- ウェブアプリケーションに必要なネットワークリソースが、サブネットを通じてアクセスできることを確認します。

セキュリティグループ

- セキュリティグループを使用して、VPC への追加のアクセスコントロールを提供します。

  VPC に属するセキュリティグループを使用すると、 WorkSpaces Secure Browser ストリーミングインスタンスとウェブアプリケーションに必要なネットワークリソース間のネットワークトラフィックを制御できます。ウェブアプリケーションに必要なネットワークリソースへのアクセスが、セキュリティグループで許可されていることを確認してください。

サポートされているアベイラビリティーゾーン

Secure Browser で使用する Virtual Private Cloud (VPC) を作成する場合、VPC のサブネットは、WorkSpaces Sec WorkSpaces ure Browser を起動するリージョン内の異なるアベイラビリティーゾーンに存在する必要があります。アベイラビリティーゾーンとは、他のアベイラビリティーゾーンで発生した障害から切り離すために作られた場所です。個別のアベイラビリティーゾーンでインスタンスを起動することにより、1 つの場所で発生した障害からアプリケーションを保護できます。各サブネットが完全に 1 つのアベイラビリティーゾーン内に含まれている必要があり、1 つのサブネットが複数のゾーンに、またがることはできません。耐障害性を最大限に高めるため、希望するリージョン内でサポートされている各 AZ にサブネットを設定することをお勧めします。

アベイラビリティーゾーンは、リージョンコードとそれに続く文字識別子によって表されます (us-east-1a など)。リソースがリージョンの複数のアベイラビリティーゾーンに分散されるようにするために、アベイラビリティーゾーンは各 AWS アカウントの名前に個別にマッピングされます。例えば、 AWS アカウントのアベイラビリティーゾーン us-east-1a の場所は、別の AWS アカウントの us-east-1a の場所と異なる可能性があります。

アカウント間でアベイラビリティーゾーンを調整するには、アベイラビリティーゾーンの一意で一貫性のある識別子である AZ ID を使用する必要があります。例えば、 use1-az2はus-east-1リージョンの AZ ID であり、すべての AWS アカウントで同じ場所にあります。

AZ ID を表示すると、あるアカウントのリソースの場所を別のアカウントのリソースに対して決定できます。たとえば、AZ ID use1-az2 のアベイラビリティーゾーンにあるサブネットを別のアカウントと共有する場合、このサブネットは AZ ID が同じく use1-az2 であるアベイラビリティーゾーンのそのアカウントでも利用できます。各 VPC とサブネットの AZ ID は Amazon VPC コンソールに表示されます。

WorkSpaces Secure Browser は、サポートされている各リージョンのアベイラビリティーゾーンのサブセットで使用できます。次の表に、各リージョンで使用できる AZ ID を示します。アカウント内のアベイラビリティーゾーンへの AZ ID のマッピングを確認するには、AWS RAM ユーザーガイドのリソースの AZ ID を参照してください。

リージョン名	リージョンコード	サポートされる AZ ID
米国東部 (バージニア北部)	us-east-1	use1-az1, use1-az2, use1-az4, use1-az5, use1-az6
米国西部 (オレゴン)	us-west-2	usw2-az1, usw2-az2, usw2-az3
アジアパシフィック (ムンバイ)	ap-south-1	aps1-az1, aps1-az3
アジアパシフィック (ソウル)	ap-northeast-2	apne2-az1 , apne2-az2 , apne2-az3
アジアパシフィック (シンガポール)	ap-southeast-1	apse1-az1 , apse1-az2 , apse1-az3
アジアパシフィック (シドニー)	ap-southeast-2	apse2-az1 , apse2-az2 , apse2-az3
アジアパシフィック (東京)	ap-northeast-1	apne1-az1 , apne1-az2 , apne1-az4
カナダ (中部)	ca-central-1	cac1-az1, cac1-az2, cac1-az4
欧州 (フランクフルト)	eu-central-1	euc1-az2, euc1-az2, euc1-az3
欧州 (アイルランド)	eu-west-1	euw1-az1, euw1-az2, euw1-az3
欧州 (ロンドン)	eu-west-2	euw2-az1, euw2-az2

アベイラビリティーゾーンと AZ IDsAmazon EC2 ユーザーガイド」の「リージョン、アベイラビリティーゾーン、ローカルゾーン」を参照してください。

VPC 接続

各 WorkSpaces Secure Browser ストリーミングインスタンスには、VPC 内のリソースへの接続と、NAT ゲートウェイを備えたプライベートサブネットが設定されている場合のインターネットへの接続を提供するカスタマーネットワークインターフェイスがあります。

インターネット接続の場合、すべての接続先に対して次のポートが開いている必要があります。変更された、またはカスタムセキュリティグループを使用している場合、手動で必須ルールを追加する必要があります。詳細については、「セキュリティグループのルール」を参照してください。

> **Note**
>
> これは下りトラフィックにも当てはまります。

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

クライアント/ユーザー接続

WorkSpaces Secure Browser は、ストリーミング接続をパブリックインターネット経由でルーティングするように設定されています。ユーザーを認証し、 WorkSpaces Secure Browser が機能するために必要なウェブアセットを配信するには、インターネット接続が必要です。このトラフィックを許可するには、「許可されたドメイン」に示されたドメインを許可する必要があります。

以下のトピックでは、 WorkSpaces Secure Browser へのユーザー接続を有効にする方法について説明します。

トピック

IP アドレスとポートの要件

WorkSpaces Secure Browser インスタンスにアクセスするには、ユーザーデバイスは次のポートでアウトバウンドアクセスを必要とします。

- ポート 443 (TCP)
  - インターネットエンドポイントを使用している場合、ポート 443 は、ユーザーデバイスとストリーミングインスタンスとの HTTPS 通信に使用されます。通常の場合、ストリーミングセッション中にエンドユーザーがウェブを閲覧すると、ウェブブラウザはストリーミングトラフィックに広範囲のソースポートをランダムに選択します。このポートへのリターントラフィックが許可されていることを確認する必要があります。
  - このポートは、許可されたドメイン に記載されている必要なドメインに開放する必要があります。
  - AWS は、Session Gateway と CloudFront ドメインが解決できる範囲を含む現在の IP アドレス範囲を JSON 形式で公開します。.json ファイルをダウンロードして現在の範囲を表示する方法についての詳細は、「AWS IP アドレスの範囲」を参照してください。または、 を使用している場合は AWS Tools for Windows PowerShell、 Get-AWSPublicIpAddressRange PowerShell コマンドを使用して同じ情報にアクセスできます。Application Auto Scaling ユーザーガイド詳細については、「AWSに対するパブリップ IP アドレス範囲のクエリの実行」を参照してください。
- (オプション) ポート 53 (UDP)
  - ポート 53 は、 ユーザーデバイスと DNS サービス間の通信に使用されます。
  - ドメイン名の解決のために DNS サーバーを使用していない場合、このポートはオプションです。
  - パブリックドメイン名を解決できるように、このポートは DNS サーバーの IP アドレスに対して開いている必要があります。

許可されたドメイン

ユーザーがローカルブラウザからウェブポータルにアクセスできるようにするには、ユーザーがサービスにアクセスしようとしているネットワークの許可リストに次のドメインを追加する必要があります。

次の表で、*{region}* を運用ウェブポータルのリージョンのコードに置き換えます。例えば、欧州 (アイルランド) リージョンのウェブポータルの場合、s3.*{region}*.amazonaws.com は s3.eu-west-1.amazonaws.com である必要があります。リージョンコードのリストについては、「Amazon WorkSpaces Secure Browser エンドポイントとクォータ」を参照してください。

カテゴリ	ドメインまたは IP アドレス
WorkSpaces Secure Browser ストリーミングアセット	s3.*{region}*.amazonaws.com s3.amazonaws.com appstream2.*{region}*.aws.amazon.com *.amazonappstream.com *.shortbread.aws.dev
WorkSpaces セキュアなブラウザの静的アセット	*.workspaces-web.com di5ry4hb4263e.cloudfront.net
WorkSpaces Secure Browser 認証	*.auth.*{region}*.amazoncognito.com cognito-identity.*{region}*.amazonaws.com cognito-idp.*{region}*.amazonaws.com *.cloudfront.net
WorkSpaces Secure Browser のメトリクスとレポート	*.execute-api.{*region*}.amazonaws.com unagi-na.amazon.com

設定した ID プロバイダーに応じて、その他のドメインを許可リストに追加する必要があることもあります。IdP のドキュメントを確認して、 WorkSpaces Secure Browser がそのプロバイダーを使用できるようにリストを許可する必要があるドメインを特定します。IAM Identity Center を使用している場合は、「IAM Identity Center の前提条件」を参照してください。

WorkSpaces Secure Browser の開始方法

Secure Browser WorkSpaces ウェブポータルを作成し、既存のブラウザから内部ウェブサイトと SaaS ウェブサイトへのアクセスをユーザーに許可するには、次の手順に従います。1 つのアカウントで、サポートされている任意のリージョンに 1 つのウェブポータルを作成できます。

> **Note**
>
> 複数のポータルの制限の引き上げをリクエストするには、 AWS アカウント ID、リクエストするポータルの数、および で サポートにお問い合わせください AWS リージョン。

通常、ウェブポータル作成ウィザードではこのプロセスに 5 分かかり、ポータルがアクティブになるまでにさらに 15 分かかります。

ウェブポータルの設定にはコストはかかりません。 WorkSpaces Secure Browser は pay-as-you-go、サービスを積極的に使用するユーザーに対して、月額料金の安さなど、料金を提供します。前払いコスト、ライセンス、または長期間のコミットメントはありません。

> **Important**
>
> 開始する前に、ウェブポータルの必要条件を完了する必要があります。前提条件の詳細については、「WorkSpaces Secure Browser のセットアップ」を参照してください。

トピック

ステップ 1: ウェブポータルを作成する

ウェブ ACL を作成するには、次のステップに従います。

トピック

- ネットワークを設定
- ポータル設定を構成する
- ユーザー設定を構成する
- ID プロバイダーの設定
- 確認して起動

ネットワークを設定

1. https://console.aws.amazon.com/workspaces-web/home で WorkSpaces Secure Browser コンソールを開きます。
2. WorkSpaces Secure Browser を選択し、次に Web ポータル を選択し、次に Create web portal を選択します。
3. [ステップ 1: ネットワーク接続を指定] ページで、次の手順を実行して VPC をウェブポータルに接続し、VPC とサブネットを設定します。

   1. ネットワークの詳細 で、ユーザーが WorkSpaces Secure Browser でアクセスするコンテンツに接続する VPC を選択します。
   2. 次の要件を満たすプライベートサブネットを 3 つまで選択します。詳細については、「ネットワークとアクセス」を参照してください。
      - ポータルを作成するには、少なくとも 2 つのプライベートサブネットを選択する必要があります。
      - ウェブポータルの高可用性を確保するために、VPC の固有のアベイラビリティーゾーンに最大数のプライベートサブネットを提供することをお勧めします。
   3. [セキュリティグループ] をクリックします。

ポータル設定を構成する

[ステップ 2: ウェブポータル設定の構成] ページで、次の手順を実行して、ユーザーがセッションを開始するときのブラウジングエクスペリエンスをカスタマイズします。

1. [ウェブポータルの詳細] の [表示名] に、ウェブポータルの識別可能な名前を入力します。
2. インスタンスタイプ で、ドロップダウンメニューからウェブポータルのインスタンスタイプを選択します。次に、ウェブポータルの最大同時ユーザー制限を入力します。詳細については、「the section called “ポータルのサービスクォータを管理する”」を参照してください。

> **Note**
>
> 新しいインスタンスタイプを選択すると、毎月のアクティブユーザーのコストが変わります。詳細については、「Amazon WorkSpaces Secure Browser の料金」を参照してください。

3. [ユーザーアクセスロギング] の [Kinesis ストリーム ID] で、データの送信先となる Amazon Kinesis Data Streams を選択します。詳細については、「the section called “ユーザーアクセスロギングをセットアップする”」を参照してください。
4. [ポリシー設定] で、以下を完了します。

   - [ポリシーオプション] では、[ビジュアルエディタ] または [JSON ファイルのアップロード] を選択します。どちらの方法でも、ウェブポータルのポリシー設定の詳細を指定できます。詳細については、「the section called “ブラウザポリシーを設定または編集する”」を参照してください。
     - WorkSpaces Secure Browser には、Chrome エンタープライズポリシーのサポートが含まれています。ポリシーは、ビジュアルエディタまたはポリシーファイルの手動アップロードのいずれかで追加または管理できます。いずれかのオプションにいつでも切り替えることができます。
     - ポリシーファイルをアップロードすると、コンソールのファイルに利用可能なポリシーが表示されます。ただし、ビジュアルエディタですべてのポリシーを編集することはできません。コンソールは、[その他の JSON ポリシー] には、ビジュアルエディタでは編集できない JSON ファイル内のポリシーを一覧表示します。これらのポリシーを変更するには、手動で編集する必要があります。
   - (オプション) [スタートアップ URL - オプション] には、ユーザーがブラウザを起動したときにホームページとして使用するドメインを入力します。ご利用の VPC では、この URL との安定した接続が必要です。
   - [プライベートブラウジング] と [履歴の削除] を選択または選択解除して、ユーザーのセッション中にこれらの機能をオンまたはオフにします。

   > **Note**
   >
   > プライベートブラウジング中にアクセスした URL、またはユーザーがブラウザ履歴を削除する前にアクセスした URL は、ユーザーアクセスロギングに記録できません。

詳細については、「the section called “ユーザーアクセスロギングをセットアップする”」を参照してください。

- URL フィルタリング では、セッション中にユーザーがアクセスできる URLsを設定できます。詳細については、「the section called “URL フィルタリングを設定する”」を参照してください。
- (オプション) [ブラウザブックマーク - オプション] では、ユーザーにブラウザに表示させたいブックマークの [表示名]、[ドメイン]、[フォルダ] を入力します。次に、[ブックマークを追加] を選択します。

> **Note**
>
> [ドメイン] はブラウザのブックマークに必須のフィールドです。
> Chrome では、ユーザーはブックマークツールバーの [マネージドブックマーク] フォルダでマネージドブックマークを検索できます。

- (オプション) ポータルにタグを追加します。タグを使用して、 AWS リソースを検索またはフィルタリングできます。タグはキーとオプションの値で構成され、ポータルリソースに関連付けられています。

5. [IP アクセスコントロール (オプション)] で、信頼できるネットワークへのアクセスを制限するかどうかを選択します。詳細については、「the section called “IP アクセスコントロールの設定 (オプション)”」を参照してください。
6. [次へ] を選択して続行します。

ユーザー設定を構成する

[ステップ 3: ユーザー設定を選択] ページで、次の手順を実行して、ユーザーがセッション中に上部のナビゲーションバーからアクセスできる機能を選択し、[次へ] を選択します。

1. [ユーザーのアクセス許可] で、シングルサインオン用の拡張機能を有効にするかどうかを選択します。詳細については、「the section called “シングルサインオンの拡張機能を有効にする (オプション)”」を参照してください。
2. [クリップボードの許可] では、[無効] または [有効] を選択します。
3. [ファイル転送] で [無効] または [有効] を選択します。
4. ユーザーがウェブポータル からローカルデバイスに印刷できるようにする で、許可 または 許可なし を選択します。

5. ウェブポータル へのディープリンクをユーザーに許可 で、許可 または 許可なし を選択します。ディープリンクの詳細については、「」を参照してくださいthe section called “ディープリンクを許可する (オプション)”。
6. [ユーザーセッションの詳細] では、以下を指定します。

   - [Disconnect timeout in minutes (切断タイムアウト (分単位))] では、ユーザーが切断した後にストリーミングセッションをアクティブのままにする時間を選択します。切断、またはこの時間間隔内のネットワークの中断の後、ユーザーが再接続を試みる場合、前のセッションに接続されます。それ以外の場合は、新しいストリーミングインスタンスで新しいセッションに接続されます。

     ユーザーがセッションを終了すると、切断タイムアウトは適用されません。代わりに、ユーザーに対して開いているドキュメントを保存するかどうかの確認が表示され、その後すぐにストリーミングインスタンスから切断されます。ユーザーが使用しているインスタンスは終了されます。
   - [Idle disconnect timeout in minutes (アイドル切断タイムアウト (分単位))] では、ユーザーがストリーミングセッションから切断されるまでにアイドル状態 (非アクティブ) であることができる時間と、[Disconnect timeout in minutes (切断タイムアウト (分単位))] 期間の開始時刻を選択します。ユーザーは、アイドル状態が原因で切断される前に通知されます。ユーザーが [Disconnect timeout in minutes (切断タイムアウト (分単位))] で指定した期間が経過する前にストリーミングセッションへの再接続を試みると、前のセッションに接続されます。それ以外の場合は、新しいストリーミングインスタンスで新しいセッションに接続されます。この値を 0 に設定すると無効になります。この値を無効にした場合、ユーザーはアイドル状態が原因で切断されることはありません。

     > **Note**
     >
     > ユーザーがストリーミングセッション中にキーボードまたはマウスの入力を停止した場合、アイドル状態であると見なされます。ファイルのアップロードとダウンロード、オーディオ入力、オーディオ出力、およびピクセルの変更は、ユーザーアクティビティとはなりません。[Idle disconnect timeout in minutes (アイドル切断タイムアウト (分単位))] の期間が経過した後でも引き続きアイドル状態である場合、ユーザーは切断されます。

ID プロバイダーの設定

ID プロバイダー (IdP) を設定するには、次のステップに従います。

トピック

ID プロバイダーのタイプを選択する

WorkSpaces Secure Browser には、Standard と の 2 つの認証タイプがありますAWS IAM Identity Center。「ID プロバイダーの設定」ページのポータルで使用する認証タイプを選択します。

- Standard (デフォルトオプション) の場合、サードパーティーの SAML 2.0 ID プロバイダー (Okta や Ping など) をポータルと直接フェデレートします。詳細については、「the section called “標準認証タイプを設定する”」を参照してください。標準タイプは、SP 開始認証フローと IdP 開始認証フローの両方をサポートします。
- IAM Identity Center (アドバンストオプション) の場合は、IAM Identity Center をポータルとフェデレーションします。この認証タイプを使用するには、IAM Identity Center と WorkSpaces Secure Browser ポータルの両方が同じ に存在する必要があります AWS リージョン。詳細については、「the section called “IAM Identity Center 認証タイプを設定する”」を参照してください。

標準認証タイプを設定する

Standard (デフォルト) の場合、サードパーティーの SAML 2.0 ID プロバイダー (Okta や Ping など) をポータルと直接フェデレートします。

標準 ID タイプは、SAML 2.0 準拠の IdP を使用した (SP 開始) および identity-provider-initiated (IdP 開始) サインインフローをサポート service-provider-initiatedできます。

ステップ 1: WorkSpaces Secure Browser で ID プロバイダーの設定を開始する

ID プロバイダーを設定するには、次のステップを実行します。

1. 作成ウィザードの [ID プロバイダーを設定] ページで、[スタンダード] を選択します。

2. 「標準 IdP で続行」を選択します。
3. SP メタデータファイルをダウンロードし、個々のメタデータ値のタブを開いたままにします。
   - SP メタデータファイルが利用可能な場合は、メタデータファイルのダウンロードを選択してサービスプロバイダー (SP) メタデータドキュメントをダウンロードし、次のステップでサービスプロバイダーメタデータファイルを IdP にアップロードします。これを行わないと、ユーザーはサインインできなくなります。
   - プロバイダーが SP メタデータファイルをアップロードしない場合は、メタデータ値を手動で入力します。
4. 「SAML サインインタイプを選択」で、SP 開始と IdP 開始の SAML アサーション または SP 開始の SAML アサーションのみ を選択します。
   - SP 開始および IdP 開始の SAML アサーションにより、ポータルは両方のタイプのサインインフローをサポートできます。IdP が開始するフローをサポートするポータルでは、ポータル URL にアクセスしてユーザーがセッションを起動することなく、サービス ID フェデレーションエンドポイントに SAML アサーションを提示できます。
     - これを選択すると、ポータルは未承諾の IdP 開始 SAML アサーションを受け入れることができます。
     - このオプションでは、SAML 2.0 ID プロバイダーでデフォルトのリレーステートを設定する必要があります。ポータルのリレーステートパラメータは、IdP が開始した SAML サインインの下のコンソールにあります。または、 の SP メタデータファイルからコピーできます`<md:IdPInitRelayState>`。
     - 注記
       - リレー状態の形式は次のとおりです: `redirect_uri=https%3A%2F%2Fportal-id.workspaces-web.com%2Fsso&response_type=code&client_id=1example23456789&identity_provider=Example-Identity-Provider`。
       - SP メタデータファイルから値をコピーして貼り付ける場合は、必ず `&` を に変更してください&。 `&`は XML エスケープ文字です。
   - SP 開始のサインインフローのみをサポートするには、ポータルに対してのみ SP 開始の SAML アサーションを選択します。このオプションは、IdP 開始サインインフローからの未承諾 SAML アサーションを拒否します。

> **Note**
>
> 一部のサードパーティー IdPs では、SP 主導のフローを利用して IdP 主導の認証エクスペリエンスを提供できるカスタム SAML アプリケーションを作成できます。例については、「Okta ブックマークアプリケーションを追加する」を参照してください。

5. このプロバイダー への SAML リクエストの署名を有効にするかどうかを選択します。SP 主導認証により、IdP は認証リクエストがポータルから送信されたことを検証できるため、他のサードパーティーリクエストを受け入れることができなくなります。

   a. 署名証明書をダウンロードし、IdP にアップロードします。同じ署名証明書を 1 回のログアウトに使用できます。

   b. IdP で署名付きリクエストを有効にします。名前は、IdP によって異なる場合があります。

   > **Note**
   >
   > RSA-SHA256 は、サポートされている唯一のリクエストおよびデフォルトのリクエスト署名アルゴリズムです。

6. 暗号化された SAML アサーションを要求する を有効にするかどうかを選択します。これにより、IdP から送信される SAML アサーションを暗号化できます。これにより、IdP と WorkSpaces Secure Browser 間の SAML アサーションでデータが傍受されるのを防ぐことができます。

   > **Note**
   >
   > 暗号化証明書は、このステップでは利用できません。ポータルの起動後に作成されます。ポータルを起動したら、暗号化証明書をダウンロードして IdP にアップロードします。次に、IdP でアサーション暗号化を有効にします (名前は IdP によって異なる場合があります。

7. シングルログアウト を有効にするかどうかを選択します。シングルログアウトを使用すると、エンドユーザーは IdP セッションと WorkSpaces Secure Browser セッションの両方を 1 回のアクションでサインアウトできます。

   a. WorkSpaces Secure Browser から署名証明書をダウンロードし、IdP にアップロードします。これは、前のステップでリクエスト署名に使用したものと同じ署名証明書です。

   b. シングルログアウトを使用するには、SAML 2.0 ID プロバイダーでシングルログアウト URL を設定する必要があります。ポータルのシングルログアウト URL は、 コンソールのサービスプ

ロバイダー (SP) の詳細 - 個々のメタデータ値 を表示するか、 の SP メタデータファイルから確認できます<md:SingleLogoutService>。

c. IdP でシングルログアウトを有効にします。名前は、IdP によって異なる場合があります。

ステップ 2: 独自の IdP で ID プロバイダーを設定する

ブラウザで新しいタブが開きます。次に、IdP で以下のステップを実行します。

1. ポータルメタデータを SAML IdP に追加します。

   前のステップでダウンロードした SP メタデータドキュメントを IdP にアップロードするか、メタデータ値をコピーして IdP の正しいフィールドに貼り付けます。一部のプロバイダーはファイルのアップロードを許可していません。

   このプロセスの詳細は、プロバイダーによって異なる場合があります。ポータルの詳細を IdP 設定に追加する方法については、the section called “特定の に関するガイダンス IdPs”「」でプロバイダーのドキュメントを参照してください。

2. SAML アサーションの NameID を確認します。

   SAML IdP が SAML アサーションの NameID にユーザーの E メールフィールドに入力していることを確認します。NameID とユーザー E メールは、ポータルで SAML フェデレーティッドユーザーを一意に識別するために使用されます。永続的な SAML 名 ID 形式を使用します。

3. オプション: IdP 開始認証のリレーステートを設定します。

   前のステップで SP 開始および IdP 開始の SAML アサーションを受け入れるを選択した場合は、のステップ 2 のステップに従って、IdP アプリケーションのデフォルトのリレーステートthe section called “ステップ 1: WorkSpaces Secure Browser で ID プロバイダーの設定を開始する”を設定します。

4. オプション: リクエスト署名を設定します。前のステップでこのプロバイダーへの SAML リクエストに署名を選択した場合は、 のステップ 3 のステップに従って署名証明書を IdP the section called “ステップ 1: WorkSpaces Secure Browser で ID プロバイダーの設定を開始する”にアップロードし、リクエスト署名を有効にします。Okta IdPs などの一部の では、リクエスト署名 を使用するには、NameIDが「永続的」タイプに属する必要がある場合があります。上記の手順に従って、SAML アサーションの NameID を確認してください。

5. オプション: アサーション暗号化 を設定します。このプロバイダー から暗号化された SAML アサーションを要求する を選択した場合は、ポータルの作成が完了するまで待ってから、以下の

「メタデータのアップロード」のステップ 4 に従って暗号化証明書を IdP にアップロードし、アサーション暗号化を有効にします。

6. オプション: シングルログアウト を設定します。シングルログアウト を選択した場合は、 のステップ 5 の手順に従って署名証明書を IdP the section called “ステップ 1: WorkSpaces Secure Browser で ID プロバイダーの設定を開始する”にアップロードし、シングルログアウト URL を入力し、シングルログアウト を有効にします。
7. WorkSpaces Secure Browser を使用するためのアクセスを IdP のユーザーに付与します。
8. IdP からメタデータ交換ファイルをダウンロードします。このメタデータは、次のステップで WorkSpaces Secure Browser にアップロードします。

ステップ 3: Secure Browser での ID WorkSpaces プロバイダーの設定を完了する

WorkSpaces Secure Browser コンソールに戻ります。作成ウィザードの ID プロバイダーの設定ページの IdP メタデータ で、メタデータファイルをアップロードするか、IdP からメタデータ URL を入力します。ポータルは、IdP からのこのメタデータを使用して信頼を確立します。

1. メタデータファイルをアップロードするには、IdP メタデータドキュメント で、ファイルの選択を選択します。前のステップでダウンロードした XML 形式のメタデータファイルを IdP からアップロードします。
2. メタデータ URL を使用するには、前のステップで設定した IdP に移動し、そのメタデータ URL を取得します。 WorkSpaces Secure Browser コンソールに戻り、IdP メタデータ URL の下に、IdP から取得したメタデータ URL を入力します。
3. 終了したら、[Next] (次へ) を選択します。
4. このプロバイダーから暗号化された SAML アサーションを要求するオプションを有効にしたポータルの場合は、ポータル IdP の詳細セクションから暗号化証明書をダウンロードし、IdP にアップロードする必要があります。その後、そこで オプションを有効にできます。

> **Note**
>
> WorkSpaces Secure Browser では、IdP の設定内の SAML アサーションで件名または NameID をマッピングして設定する必要があります。IdP はこれらのマッピングを自動的に作成できます。これらのマッピングが正しく設定されていないと、ユーザーはウェブポータルにサインインしてセッションを開始できません。
> WorkSpaces Secure Browser では、SAML レスポンスに次のクレームが存在する必要があります。コンソールまたは CLI を使用して、ポータルのサービスプロバイダーの詳細ま

たはメタデータドキュメントから <*SP ###### ID*> *###* <*SP ACS URL*> を確認できます。

- SP エンティティ ID をレスポンスのターゲットとして設定するAudience値を持つAudienceRestrictionクレーム。例：

```
<saml:AudienceRestriction>
    <saml:Audience><Your SP Entity ID></saml:Audience>
</saml:AudienceRestriction>
```

- 元の SAML リクエスト ID の値 InResponseTo を含む Response クレーム。例：

```
<samlp:Response ... InResponseTo="<originalSAMLrequestId>">
```

- SP ACS URL Recipientの値と、元の SAML リクエスト ID に一致するInResponseTo値を持つSubjectConfirmationDataクレーム。例：

```
<saml:SubjectConfirmation>
    <saml:SubjectConfirmationData ...
        Recipient="<Your SP ACS URL>"
        InResponseTo="<originalSAMLrequestId>"
        />
</saml:SubjectConfirmation>
```

WorkSpaces Secure Browser は、リクエストパラメータと SAML アサーションを検証します。IdP が開始する SAML アサーションの場合、リクエストの詳細は HTTP POST リクエストの本文でRelayStateパラメータとしてフォーマットする必要があります。リクエスト本文には、SAMLResponseパラメータとして SAML アサーションも含める必要があります。前のステップに従った場合は、これらの両方が存在する必要があります。
以下は、IdP が開始する SAML プロバイダーのPOST本文の例です。

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

特定の に関するガイダンス IdPs

ポータルの SAML フェデレーションを正しく設定するには、一般的に使用される のドキュメントについて、以下のリンクを参照してください IdPs。

IdP	SAML アプリケーションのセットアップ	ユーザー管理	IdP 開始認証	リクエスト署名	アサーション暗号化	シングルログアウト
Okta	SAML アプリケーション統合を作成する	ユーザー管理	Application Integration Wizard SAML フィールドリファレンス	Application Integration Wizard SAML フィールドリファレンス	Application Integration Wizard SAML フィールドリファレンス	Application Integration Wizard SAML フィールドリファレンス
Entra	独自のアプリケーションを作成する	クイックスタート: ユーザーアカウントを作成して割り当てる	エンタープライズアプリケーションのシングルサインオンを有効にする	SAML リクエスト署名の検証	Microsoft Entra SAML トークン暗号化を設定する	シングルサインアウト SAML プロトコル
Ping	SAML アプリケーションを追加する	[ユーザー]	IdP 開始 SSO の有効化	Enterprise PingOne の認証リクエストサインインの設定	PingOne for Enterprise は暗号化をサポートしていますか？	SAML 2.0 シングルログアウト
1 回のログイン	SAML カスタムコネクタ (アドバンスト) (4266907)	ユーザー OneLogin を手動で追加する	SAML カスタムコネクタ (アドバンスト) (4266907)	SAML カスタムコネクタ (アドバンスト) (4266907)	SAML カスタムコネクタ (アドバンスト) (4266907)	SAML カスタムコネクタ (アドバンスト) (4266907)

IdP	SAML アプリケーションのセットアップ	ユーザー管理	IdP 開始認証	リクエスト署名	アサーション暗号化	シングルログアウト
IAM アイデンティティセンター	独自の SAML 2.0 アプリケーションをセットアップする	独自の SAML 2.0 アプリケーションをセットアップする	独自の SAML 2.0 アプリケーションをセットアップする	該当なし	該当なし	該当なし

IAM Identity Center 認証タイプを設定する

IAM Identity Center タイプ (上級) の場合、IAM Identity Center をポータルにフェデレーションします。次の条件が当てはまる場合にのみ、このオプションを選択してください。

- IAM Identity Center は、ウェブポータルと同じ AWS アカウント と AWS リージョン で設定されます。
- を使用している場合は AWS Organizations、管理アカウントを使用します。

IAM Identity Center 認証タイプでウェブポータルを作成する前に、IAM Identity Center をスタンドアロンプロバイダーとして設定する必要があります。詳細については、「IAM Identity Center での一般的なタスクの開始方法」を参照してください。または、SAML 2.0 IdP を IAM Identity Center に接続することもできます。詳細については、「外部 ID プロバイダーに接続する」を参照してください。そうしないと、ウェブポータルに割り当てるユーザーやグループがありません。

既に IAM Identity Center を使用している場合は、プロバイダータイプとして IAM Identity Center を選択し、以下の手順に従ってウェブポータルからユーザーまたはグループを追加、表示、または削除できます。

> **Note**
>
> この認証タイプを使用するには、IAM Identity Center が AWS リージョン WorkSpaces Secure Browser ポータルと同じ AWS アカウント と にある必要があります。IAM Identity Center が別の AWS アカウント または にある場合は AWS リージョン、標準認証タイプの手

順に従ってください。詳細については、「the section called “標準認証タイプを設定する”」を参照してください。
を使用している場合は AWS Organizations、管理アカウントを使用して IAM Identity Center と統合された WorkSpaces Secure Browser ポータルのみを作成できます。

IAM Identity Center でウェブポータルを作成するには

1. ステップ 4: ID プロバイダー を設定するでポータルを作成するときに、 を選択しますAWS IAM Identity Center。
2. 「IAM Identity Center で続行」を選択します。
3. ユーザーとグループの割り当てページで、ユーザーおよび/またはグループタブを選択します。
4. ポータルに追加するユーザー (複数可) またはグループ (複数可) の横にあるチェックボックスをオンにします。
5. ポータルを作成すると、関連付けたユーザーは IAM Identity Center のユーザー名とパスワードを使用して WorkSpaces Secure Browser にサインインできます。

IAM Identity Center でウェブポータルを管理するには

1. ポータルを作成すると、設定されたアプリケーションとして IAM Identity Center コンソールに一覧表示されます。
2. このアプリケーションの設定にアクセスするには、サイドバーで[アプリケーション] を選択し、ウェブポータルの表示名と一致する名前の設定済みアプリケーションを探します。

> **Note**
>
> 表示名を入力していない場合は、代わりにポータルの GUID が表示されます。GUID はウェブポータルのエンドポイント URL にプレフィックスが付く ID です。

既存のウェブポータルにユーザーやグループを追加するには

1. で WorkSpaces Secure Browser コンソールを開きますhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. WorkSpaces Secure Browser 、Web ポータル を選択し、ウェブポータルを選択してから、編集を選択します。

3. [ID プロバイダー設定] と [追加のユーザーとグループを割り当てる] を選択します。ここから、ユーザーやグループをウェブポータルに追加できます。

> **Note**
>
> IAM Identity Center コンソールからユーザーまたはグループを追加することはできません。これは、 WorkSpaces Secure Browser ポータルの編集ページから行う必要があります。

ウェブポータルのユーザーとグループを表示または削除するには

- このアプリケーションへのユーザーアクセスを表示または削除するには、割り当て済みユーザーテーブルで使用可能なアクションを使用します。詳細については、「アプリケーションへのアクセスを管理する」を参照してください。

> **Note**
>
> WorkSpaces Secure Browserportal の編集ページでは、ユーザーとグループを表示または削除することはできません。これは IAM Identity Center コンソールの編集ページから行う必要があります。

ID プロバイダーのタイプを変更する

ポータルの認証タイプをいつでも変更するには、次の手順に従います。

- IAM Identity Center から標準 に変更するには、「」のステップに従いますthe section called “標準認証タイプを設定する”。
- Standard から IAM Identity Center に変更するには、「」のステップに従いますthe section called “IAM Identity Center 認証タイプを設定する”。

ID プロバイダータイプの変更はデプロイに最大 15 分かかる場合があり、進行中のセッションは自動的に終了しません。

`UpdatePortal` イベントを調べる AWS CloudTrail ことで、 を通じてポータルへの ID プロバイダータイプの変更を表示できます。タイプは、イベントのリクエストペイロードとレスポンスペイロードに表示されます。

確認して起動

1. [ステップ 5: 確認して起動] ページで、ウェブポータル用に選択した設定を確認します。[編集] を選択して、特定のセクション内の設定を変更できます。これらの設定は、コンソールの [ウェブポータル] タブから後で変更することもできます。
2. 完了したら、[ウェブポータルを起動] を選択します。
3. ウェブポータルのステータスを表示するには、[ウェブポータル] を選択し、ポータルを選択して [詳細を表示] を選択します。

   ウェブポータルのステータスは、次のいずれかです。

   - [不完全] - ウェブポータルの構成に必要な ID プロバイダー設定がありません。
   - [保留中] - ウェブポータルは設定に変更を適用しています。
   - [アクティブ] - ウェブポータルは準備が整い、使用可能です。
4. ポータルがアクティブになるまで最大 15 分待ってください。

ステップ 2: ウェブポータルをテストする

ウェブポータルを作成したら、Secure Browser WorkSpaces エンドポイントにサインインして、エンドユーザーと同じように接続されたウェブサイトを参照できます。

the section called “ID プロバイダーの設定” でこれらのステップをしでに完了している場合は、このセクションをスキップして ステップ 3: ウェブポータルを配信する に進んでください。

1. https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/ で WorkSpaces Secure Browser コンソールを開きます。
2. WorkSpaces Secure Browser 、Web ポータル を選択し、ウェブポータルを選択してから、詳細の表示 を選択します。
3. [ウェブポータルエンドポイント] で、ポータルの指定した URL に移動します。ウェブポータルエンドポイントは、ポータルに設定されている ID プロバイダーを使用してユーザーがサインインした後にウェブポータルを起動するアクセスポイントです。インターネット上で公開されており、ネットワークに埋め込むことができます。
4. WorkSpaces Secure Browser のサインインページで、「サインイン」、「SAML」を選択し、「SAML 認証情報」を入力します。
5. セッションの準備中ページが表示されると、 WorkSpaces Secure Browser セッションが起動します。このページを閉じたり、終了しないでください。

6. ウェブブラウザが起動し、スタートアップ URL と、ブラウザのポリシー設定で設定したその他の動作が表示されます。
7. これで、リンクを選択するか、またはアドレスバーに URL を入力して、接続されているウェブサイトを参照できるようになりました。

ステップ 3: ウェブポータルを配信する

ユーザーが WorkSpaces Secure Browser の使用を開始する準備ができたら、次のオプションから選択してポータルを配布します。

- ポータルを SAML アプリケーションゲートウェイに追加して、ユーザーが IdP から直接セッションを起動できるようにします。これを行うには、SAML 2.0 準拠の IdP で IdP 開始のサインインフローを使用します。詳細については、「」の「SP 開始および IdP 開始の SAML アサーション」を参照してくださいthe section called “標準認証タイプを設定する”。または、SP 開始フローを使用して IdP 開始認証エクスペリエンスを配信できるカスタム SAML アプリケーションを作成することもできます。詳細については、「ブックマークアプリケーション統合の作成」を参照してください。
- 所有しているウェブサイトにポータル URL を追加し、ブラウザリダイレクトを使用してユーザーをそのウェブポータルに誘導します。
- ポータル URL をユーザーに E メールで送信するか、ブラウザのホームページまたはブックマークとして管理しているデバイスにプッシュします。

次のステップ

最初のウェブポータルを作成すると、詳細の表示、詳細の編集、またはウェブポータルの削除をいつでも行うことができます。詳細については、「ウェブポータルの管理」を参照してください。

AWS アカウント は、 WorkSpaces Secure Browser AWS リージョン が利用可能な各 にウェブポータルを作成できます。各ウェブポータルは、いつでも最大 25 のユーザー接続をサポートできます。1 つのリージョンで作成できるポータル数を増やすことや、1 つのポータルでより多くの同時セッションをサポートする方法については、「the section called “ポータルのサービスクォータを管理する”」を参照してください。

ウェブポータルの管理

ウェブポータルを設定すると、詳細を表示または編集できるほか、不要になったポータルを削除できます。

トピック

ウェブポータルの詳細を表示する

ウェブポータルの詳細を表示する

1. で WorkSpaces Secure Browser コンソールを開きますhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. WorkSpaces Secure Browser 、Web ポータル を選択し、ウェブポータルを選択してから、詳細の表示 を選択します。

ウェブポータルを編集する

ウェブポータルを編集するには

1. で WorkSpaces Secure Browser コンソールを開きますhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. WorkSpaces Secure Browser 、Web ポータル を選択し、ウェブポータルを選択してから、編集を選択します。

> **Note**
>
> ネットワーク設定またはタイムアウト設定を変更すると、アクティブなすべてのポータルセッションが直ちに終了します。ユーザーは切断され、新しいセッションを開始するには再接続する必要があります。[クリップボードの許可]、[ファイル転送の許可]、または [ローカルデバイスに出力] は、最初の新しいセッションから適用されます。現在アクティブなセッションは切断されません。アクティブなセッションに接続しているユーザーは、接続を切断して新しいセッションに接続するまで変更の影響を受けません。

ウェブポータルを削除する

ウェブポータルを削除するには

1. で WorkSpaces Secure Browser コンソールを開きますhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. WorkSpaces Secure Browser 、Web ポータル を選択し、ウェブポータルを選択し、Delete を選択します。

ポータルのサービスクォータを管理する

を作成すると AWS アカウント、 でのリソース使用量のデフォルトのサービスクォータ (制限とも呼ばれます) が自動的に設定されます AWS サービス。管理者は、ユースケースをサポートするために引き上げる必要がある 2 つのクォータを認識する必要があります。これら 2 つのクォータは、各リージョンで作成できるウェブポータルの数と、各リージョンで使用可能な各インスタンスタイプでサポートできる最大同時セッション数です。これらの引き上げは、 AWS コンソールの Service Quotas ページからリクエストできます。

次の表に、デフォルトのサービスクォータ制限を示します。

アカウント AWS リージョン 別の 内のデフォルトのクォータ	値
ウェブポータル	3
最大同時セッション数 - standard.regular	25
最大同時セッション数 - standard.large	10
最大同時セッション数 - standard.xlarge	5

> **Important**
>
> サービスクォータは、一度に 1 AWS リージョン つに影響します。より多くのリソースが必要な各 で、サービスクォータの引き上げ AWS リージョン をリクエストする必要があります。詳細については、Amazon WorkSpaces Secure Browser エンドポイントとクォータ を参照してください。

サービスクォータ引き上げをリクエストするには

1. [AWS サポートダッシュボード] を開きます。
2. [サービス制限の引き上げ] を選択します。

   > **Important**
   >
   > WorkSpaces Secure Browser サービスクォータは、一度に 1 つのリージョンに影響します。より多くのリソースを必要とする各 AWS リージョンに対して、サービスクォータの引き上げをリクエストする必要があります。詳細については、「AWS のサービスエンドポイント」を参照してください。

3. [ユースケースの説明] で、以下の情報を入力します。

   - ウェブポータル数の引き上げをリクエストする場合は、このリソースタイプを指定し、AWS アカウント ID、引き上げたいリージョン、新しい制限値を含めます。
   - 同時セッション数の引き上げをリクエストする場合は、このリソースタイプを指定し、AWS アカウント ID、引き上げたいリージョン、ウェブポータル ARN、新しい制限値を含めます。

4. (オプション) 複数のサービスクォータの引き上げを同時にリクエストするには、[リクエスト] セクションで 1 つのクォータの引き上げリクエストを完了し、[別のリクエストを追加] を選択します。

ポータルの引き上げをリクエストする

ポータルは、サービスの基盤となるリソースです。各ポータルは、SAML 2.0 ID プロバイダーと、インターネットおよびプライベートウェブコンテンツへのネットワーク接続との関連付けです。各ポータルには個別のポータルブラウザポリシーとユーザー設定を含めることができるため、管理者は通常、異なるユースケースに対応するために同じリージョンに複数のポータルを作成します。例えば、制限ポリシー (クリップボードやファイル転送が無効など) を持つ特定のウェブサイトへのアクセスをグループ A に許可し、URL フィルタリングなしで一般的なインターネットへのアクセスをグループ B に許可できます。サポートされている任意の にポータルを作成できます AWS リージョン。現在のサービスの可用性を確認するには、「リージョン別の AWS のサービス」を参照してください。

サービスクォータ引き上げをリクエストするには

1. 目的のリージョンで Service Quotas ページを開きます。
2. ウェブポータルの数 を選択します。
3. アカウントレベルで引き上げをリクエスト を選択します。
4. クォータ値を増やす に、クォータにする合計量を入力します。

同時セッションの最大増加をリクエストする

同時セッションの最大クォータは、ポータルに同時に接続できるユーザーの最大数です。同時セッションの最大数に対するサービスクォータ制限が適切に設定されていない場合、ユーザーはサインイン時にセッションが利用できないことがあります。このサービスクォータを増やすことに加えて、VPC とサブネットに最大同時セッションをサポートするのに十分な IP スペースがあることも確認する必要があります。

同時セッションの最大増加をリクエストするには

1. 目的のリージョンで Service Quotas ページを開きます。
2. 増やすインスタンスタイプのポータルあたりの最大同時セッション数を選択します。
3. アカウントレベルで引き上げをリクエスト を選択します。
4. クォータ値の増加 に、クォータにする合計量を入力します。

> **Note**
>
> 大規模または緊急の増加については、Service Quotas の履歴ページに移動し、リクエストのステータス列のリンクを選択し、サポートケースにリンクして、ユースケースや緊急性に関する詳細を含む返信を追加します。この情報は、サービスチームがリクエストに優先順位を付け、アカウントに十分な容量が割り当てられるようにするのに役立ちます。

制限の例

例えば、管理者が米国東部 (バージニア北部) で 2 つのウェブポータルを合計 125 人のユーザー用に設定しているとします。ウェブポータルを作成する前に、管理者は最初のウェブポータル (ポータル A) が 100 ユーザーをサポートすることを確認します。これらのユーザーのワークフローをテストする場合、管理者はセッション中にオーディオとビデオのストリーミングをサポートするために XL インスタンスタイプが必要であると判断します。2 つ目のウェブポータル (ポータル B) は、お客様の VPC でホストされている 1 つの静的ウェブページへのアクセスをサポートするために、最大 25 人のユーザーが利用できる必要があります。このユースケースをテストする場合、管理者は標準インスタンスタイプがこのユースケースをサポートできると判断します。

ポータル A の場合、管理者はサービスクォータ引き上げリクエストを送信して、XL インスタンスの制限をリージョンのデフォルト (5) から 100 に引き上げる必要があります。処理が完了すると、管理者はウェブポータルを編集して容量を割り当てることができます。ポータル B の場合、管理者はクォータの引き上げをリクエストせずに先に進むことができます (つまり、リージョンの標準インスタンスタイプのデフォルトクォータは 25 であるため) 。

サービスクォータの管理

各リージョンのアカウントに割り当てられたサービスクォータをいつでも表示するには、Service Quotas」ページを参照してください。

その他のサービスクォータ

Service Quotas ページ に記載されている他のクォータの引き上げを表示およびリクエストできます。実際には、ほとんどのお客様は、これらの制限の引き上げをリクエストする必要はありません。これらのクォータは、数値 とレート の 2 つのタイプに大別されます。

数値クォータの場合、ウェブポータルの数のサービスクォータの引き上げを送信すると、一意のポータルの作成に必要なサブリソースの数が自動的に増加します。これは Service Service Quotas ページに反映されます。例えば、ポータルの 3 から 5 への引き上げをリクエストすると、ブラウザとユーザー設定の両方でサービスクォータが 3 から 5 に自動的に引き上げられます。必要に応じて、新しいサブリソースを再利用または作成できます。

まれに、他のリソースクォータの数や割合を増やすユースケースが見つかることがあります。例えば、管理者は追加のポータル設定をテストするためにブラウザ設定の数を増やすことができます。これらのサービスクォータリクエストは、 case-by-case ベースでレビューおよび受理されます。

Rate クォータの場合、アカウントポータルの制限に関係なく、Service Quotas で公開されるレート制限を調整する必要はありません。

SAML IdP トークンの再認証間隔の制御

ユーザーが WorkSpaces Secure Browser ポータルにアクセスすると、サインインしてストリーミングセッションを開始できます。5 分以内にサインインしないと、すべてのセッションはスタートページから開始します。ポータルは ID プロバイダー (IdP) トークンを確認して、セッションの開始時にユーザーに認証情報の入力を求めるかどうかを決定します。有効な IdP トークンを持たないユーザーは、ストリーミングセッションを開始するために、ユーザー名、パスワード (オプションで多要素認証 (MFA)) を入力する必要があります。ユーザーが IdP または同じ IdP で保護されているアプリにサインインして SAML IdP トークンをすでに生成している場合、サインイン認証情報の入力は求められません。

ユーザーが有効な SAML IdP トークンを持っている場合は、 WorkSpaces Secure Browser にアクセスできます。SAML IdP トークンの再認証間隔を制御することができます。

SAML IdP トークンの再認証間隔を制御するには

1. SAML IdP プロバイダーで IdP タイムアウト時間を設定します。IdP のタイムアウト期間は、ユーザーがタスクを完了するのに必要な最短時間に設定することをお勧めします。

   - Okta の詳細については、「すべてのポリシーに制限付きセッションの有効期限を適用する」を参照してください。
   - Azure AD の詳細については、「認証セッション制御の設定」を参照してください。
   - Ping の詳細については、「セッション」を参照してください。
   - の詳細については AWS IAM Identity Center、「セッション期間の設定」を参照してください。

2. WorkSpaces Secure Browser ポータルの非アクティブおよびアイドルタイムアウト値を設定します。これらの値は、ユーザーの最後の操作から、Secure Browser WorkSpaces セッションが非アクティブにより終了するまでの時間を制御します。セッションが終了すると、ユーザーはセッション状態 (開いているタブ、保存されていないウェブコンテンツ、履歴を含む) を失い、次のセッションの開始時に新しい状態に戻ります。詳細については、「the section called “ステップ 1: ウェブポータルを作成する”」のステップ 5 を参照してください。

> **Note**
>
> ユーザーのセッションがタイムアウトしても、ユーザーが有効な SAML IdP トークンを持っている場合は、新しい WorkSpaces Secure Browser セッションを開始するためにユーザー名とパスワードを入力する必要はありません。トークンの再認証方法を制御するには、前のステップのガイドに従ってください。

ユーザーアクセスロギングをセットアップする

ユーザーイベントを記録するユーザーアクセスロギングを設定します

- セッション開始 - WorkSpaces Secure Browser セッションの開始をマークします。
- セッション終了 - WorkSpaces Secure Browser セッションの終了をマークします。
- URL ナビゲーション - ユーザーが読み込んだ URL を記録します。

> **Note**
>
> URL ナビゲーションログはブラウザ履歴から記録されます。ブラウザ履歴に記録されていない (シークレットモードでアクセスした、またはブラウザ履歴から削除された) URL はログに記録されません。ブラウザポリシーでシークレットモードまたは履歴の削除をオフにするかは、カスタマーの判断に委ねられます。

さらに、各イベントには次の情報が含まれます。

- イベント時間
- ユーザーネーム
- ウェブポータル ARN

お客様は、 WorkSpaces Secure Browser の使用に伴って発生する可能性のある法的問題を理解し、Secure Browser WorkSpaces の使用がすべての適用可能な法律および規制に準拠していることを確認する責任があります。これには、アプリケーション内で実行されるアクティビティなど、従業員による WorkSpaces Secure Browser の使用を監視する雇用主の能力を規制する法律が含まれます。

WorkSpaces Secure Browser ポータルでユーザーアクセスログをアクティブ化すると、Amazon Kinesis Data Streams から料金が発生する可能性があります。料金の詳細については、「Amazon Kinesis Data Streams の料金」を参照してください。

WorkSpaces Secure Browser コンソールでユーザーアクセスログを有効にするには、ユーザーアクセスログ で、データを受信するために使用する Kinesis Stream ID を選択します。記録されたデータはそのストリームに直接配信されます。

Amazon Kinesis Data Streams を作成する方法の詳細については、「Amazon Kinesis Data Streams とは」を参照してください。

> **Note**
>
> WorkSpaces Secure Browser からログを受信するには、amazon-workspaces-web「-*」で始まる Amazon Kinesis Data Streams が必要です。Amazon Kinesis データストリームでは、サーバー側の暗号化がオフになっているか、サーバー側の暗号化 AWS マネージドキー に を使用する必要があります。
> Amazon Kinesis でサーバー側の暗号化を有効にする方法については、「サーバー側の暗号化を使用開始する方法」を参照してください。

サンプルログ

以下は、検証 、、、 などStartSession、使用可能な各イベントの例ですVisitPageEndSession。

各イベントには常に以下のフィールドが含まれます。

- timestamp はエポックタイムとしてミリ秒単位で含まれます。
- eventType は文字列として含まれます。
- details は別の JSON オブジェクトとして含まれます。
- PortalArn と userName は、Validation を除くすべてのイベントに含まれています。

```
{
  "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"
}
```

ブラウザポリシーを設定または編集する

WorkSpaces Secure Browser を使用すると、最新の安定バージョンで利用可能な Chrome ポリシーを使用してカスタムブラウザポリシーを設定できます。1 つのウェブポータルに適用できるポリシー

は 300 種類以上あります。詳しくは the section called “カスタムブラウザポリシーの設定 (例)” および Chrome エンタープライズポリシーリストをご覧ください。

コンソールビューを使用してウェブポータルを作成することで、次のポリシーを適用できます。

- StartURL
- ブックマークとブックマークフォルダー
- プライベートブラウジングのオンとオフの切り替え
- 履歴の削除
- AllowURL および BlockURL を使用した URL フィルタリング

コンソールビューポリシーの使用に関する詳細については、「WorkSpaces Secure Browser の開始方法」を参照してください。

WorkSpaces Secure Browser は、指定したポリシーとともに、すべてのポータルにベースラインブラウザポリシー設定を適用します。これらのポリシーの一部はカスタム JSON ファイルを使用して編集できます。詳細については、「the section called “ベースラインブラウザポリシーを編集します。”」を参照してください。

トピック

- カスタムブラウザポリシーの設定 (例)
- ベースラインブラウザポリシーを編集します。

カスタムブラウザポリシーの設定 (例)

JSON ファイルをアップロードすることで、サポートされている Linux 用の Chrome ポリシーをすべて設定できます。Chrome ポリシーについて詳しくは、「Chrome エンタープライズポリシーリスト」を参照して Linux プラットフォームを選択してください。次に、最新の安定したバージョンに関するポリシーを検索して確認します。

次の例では、以下のポリシーコントロールを含むウェブポータルを作成します。

- ブックマークをセットアップする
- 既定のスタートアップページをセットアップする
- ユーザーが他の拡張機能をインストールできないようにする
- ユーザーが履歴を削除できないようにする

- ユーザーがシークレットモードにアクセスできないようにする
- Okta プラグイン拡張機能をすべてのセッションにプレインストールする

トピック

ステップ 1: ウェブポータルを作成する

Chrome ポリシー JSON ファイルをアップロードするには、 WorkSpaces Secure Browser ポータルを作成する必要があります。詳細については、「the section called “ステップ 1: ウェブポータルを作成する”」を参照してください。

ステップ 2: ポリシーを収集する

Chrome ポリシーから必要なポリシーを検索して特定します。次に、ポリシーを使用して、次のステップで JSON ファイルを作成します。

1. [Chrome エンタープライズポリシーリスト] に移動します。
2. プラットフォーム Linux を選択し、Chrome の最新バージョンを選択します。
3. 設定するポリシーを検索します。この例では、拡張機能を検索して、それらを管理するためのポリシーを見つけてます。各ポリシーには、説明、Linux 設定名、サンプル値が含まれています。
4. 検索結果から、一緒に使用するとビジネス要件を満たす 3 つのポリシーが見つかりました。
   - ExtensionSettings – ブラウザの起動時に拡張機能をインストールします。
   - ExtensionInstallBlocklist – 特定の拡張機能がインストールされないようにします。
   - ExtensionInstallAllowlist – 特定の拡張機能のインストールを許可します。
5. その他のポリシーでも残りの要件を満たします。
   - ManagedBookmarks – ウェブページにブックマークを追加します。
   - RestoreOnStartupURLs- 新しいブラウザウィンドウが起動されるたびに開くウェブページを設定します。
   - AllowDeletingBrowserHistory – ユーザーが閲覧履歴を削除できるかどうかを設定します。

- IncognitoModeAvailability – ユーザーがシークレットモードで にアクセスできるかどうかを設定します。

ステップ 3: カスタム JSON ポリシーファイルを作成する

テキストエディタ、テンプレート、および前の手順で見つけたポリシーを使用して、JSON ファイルを作成します。

1. テキストエディタを開きます。
2. 次のテキストをコピーし、テキストエディタに貼り付けます。

```
{
  "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
        }
    }
}
```

ステップ 4: ポリシーをテンプレートに追加する

ビジネス要件ごとにカスタムポリシーをテンプレートに追加します。

1. ブックマーク URL を設定します。
   a. `value` キーの下に、追加するブックマークごとに`name` と `url` キーのペアを追加します。
   b. `bookmark-url-1` を `https://www.amazon.com` に設定します。

c. bookmark-url-2 を https://docs.aws.amazon.com/workspaces-web/latest/adminguide/ に設定します。

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

2. スタートアップ URL をセットアップします。このポリシーにより、管理者はユーザーが新しいブラウザウィンドウを起動したときに表示されるウェブページを設定できます。

   a. RestoreOnStartup を 4 に設定します。これにより、URL RestoreOnStartup のリストを開くアクションが設定されます。スタートアップ URL でその他のアクションを使用することもできます。詳しくは Chrome エンタープライズポリシーリストをご覧ください。

   b. RestoreOnStartupURLs を https://www.aboutamazon.com/news に設定します。

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

3. ユーザーがブラウザの履歴を削除できないようにするには、AllowDeletingBrowserHistory を false に設定します。

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

4. ユーザーがシークレットモードにアクセスできないようにするには、IncognitoModeAvailability を 1 に設定します。

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

5. Okta プラグインを以下のポリシーで設定して適用します。

   - ExtensionSettings - ブラウザの起動時に拡張機能をインストールします。拡張機能の値は Okta プラグインのヘルプページから確認できます。
   - ExtensionInstallBlocklist – 特定の拡張機能がインストールされないようにします。* 値を指定すると、すべての拡張機能がデフォルトで禁止されます。管理者はどの拡張機能を ExtensionInstallAllowlist で許可するかを制御できます。
   - ExtensionInstallAllowlist は特定の拡張機能のインストールを許可します。ExtensionInstallBlocklist が * に設定されているので、これを許可するには Okta プラグインの値をここに追加します。

   Okta プラグインを有効にするポリシーの例を以下に示します。

```
"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"
            }
        }
```

ステップ 5: ポリシー JSON ファイルをウェブポータルにアップロードします。

1. で WorkSpaces Secure Browser コンソールを開きますhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. WorkSpaces Secure Browser を選択し、Web ポータル を選択します。
3. ウェブポータルを選択し、[編集] を選択します。
4. [ポリシー設定] を選択し、[JSON ファイルのアップロード] を選択します。
5. [ファイルの選択] を選択します。JSON ファイルに移動し、選択してアップロードします。
6. [保存] を選択します。

ベースラインブラウザポリシーを編集します。

サービスを配信するために、 WorkSpaces Secure Browser はすべてのポータルにベースラインブラウザポリシーを適用します。このベースラインポリシーは、コンソールビューまたは JSON アップロードから指定したポリシーに加えて適用されます。以下は、JSON 形式でサービスによって適用されるポリシーのリストです。

```
{
    "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",
            ]
        }
    }
}
```

カスタマーは以下のポリシーを変更できません。

- DefaultDownloadDirectory – このポリシーは編集できません。このポリシーへの変更はすべてサービスによって上書きされます。
- DownloadDirectory – このポリシーは編集できません。このポリシーへの変更はすべてサービスによって上書きされます。

カスタマーはウェブポータルの以下のポリシーを更新できます。

- DownloadRestrictions – デフォルトでは、Chrome セーフブラウジングによって悪質と判定されたダウンロードを防ぐように 1 に設定されています。詳しくは、「ユーザーによる有害なファイルのダウンロードを防止する」を参照してください。値は 0 から 4 に設定できます。
- URLAllowlist および URLBlocklist ポリシーは、コンソールビューの URL フィルタリング機能または JSON アップロードを使用して拡張できます。ただし、ベースライン URL は上書きできません。これらのポリシーは、ウェブポータルからダウンロードした JSON ファイルからは見えません。ただし、セッション中に「chrome: //policy」にアクセスすると、リモートブラウザには適用されたポリシーが表示されます。

Input Method Editor (IME) を設定します。

Input Method Editor (IME) は、QWERTY キーボード以外のキーボードレイアウトを使用する言語でテキストを入力するためのオプションをエンドユーザーに提供するユーティリティです。IME は、日本語、中国語、韓国語など、大きく複雑な言語セットを有する言語でテキストを入力するのに役立ちます。 WorkSpaces セキュアブラウザセッションには、デフォルトで IME サポートが含まれています。ユーザーは、セッション内の IME ツールバーから、またはキーボードショートカットを使用して代替言語を選択できます。

現在、 WorkSpaces Secure Browser の IME では以下の言語がサポートされています。

- 英語
- 簡体字中国語 (Pinyin)
- 繁体字中国語 (Bopomofo)
- 日本語
- 韓国語

IME ツールバーから言語を選択するには、次を行います。

1. 上部の黒いパネルバーの右側にある言語セレクタードロップダウンを選択します。デフォルトでは、セレクターには英語、en が表示されます。
2. ドロップダウンメニューで、目的の言語を選択します。
3. 言語を選択すると表示されるサブメニューで、その他の言語の詳細を選択します。

キーボードショートカットを使用して言語を選択するには、以下を使用します。

- すべての IME
  - IME を順方向に切り替える (または右側のキーボードレイアウトに移動する) には、Shift+Control+Left Alt を押します。
- 日本語
  - ひらがなを選択するには、F6 を押します。
  - カタカナを選択するには、F7 を押します。
  - ラテンを選択するには、F10 を押します。
  - ワイドラテンを選択するには、F9 を押します。
  - ダイレクト入力を選択するには、ALT +、ALT+@、全角半角キーを押します。

- 韓国語
  - ハングルを選択するには、Shift+Space を押します。
  - 漢字を選択するには、F9 を押します。

IME ツールバーとメニューを削除するか、 WorkSpaces Secure Browser セッションから画面上のキーボードをオフにするには、 にお問い合わせください AWS Support。

セッション内ローカリゼーションを設定する

ユーザーがセッションを開始すると、 WorkSpaces Secure Browser はユーザーのローカルブラウザ言語とタイムゾーンの設定を検出し、セッションに適用します。これはセッション中の表示言語に影響し、表示される時刻がユーザーの所在地の現在時刻と一致していることを確認するのに役立ちます。

次のリストは、 WorkSpaces Secure Browser で現在サポートされている言語コードを示しています。ユーザーのローカルブラウザがサポートされていない言語コードを使用するように設定されている場合、セッションはデフォルトで英語 (en-US) になります。

- ドイツ語
  - de – ドイツ語
  - de-AT – ドイツ語 (オーストリア)
  - de-DE – ドイツ語 (ドイツ)
  - de-CH – ドイツ語 (スイス)
  - de-LI – ドイツ語 (リヒテンシュタイン)
- 英語
  - en – 英語
  - en-AU – 英語 (オーストラリア)
  - en-CA – 英語 (カナダ)
  - en-IN – 英語 (インド)
  - en-NZ – 英語 (ニュージーランド)
  - en-ZA – 英語 (南アフリカ)
  - en-GB – 英語 (英国)
  - en-US – 英語 (米国)
- スペイン語

  - es – スペイン語
  - es-AR – スペイン語 (アルゼンチン)
  - es-CL – スペイン語 (チリ)
  - es-CO – スペイン語 (コロンビア)
  - es-CR – スペイン語 (コスタリカ)
  - es-HN – スペイン語 (ホンジュラス)
  - es-419 – スペイン語 (ラテンアメリカ)
  - es-MX – スペイン語 (メキシコ)
  - es-PE – スペイン語 (ペルー)
  - es-ES – スペイン語 (スペイン)
  - es-US – スペイン語 (米国)
  - es-UY – スペイン語 (ウルグアイ)
  - es-VE – スペイン語 (ベネズエラ)
- フランス語
  - fr – フランス語
  - fr-CA – フランス語 (カナダ)
  - fr-FR – フランス語 (フランス)
  - fr-CH – フランス語 (スイス)
- インドネシア語
  - id – インドネシア語
  - id-ID – インドネシア語 (インドネシア)
- イタリア語
  - it – イタリア語
  - it-IT – イタリア語 (イタリア)
  - it-CH – イタリア語 (スイス)
- 日本語
  - ja – 日本語
  - ja-JP – 日本語 (日本)
- 韓国語
  - ko – 韓国語

  - ko-KR – 韓国語 (韓国)
- ポルトガル語
  - pt – ポルトガル語
  - pt-BR – ポルトガル語 (ブラジル)
  - pt-PT – ポルトガル語 (ポルトガル)
- 中国語
  - zh – 中国語
  - zh-CN – 中国語 (中国)
  - zh-HK – 中国語 (香港)
  - zh-TW – 中国語 (台湾)

セッション言語は以下の優先順位で決定されます。

1. ウェブポータルのブラウザ設定のForcedLanguagesポリシー。詳細については、「」を参照してくださいForcedLanguages。
2. エンドユーザーのローカルブラウザ言語設定。
3. デフォルト値は、英語 (en-US) です。

タイムゾーンは、エンドユーザーのブラウザで指定されたローカルタイムゾーン設定によって決まります。タイムゾーン設定が有効でない場合は、UTC が使用されます。

WorkSpaces Secure Browser の以下のコンポーネントはローカリゼーションをサポートしています。

- WorkSpaces Secure Browser のサインインページ
- WorkSpaces Secure Browser ポータルのステータスメッセージ (メッセージやエラーのロードを含む)
- Chrome ブラウザ
- システムの[コンテキスト] メニューと [名前を付けて保存] ウィンドウ

ユーザーのローカルブラウザ設定を設定するには、以下のいずれかを実行します。

- Chrome では、[設定] を選択し、[言語] を選択して、好みに応じて言語を並べ替えます。
- Firefox では、[設定]、[一般]、[言語] を選択し、ドロップダウンメニューから言語を選択します。

- Edge では、[設定]、[言語] を選択し、好みに応じて言語を並べ替えます。

IP アクセスコントロールの設定 (オプション)

WorkSpaces Secure Browser を使用すると、ウェブポータルにアクセスできる IP アドレスを制御できます。IP アドレス設定を使用すると、信頼できる IP アドレスのグループを定義および管理し、信頼できるネットワークに接続しているときにだけポータルにアクセスできるようにすることができます。

デフォルトでは、 WorkSpaces Secure Browser により、ユーザーはどこからでもウェブポータルにアクセスできます。IP アクセスコントロールグループは、ウェブポータルへの接続に使用できる IP アドレスをフィルタリングする仮想ファイアウォールとして機能します。IP アクセス設定をウェブポータルに関連付けると、認証前にユーザー IP を検出して、そのユーザーが接続できるかどうかを判断します。接続後、 WorkSpaces Secure Browser はユーザーの IP アドレスを継続的にモニタリングして、信頼できるネットワークから接続されたままであることを確認します。ユーザーの IP が変更されると、 WorkSpaces Secure Browser はセッションを検出して終了します。

CIDR アドレス範囲を指定するには、IP アクセスコントロールグループにルールを追加し、グループをウェブポータルに関連付けます。各 IP アクセス設定は、1 つ以上のウェブポータルに関連付けることができます。信頼できるネットワークのパブリック IP アドレスと IP アドレスの範囲を指定するには、IP アクセスコントロールグループにルールを追加します。ユーザーが NAT ゲートウェイまたは VPN 経由でウェブポータルにアクセスする場合は、NAT ゲートウェイまたは VPN のパブリック IP アドレスからのトラフィックを許可するルールを作成する必要があります。

> **Note**
>
> お客様は、 WorkSpaces Secure Browser の使用に伴って発生する可能性のある法的問題を理解し、Secure Browser WorkSpaces の使用がすべての適用可能な法律および規制に準拠していることを確認する必要があります。これには、アプリケーション内で実行されるアクティビティなど、従業員による WorkSpaces Secure Browser の使用を監視する雇用主の能力を規制する法律が含まれます。

IP アクセスコントロールグループを作成する

IP アクセスコントロールグループを作成するには、以下の手順に従います。

1. で WorkSpaces Secure Browser コンソールを開きますhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. ナビゲーションペインで [IP アクセスコントロール] を選択します。
3. [IP アクセスコントロールグループを作成] を選択します。
4. [IP アクセスコントロールグループの作成] ダイアログボックスで、グループの名前 (必須) と説明 (オプション) を入力します。
5. [ソース] に関連付ける IP アドレスまたは CIDR IP 範囲と、[説明] (オプション) を入力します。
6. [タグ] で、各 IP アクセスコントロールグループのキーと値のペアにタグを付けるかどうかを選択します。
7. ルールとタグの追加を完了したら、[保存] を選択します。

IP アクセス設定をウェブポータルに関連付ける

IP アクセスコントロールグループを既存のウェブポータルに関連付けるには、以下の手順に従います。

1. で WorkSpaces Secure Browser コンソールを開きますhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. ナビゲーションペインで、[ウェブポータル] を選択します。
3. ウェブポータルを選択し、[編集] を選択します。
4. [IP アクセスコントロールグループ] で、ウェブポータルの IP アクセスコントロールグループを選択します。
5. [保存] を選択します。

新しいウェブポータルを作成するときに、IP アクセスコントロールグループを関連付けるには、以下の手順に従います。

1. the section called “ポータル設定を構成する” のステップ 1～4 を実行して [IP アクセスコントロール (オプション)] にアクセスします。
2. [IP アクセスコントロールを作成] を選択します。
3. [IP グループの作成] ダイアログボックスで、グループ名と説明を入力します。
4. [ソース] に関連付ける IP アドレスまたは CIDR IP 範囲と、[説明] (オプション) を入力します。
5. [タグ] で、各 IP アクセスコントロールグループのキーと値のペアにタグを付けるかどうかを選択します。

6. ルールとタグの追加を完了したら、[IP アクセスコントロールを作成] を選択します。
7. IP アクセスコントロールグループは、起動時にこのウェブポータルに関連付けられます。

IP アクセスコントロールグループを編集する

IP アクセス設定からいつでもルールを削除できます。ウェブポータルへの接続を許可するために使用されたルールを削除すると、現在のセッションのすべてのユーザーがウェブポータルから切断されます。

IP アクセスコントロールグループを編集するには、以下の手順に従います。

1. で WorkSpaces Secure Browser コンソールを開きますhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. ナビゲーションペインで [IP アクセスコントロール] を選択します。
3. グループを選択してから、[編集] を選択します。
4. 既存のルール [ソース] と [説明] (オプション) を編集するか、ルールを追加します。
5. [タグ] で、各 IP アクセスコントロールグループのキーと値のペアにタグを付けるかどうかを選択します。
6. ルールとタグの追加を完了したら、[保存] を選択します。
7. 既存の IP アクセス設定を更新した場合は、新しいルールまたは編集したルールが有効になるまで最大 15 分待ってください。

IP アクセスコントロールグループを削除する

IP アクセスコントロールグループからいつでもルールを削除できます。ウェブポータルへの接続を許可するために使用されたルールを削除すると、現在のセッションのすべてのユーザーがウェブポータルから切断されます。

IP アクセスコントロールグループを削除するには、以下の手順に従います。

1. で WorkSpaces Secure Browser コンソールを開きますhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. ナビゲーションペインで [IP アクセスコントロールグループ] を選択します。
3. グループを選択し、[削除] を選択します。

シングルサインオンの拡張機能を有効にする (オプション)

エンドユーザーがポータルのサインオンをより快適に行えるように、拡張機能を有効にできます。例えば、ポータルの SAML 2.0 ID プロバイダー (IdP) として Okta を使用し、それをセッション中にユーザーに訪問させたいウェブサイトの IdP としても使用する場合、Okta サインイン Cookie を拡張機能のあるセッションに渡すことができます。その後、ユーザーが Okta ドメイン Cookie を必要とするウェブサイトにアクセスすると、セッション中にサインインしなくてもそのウェブサイトにアクセスできます。

この拡張機能は、Chrome および Firefox ブラウザでサポートされています。この拡張機能により、ユーザーのサインインからセッションまで、許可されたドメインの Cookie を同期できます。この拡張機能はユーザーがログインする必要がなく、背後で機能して、インストール後にユーザーが何も操作しなくても Cookie の同期を有効にします。拡張機能によって保存されるデータはありません。

ユーザーは、ポータルにサインインするときに拡張機能のインストールを求められます。

デフォルトでは、Chrome では、シークレットウィンドウまたは Firefox プライベートブラウジングウィンドウの拡張機能は有効になっていません。ユーザーは手動で有効にできます。Chrome の詳細については、「非シークレットモードの拡張機能」を参照してください。Firefox の詳細については、「 プライベートブラウジングの拡張機能」を参照してください。

ポータルの既存のユーザー設定構成を更新することも、ウェブポータルを初めて作成することもできます。まず、SAML IdP とウェブサイトに必要なドメインを決定します。最大 10 個のドメインを追加できます。

お客様は、同期する Cookie の適切なドメインをテストして特定する責任があります。シングルサインオンを期待どおりに動作させるには、IdP またはウェブサイトの認証レベルで変更が必要な場合があります。

最も一般的な IdP で使用するドメインを確認するには、次の表を参照してください。

IdP とドメイン

IdP	[ドメイン]
Okta	okta.com
Entra ID	microsoftonline.com
AWS Identity Center	awsapps.com

IdP	[ドメイン]
1 回のログイン	onelogin.com
Duo	duosecurity.com

次に、 コンソールでウェブポータルにアクセスします。その後、拡張機能を許可し、どのドメインの Cookie を同期させるかを追加します。以下の手順に従って、拡張機能が許可された新しいポータルを作成するか、既存のポータルを更新します。

ウェブポータルの新規作成時に拡張機能を許可するには、以下の手順を行います。

1. the section called “ユーザー設定を構成する” に到達するまで、the section called “ステップ 1: ウェブポータルを作成する” の手順に従います。
2. the section called “ユーザー設定を構成する” のステップ 1 では、[ユーザーのアクセス許可] で [許可] を選択してウェブポータルの拡張機能を有効にします。
3. Cookie を同期するドメインを入力し、[新しいドメインを追加] を選択します。
4. the section called “ユーザー設定を構成する” の手順と the section called “ステップ 1: ウェブポータルを作成する” の残りのセクションを実行してウェブポータルを作成します。

既存のウェブポータルに拡張機能を追加するには、次の手順に従います。

1. https://console.aws.amazon.com/workspaces-web/home で WorkSpaces Secure Browser コンソールを開きます。
2. 編集するウェブポータルを選択します。
3. [ユーザー設定]、[ユーザーのアクセス許可]、[許可] を選択してウェブポータルの拡張機能を有効にします。
4. Cookie を同期するドメインを入力し、[新しいドメインを追加] を選択します。
5. ポータルの変更を保存します。ポータルは 15 分以内に拡張機能をインストールするようユーザーに求めます。

ドメインを編集したり、拡張機能を削除したりするには、次の手順に従います。

1. https://console.aws.amazon.com/workspaces-web/home で WorkSpaces Secure Browser コンソールを開きます。

2. 編集するウェブポータルを選択します。
3. ウェブポータルの拡張機能を削除するには、[ユーザー設定]、[ユーザーのアクセス許可]、[許可されていません] を選択します。
4. ドメインを個別に削除または編集します。
5. 削除されると、ユーザーがブラウザに WorkSpaces Secure Browser 拡張機能をインストールしている場合でも、セッションは Cookie を同期しなくなります。

拡張機能のユーザーエクスペリエンスの詳細については、「the section called “シングルサインオンの拡張機能”」を参照してください。

URL フィルタリングを設定する

Chrome ポリシーを使用して、ユーザーがリモートブラウザからアクセスできる URLsをフィルタリングできます。Chrome ポリシーには、URLsつのメカニズム、URLAllowlist と URLBlocklist があります。 WorkSpaces Secure Browser コンソールインターフェイスを使用して、URL フィルタリングをポータル設定として設定することも、カスタム JSON ステートメントの一部として追加することもできます (インラインエディタまたは JSON ファイルのアップロード) 。

コンソールを使用して URL フィルタリングを設定するには

1. で WorkSpaces Secure Browser コンソールを開きますhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. WorkSpaces Secure Browser 、Web ポータル を選択し、ウェブポータルを選択してから、詳細の表示 を選択します。
3. URL フィルタリング では、次のオプションから選択します。

   - すべての URLs へのアクセスを許可する: デフォルトでは、ウェブポータルはすべての URLs へのアクセスを許可します。BlockURL リストに特定のウェブサイトを追加して、セッション中にユーザーがそれらのサイトにアクセスできないようにすることができます。例えば、www.anycorp.com を BlockURL リストに追加すると、ユーザーはセッション中に www.anycorp.com に移動できなくなります。
   - すべての URLs へのアクセスをブロックする: デフォルトでは、ウェブポータルはすべての URL へのアクセスをブロックします。URL 許可リストに特定のウェブサイトを追加して、ユーザーがアクセスできるウェブサイトのリストをキュレートし、他のウェブサイトへのトラフィックをブロックできます。セッション中にユーザーがワンクリックアクセスできるように、各 URL をブックマークとして追加することを検討してください。

- 詳細設定： このオプションを選択すると、allowURL リストと blockURLリストが並行して作成されます。URL 許可リスト は、URL ブロックリスト よりも優先されます。このオプションは、パスによる URL フィルタリングを有効にします。例えば、ブロックリストに www.anycorp.com を追加し、許可リストに www.anycorp.com/hr を追加できます。これにより、ユーザーは www.anycorp.com/hr, にアクセスできますが、www.anycorp.com/finance. などの他の URL パスにアクセスできなくなります。

ブロックおよび許可 URLs「ウェブサイトへのアクセスを許可またはブロックする」を参照してください。最良の結果を得るには、Chrome のブロックリストフィルター形式に従って、これらのリストに URLs を追加します。詳細については、「URL ブロックリストフィルター形式」を参照してください。

JSON エディタまたはファイルアップロードを使用して URL フィルタリングを設定するには

1. ポリシー設定モジュールから JSON エディタを選択し、エディタビューまたはファイルアップロードビューのコンソール UI モジュールをバイパスします。
   - エディタを使用すると、お客様は コンソールでカスタムポリシーステートメントをインラインで作成できます。エディタは、ポリシーの作成中に JSON ステートメントのエラーを強調表示します。
   - ファイルのアップロードでは、コンソールの外部で作成された JSON ファイルを追加できます (既存の Chrome ブラウザからエクスポートするなど) 。
2. ウェブポータルの allow/denyURL リストを適切にフォーマットするには、「Chrome Policy details for URLAllowlist and URLBlocklist」を参照してください。詳細については、URLAllowlist」およびURLBlocklist」を参照してください。

ディープリンクを許可する (オプション)

ユーザーが WorkSpaces Secure Browser にサインインすると、管理者が設定したホームページでセッションが開始されます。また、ポータルがセッション中にユーザーを特定のウェブサイトに接続するディープリンクを受信できるようにすることもできます。ディープリンクを選択すると、ポータルにはディープリンクで指定された URL が表示されます。リンクは、セッションの開始用に設定されたホームページ (またはセッションがすでに進行中の場合はそれ自体) と一緒に表示されます。この機能により、管理者は WorkSpaces Secure Browser を使用してより動的なユーザーエクスペリエンスを作成できます。ディープリンクのアクセス許可を許可するには、ユーザー設定の作成時に許可

を選択します。詳細については、「the section called “ユーザー設定を構成する”」を参照してください。

ディープリンクは、 WorkSpaces Secure Browser セッションでページを開きます。セッションがすでに実行されている場合、新しいタブでディープリンクが開きます。セッションがまだ実行されていない場合は、新しいタブでディープリンク URL を開き、別のタブでポータルのデフォルトホームページを開きます。ディープリンクに複数の URL が含まれている場合、最初にフォーカスしてリストされたディープリンク URL が表示され、後続の各 URL (デフォルトのホームページを含む) が別々のタブで開かれます。

ディープリンクは、次の要件を満たしている必要があります。

- ポータルには、ディープリンクのアクセス許可が許可された に設定されている必要があります。詳細については、「the section called “ユーザー設定を構成する”」を参照してください。
- ディープリンク先のサイトは URL エンコードされている必要があります。例えば、ユーザーをhttps://www.example.com/?query=true”, にリンクするには、リンクを https%3A%2F%2Fwww.example.com%2F%3Fquery%3Dtrue に更新します。
- 許可リストに登録されているポータル URL に URL を次の形式で追加します。UUID はポータル ID です。

  https://<uuid>.workspaces-web.com/?deepLinks=https%3A%2F%2Fwww.example.com%2F%3Fquery%3Dtrue
- ディープリンクには、カンマで区切られた最大 10 URLs を含めることができます。例:

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

このポータルリンクを共有するユーザーは、URL ブロックリストではなくポータルからドメインにアクセスできる場合、ディープリンク値を操作してウェブサイトにアクセスできます。制限付き許可リストまたはブロックリストを作成して、ユーザーがポータルで意図しないドメインにアクセスできないようにするには、URL フィルタリングを使用します。ポータルの許可リストとブロックリストは、ポータルのブラウザ設定で URL フィルタリングを使用して編集できます。詳細については、the section called “URL フィルタリングを設定する”「」および「ウェブサイトへのアクセスを許可またはブロックする」を参照してください。

Amazon WorkSpaces Secure Browser のセキュリティ

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャからメリットを得られます。

セキュリティは、 AWS とユーザーの間で共有される責任です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ — クラウドで AWS サービスを実行するインフラストラクチャを保護する責任 AWS は AWS にあります。 AWS また、 では、安全に使用できるサービスも提供しています。コンプライアンスAWS プログラムコンプライアンスプログラム の一環として、サードパーティーの監査者は定期的にセキュリティの有効性をテストおよび検証。Amazon WorkSpaces Secure Browser に適用されるコンプライアンスプログラムの詳細については、「コンプライアンスプログラムによる AWS 対象範囲内のサービス」「コンプライアンスプログラム」を参照してください。
- クラウドのセキュリティ — お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、お客様のデータの機密性、企業の要件、およびデータに適用可能な法律や規制といった他の要因についても責任を担います。

このドキュメントは、Amazon WorkSpaces Secure Browser を使用する際の責任共有モデルの適用方法を理解するのに役立ちます。ここでは、セキュリティおよびコンプライアンスの目的を達成するように Amazon WorkSpaces Secure Browser を設定する方法について説明します。また、Amazon WorkSpaces Secure Browser リソースのモニタリングや保護に役立つ他の AWS のサービスの使用方法についても説明します。

内容

- Amazon WorkSpaces Secure Browser のセキュリティのベストプラクティス

Amazon WorkSpaces Secure Browser でのデータ保護

責任 AWS 共有モデル、Amazon WorkSpaces Secure Browser でのデータ保護に適用されます。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。お客様は、このインフラストラクチャでホストされているコンテンツに対する管理を維持する責任があります。また、使用する AWS サービス のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、「データプライバシーFAQ」を参照してください。欧州でのデータ保護の詳細については、AWS 「 セキュリティブログ」のAWS 「責任共有モデル」とGDPRブログ記事を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM Identity Center または AWS Identity and Access Management () を使用して個々のユーザーを設定することをお勧めしますIAM。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。1TLS.2 が必要で、1.3 TLS をお勧めします。
- を使用して APIとユーザーアクティビティのログ記録を設定します AWS CloudTrail。
- AWS 暗号化ソリューションと、 内のすべてのデフォルトのセキュリティコントロールを使用します AWS サービス。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは AWS を介して にアクセスするときに FIPS 140-3 検証済みの暗号化モジュールが必要な場合はAPI、FIPSエンドポイントを使用します。利用可能なFIPSエンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これは、コンソール、、またはを使用して WorkSpaces Secure Browser または他の AWS サービス を使用する場合API AWS CLIも同様です AWS SDKs。名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。URL を外部サーバーに提供する場合は、そのサーバーへのリクエストを検証URLするために認証情報を に含めないことを強くお勧めします。

データ暗号化

Amazon WorkSpaces Secure Browser は、ブラウザ設定、ユーザー設定、ネットワーク設定、ID プロバイダー情報、トラストストアデータ、トラストストア証明書データなどのポータルカスタマイズデータを収集します。 WorkSpaces Secure Browser は、ブラウザポリシーデータ、ユーザー設定 (ブラウザ設定用) 、セッションログも収集します。収集されたデータは Amazon DynamoDB と Amazon S3 に保存されます。 WorkSpaces Secure Browser は暗号化 AWS Key Management Service に を使用します。

コンテンツを保護するには、次のガイドラインに従ってください。

- 最小特権アクセスを実装し、 WorkSpaces Secure Browser アクションに使用する特定のロールを作成します。IAM テンプレートを使用して、フルアクセスロールまたは読み取り専用ロールを作成します。詳細については、「AWS WorkSpaces Secure Browser の マネージドポリシー」を参照してください。
- カスタマーマネージドキーを提供することでデータをエンドツーエンドで保護し、 WorkSpaces Secure Browser が保管中のデータを指定したキーで暗号化できるようにします。
- ポータルのドメインとユーザー認証情報を共有する場合は注意が必要です。
  - 管理者は Amazon WorkSpaces コンソールにログインする必要があり、ユーザーは WorkSpaces Secure Browser ポータルにログインする必要があります。
  - インターネット上の誰でもウェブポータルにアクセスできますが、ポータルへの有効なユーザー認証情報がないとセッションを開始できません。
- ユーザーは [セッションの終了] を選択してセッションを明示的に終了できます。これにより、ブラウザセッションをホストしているインスタンスが破棄され、ブラウザが分離されます。

WorkSpaces Secure Browser は、すべての機密データを で暗号化することで、デフォルトでコンテンツとメタデータを保護します AWS KMS。ブラウザポリシーとユーザー設定を収集して、WorkSpaces Secure Browser セッション中にポリシーと設定を適用します。既存の設定を適用する際にエラーが発生した場合、ユーザーは新しいセッションにアクセスできず、会社の内部サイトや SaaS アプリケーションにもアクセスできません。

保管中の暗号化

[保管時の暗号化] はデフォルトで構成されます。 WorkSpaces Secure Browser で使用される顧客固有のデータは、 を使用して暗号化されます AWS KMS。 WorkSpaces Secure Browser は、作成するリソースの保管時の暗号化を提供します。サービスは、リソースの作成時に AWS KMS カスタマー

マネージドキーを受け入れ、指定されていない場合は、 AWS 所有キーを使用して保管中のリソースを暗号化します。このサービスは、ブラウザセッションをカスタマイズするのに提供できるブラウザポリシードキュメント、ID プロバイダーの設定、ポータルの表示名を暗号化します。この情報は、バックエンドに保存されている間、カスタマーマネージドキーまたは AWS 所有キーを使用して暗号化されたままになります。

WorkSpaces Secure Browser リソースを作成するときに使用するキーを決定できます。そのリソースの一部であるデータが暗号化されている場合、 WorkSpaces Secure Browser は の一部として `create customerManagedKeyArn`フィールドを受け入れますAPI。指定するキーは対称 AWS KMS キーでなければならず、このキーを使用してリソースを作成する管理者には `kms:Decrypt`、`kms:GenerateDataKey`、`kms:CreateGrant` アクセス許可が必要です。キーを使用してリソースを作成した後は、キーを削除したり変更したりすることはできません。カスタマーマネージドキーを使用した場合、リソースにアクセスする管理者には `kms:Decrypt` および `kms:GenerateDataKey` アクセス許可が必要です。コンソールの使用中にアクセスが拒否されるというエラーが表示された場合は、コンソールを使用するユーザーが、使用したキーでこれらのアクセス許可を持っていることを確認してください。

AWS KMS グラントのステータスを確認することで、キーの使用をトラブルシューティングおよび監査できます。詳細については、「グラントの管理」を参照してください。ポータルの作成時に、WorkSpaces Secure Browser は、サービスがキーに非同期的にアクセスできるように許可を作成します。グラントを確認することで、キーの使用状況を確認できるほか、グラントの使用時に提供される暗号化コンテキストも確認できます。暗号化コンテキストには、キー `aws:workspaces-web:portal:id` とポータル ID と同じ値を含むエントリが必ず含まれます。その他のリソースの場合、暗号化コンテキストには常に `aws:workspaces-web:`*`RESOURCE_TYPE`*`:id` 形式のエントリと対応するリソース ID が含まれます。

転送中の暗号化

WorkSpaces Secure Browser は、 HTTPSおよび 1.2 TLS を介して転送中のデータを暗号化します。コンソールまたは直接API呼び出し WorkSpaces を使用して、 にリクエストを送信できます。転送されるリクエストデータは、 HTTPSまたは TLS接続を介してすべてを送信することで暗号化されます。リクエストデータは、 AWS コンソール、 AWS Command Line Interfaceまたは AWS SDK WorkSpaces Secure Browser に転送できます。

転送中の暗号化はデフォルトで設定され、安全な接続 (HTTPS、TLS) はデフォルトで設定されます。

キー管理

独自のカスタマーマネージド AWS KMS キーを指定して、顧客情報を暗号化できます。指定しない場合、 WorkSpaces Secure Browser は AWS 所有キーを使用します。を使用してキーを設定できます AWS SDK。

ネットワーク間トラフィックのプライバシー

WorkSpaces Secure Browser とオンプレミスアプリケーション間の接続を保護するには、WorkSpaces Secure Browser を使用して、独自の 内でブラウザセッションを起動しますVPC。オンプレミスアプリケーションへの接続は独自の で設定されVPC、 WorkSpaces Secure Browser によって制御されません。

アカウント間の接続を保護するために、 WorkSpaces Secure Browser はサービスにリンクされたロールを使用してお客様のアカウントに安全に接続し、お客様に代わってオペレーションを実行します。詳細については、「WorkSpaces Secure Browser のサービスにリンクされたロールの使用」を参照してください。

ユーザーアクセスロギング

管理者は、開始、停止、URL訪問などの WorkSpaces Secure Browser セッションイベントを記録できます。これらのログは暗号化され、Amazon Kinesis Data Streams を通じてカスタマーに安全に配信されます。ユーザーアクセスのログ記録からの閲覧情報は、 によって保存されず AWS、ログ記録が設定されていないセッションからも使用できます。URL シークレットモードでの の訪問、またはブラウザ履歴URLsから削除された の訪問は、ユーザーアクセスログには記録されません。

Amazon WorkSpaces Secure Browser の Identity and Access Management

AWS Identity and Access Management （ IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS サービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰に WorkSpaces Secure Browser リソースの使用を許可する (アクセス許可を付与する) かを制御します。IAM は追加料金なしで AWS サービス 使用できる です。

トピック

- 対象者

- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- Amazon WorkSpaces Secure Browser と の連携方法 IAM
- Amazon WorkSpaces Secure Browser のアイデンティティベースのポリシーの例
- AWS WorkSpaces Secure Browser の マネージドポリシー
- Amazon WorkSpaces Secure Browser のアイデンティティとアクセスのトラブルシューティング
- WorkSpaces Secure Browser のサービスにリンクされたロールの使用

対象者

AWS Identity and Access Management （ IAM) の使用方法は、 WorkSpaces Secure Browser で行う作業によって異なります。

サービスユーザー – ジョブを実行するために WorkSpaces Secure Browser サービスを使用する場合、管理者から必要な認証情報とアクセス許可が与えられます。作業を実行するためにさらに多くの WorkSpaces Secure Browser 機能を使用するときは、追加のアクセス許可が必要になる場合があります。アクセスの管理方法を理解しておくと、管理者に適切な許可をリクエストするうえで役立ちます。 WorkSpaces Secure Browser の機能にアクセスできない場合は、「」を参照してくださいAmazon WorkSpaces Secure Browser のアイデンティティとアクセスのトラブルシューティング。

サービス管理者 – 社内の WorkSpaces Secure Browser リソースを担当している場合は、通常、Secure Browser WorkSpaces へのフルアクセスがあります。サービスユーザーがどの WorkSpaces Secure Browser 機能やリソースにアクセスするかを決めるのは管理者の仕事です。次に、サービスユーザーのアクセス許可を変更するリクエストをIAM管理者に送信する必要があります。このページの情報を確認して、 の基本概念を理解してくださいIAM。会社で WorkSpaces Secure Browser IAMを使用する方法の詳細については、「」を参照してくださいAmazon WorkSpaces Secure Browser と の連携方法 IAM。

IAM 管理者 – IAM管理者は、 WorkSpaces Secure Browser へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります。で使用できる WorkSpaces Secure Browser アイデンティティベースのポリシーの例を表示するにはIAM、「」を参照してくださいAmazon WorkSpaces Secure Browser のアイデンティティベースのポリシーの例。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。として、IAMユーザーとして AWS アカウントのルートユーザー、または IAMロールを引き受けることによって認証 (にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM Identity Center （ IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook の認証情報は、フェデレーティッド ID の例です。フェデレーティッド ID としてサインインすると、管理者は以前に IAMロールを使用して ID フェデレーションをセットアップしていました。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、 AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「 ユーザーガイド」の「 にサインインする方法 AWS アカウントAWS サインイン 」を参照してください。

AWS プログラムで にアクセスする場合、 はソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストに暗号で署名します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。推奨される方法を使用してリクエストを自分で署名する方法の詳細については、「 IAMユーザーガイド」のAWS API「リクエストの署名」を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、 AWS では、アカウントのセキュリティを高めるために多要素認証 (MFA) を使用することをお勧めします。詳細については、「 AWS IAM Identity Center ユーザーガイド」の「多要素認証」および「 ユーザーガイド」の「 での多要素認証 (MFA) AWS IAM の使用」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS サービス 完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「 IAMユーザーガイド」の「ルートユーザーの認証情報を必要とするタスク」を参照してください。

フェデレーティッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、一時的な認証情報を使用して にアクセスするために ID プロバイダーとのフェデレーションを使用することを要求 AWS サービス します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、AWS Directory Service、アイデンティティセンターディレクトリのユーザー、またはアイデンティティソースを通じて提供された認証情報 AWS サービス を使用して にアクセスするユーザーです。フェデレーティッド ID が にアクセスすると AWS アカウント、ロールを引き受け、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成することも、独自の ID ソース内のユーザーとグループのセットに接続して同期して、すべての AWS アカウント とアプリケーションで使用することもできます。IAM Identity Center の詳細については、「 ユーザーガイド」のIAM「Identity Center とはAWS IAM Identity Center 」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を持つIAMユーザーを作成するのではなく、一時的な認証情報を使用することをお勧めします。ただし、IAMユーザーとの長期的な認証情報を必要とする特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「 ユーザーガイド」の「長期的な認証情報を必要とするユースケースでアクセスキーを定期的にローテーションするIAM」を参照してください。

IAM グループは、IAMユーザーのコレクションを指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、 という名前のグループを作成しIAMAdmins、そのグループにIAMリソースを管理するアクセス許可を付与できます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、「 ユーザーガイド」のIAM「 (ロールではなく) ユーザーを作成する場合IAM」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。ユーザーと似ていますがIAM、特定のユーザーに関連付けられていません。IAM ロール を切り替える AWS Management Console ことで、 で ロールを一時的に引き受けることができます。ロールを引き受けるには、 または AWS API オペレーションを AWS CLI 呼び出すか、カスタム を使用しますURL。ロールの使用方法の詳細については、「 ユーザーガイド」のIAM「ロールの使用IAM」を参照してください。

IAM 一時的な認証情報を持つ ロールは、以下の状況で役立ちます。

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールの詳細については、「 ユーザーガイド」の「サードパーティー ID プロバイダーのロールの作成IAM」を参照してください。IAM Identity Center を使用する場合は、アクセス許可セットを設定します。ID が認証後にアクセスできる内容を制御するために、IAMIdentity Center はアクセス許可セットを のロールに関連付けますIAM。アクセス許可セットの詳細については、「AWS IAM Identity Center ユーザーガイド」の「アクセス許可セット」を参照してください。
- 一時的なIAMユーザーアクセス許可 – IAM ユーザーまたはロールは、 IAMロールを引き受けて、特定のタスクに対して異なるアクセス許可を一時的に引き受けることができます。
- クロスアカウントアクセス – IAMロールを使用して、別のアカウントのユーザー (信頼されたプリンシパル) が自分のアカウントのリソースにアクセスすることを許可できます。クロスアカウントアクセスを許可する主な方法は、ロールを使用することです。ただし、一部の では AWS サービス、 (ロールをプロキシとして使用する代わりに) ポリシーをリソースに直接アタッチできます。クロスアカウントアクセスのロールとリソースベースのポリシーの違いについては、「 ユーザーガイド」の「 でのクロスアカウントリソースアクセスIAMIAM」を参照してください。
- クロスサービスアクセス — 一部の は、他の の機能 AWS サービス を使用します AWS サービス。例えば、サービスで呼び出しを行うと、そのサービスが Amazon でアプリケーションを実行EC2したり、Amazon S3 にオブジェクトを保存したりするのが一般的です。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS サービス、ダウンストリームサービス AWS サービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他

の AWS サービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するための権限が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

- サービスロール – サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受ける IAMロールです。IAM 管理者は、 内からサービスロールを作成、変更、削除できますIAM。詳細については、「 ユーザーガイド」の「 にアクセス許可を委任するロールの作成 AWS サービスIAM」を参照してください。
- サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS サービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

- Amazon で実行されているアプリケーション EC2 – IAMロールを使用して、EC2インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2インスタンス内にアクセスキーを保存するよりも望ましいです。 AWS ロールをEC2インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルには ロールが含まれており、EC2インスタンスで実行されているプログラムが一時的な認証情報を取得できるようにします。詳細については、「 ユーザーガイド」の「 IAMロールを使用して Amazon EC2インスタンスで実行されているアプリケーションにアクセス許可を付与するIAM」を参照してください。

IAM ロールとIAMユーザーのどちらを使用するかについては、「 ユーザーガイド」の「 IAMロールを作成するタイミング (ユーザーではなく) IAM」を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、 AWS ID またはリソースにアタッチします。ポリシーは、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義するのオブジェクトです。プリンシパル (ユーザー、ルートユーザー、またはロールセッション) AWS がリクエストを行うと、 はこれらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーはJSONドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「 ユーザーガイド」のJSON「ポリシーの概要IAM」を参照してください。

管理者はポリシーを使用して AWS JSON、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。必要なリソースに対してアクションを実行するアクセス許可をユーザーに付与するために、IAM管理者はIAMポリシーを作成できます。その後、管理者はIAMポリシーをロールに追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行に使用する方法に関係なく、アクションのアクセス許可を定義します。例えば、`iam:GetRole`アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS Management Console、、 AWS CLIまたは AWS からロール情報を取得できますAPI。

アイデンティティベースのポリシー

ID ベースのポリシーは、IAMユーザー、ユーザーのグループ、ロールなどの ID にアタッチできるJSONアクセス許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「 ユーザーガイド」のIAM「ポリシーの作成IAM」を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。管理ポリシーとインラインポリシーのどちらかを選択する方法については、「 IAM ユーザーガイド」の「管理ポリシーとインラインポリシーの選択」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースにアタッチするJSONポリシードキュメントです。リソースベースのポリシーの例としては、IAMロールの信頼ポリシー や Amazon S3 バケットポリシー などがあります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS サービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーIAMでは、 の AWS 管理ポリシーを使用できません。

アクセスコントロールリスト (ACLs)

アクセスコントロールリスト (ACLs) は、リソースへのアクセス許可を持つプリンシパル (アカウントメンバー、ユーザー、またはロール) を制御します。ACLs はリソースベースのポリシーに似ていますが、JSONポリシードキュメント形式を使用しません。

Amazon S3、 AWS WAF、および Amazon VPCは、 をサポートするサービスの例ですACLs。の詳細についてはACLs、Amazon Simple Storage Service デベロッパーガイドの「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS は、一般的ではない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 – アクセス許可の境界は、アイデンティティベースのポリシーがIAMエンティティ (IAMユーザーまたはロール) に付与できるアクセス許可の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「 IAMユーザーガイド」の「 IAMエンティティのアクセス許可の境界」を参照してください。
- サービスコントロールポリシー (SCPs) – SCPsは、 の組織または組織単位 (OU) に対する最大アクセス許可を指定するJSONポリシーです AWS Organizations。 AWS Organizations は、 AWS アカウント ビジネスが所有する複数の をグループ化して一元管理するためのサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCPs) をアカウントの一部またはすべてに適用できます。は、各 を含むメンバーアカウントのエンティティのアクセス許可SCP を制限します AWS アカウントのルートユーザー。Organizations と の詳細についてはSCPs、「 AWS Organizations ユーザーガイド」の「サービスコントロールポリシー」を参照してください。
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「 ユーザーガイド」の「セッションポリシーIAM」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、「 ユーザーガイド」の「ポリシー評価ロジックIAM」を参照してください。

Amazon WorkSpaces Secure Browser と の連携方法 IAM

IAM を使用して WorkSpaces Secure Browser へのアクセスを管理する前に、Secure Browser WorkSpaces で使用できるIAM機能を確認してください。

IAM Amazon WorkSpaces Secure Browser で使用できる の機能

IAM 機能	WorkSpaces Secure Browser のサポート
アイデンティティベースのポリシー	あり
リソースベースのポリシー	なし
ポリシーアクション	あり
ポリシーリソース	Yes
ポリシー条件キー	あり
ACLs	なし
ABAC (ポリシー内のタグ)	部分的
一時的な認証情報	あり
プリンシパル権限	あり
サービスロール	いいえ
サービスリンクロール	あり

WorkSpaces Secure Browser およびその他の AWS のサービスがほとんどの IAM 機能と連携する方法の概要を把握するには、IAM「 ユーザーガイド」のAWS 「 と連携する のサービスIAM」を参照してください。

WorkSpaces Secure Browser のアイデンティティベースのポリシー

アイデンティティベースのポリシーのサポート: あり

ID ベースのポリシーは、IAMユーザー、ユーザーのグループ、ロールなどの ID にアタッチできるJSONアクセス許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「 ユーザーガイド」のIAM「ポリシーの作成IAM」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否されたアクションとリソース、およびアクションが許可または拒否される条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素については、「 ユーザーガイド」の「 IAMJSONポリシー要素のリファレンスIAM」を参照してください。

WorkSpaces Secure Browser のアイデンティティベースのポリシーの例

WorkSpaces Secure Browser のアイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAmazon WorkSpaces Secure Browser のアイデンティティベースのポリシーの例。

WorkSpaces Secure Browser 内のリソースベースのポリシー

リソースベースのポリシーのサポート: なし

リソースベースのポリシーは、リソースにアタッチするJSONポリシードキュメントです。リソースベースのポリシーの例としては、IAMロールの信頼ポリシー や Amazon S3 バケットポリシー などがあります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS サービス。

クロスアカウントアクセスを有効にするには、リソースベースのポリシーで、アカウント全体または別のアカウントのIAMエンティティをプリンシパルとして指定できます。リソースベースのポリシー

にクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる にある場合 AWS アカウント、信頼されたアカウントのIAM管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス許可も付与する必要があります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーをさらに付与する必要はありません。詳細については、「 ユーザーガイド」の「 でのクロスアカウントリソースアクセスIAMIAM」を参照してください。

WorkSpaces Secure Browser のポリシーアクション

ポリシーアクションのサポート: あり

管理者はポリシーを使用して AWS JSON、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの `Action`要素は、ポリシーでアクセスを許可または拒否するために使用できるアクションを記述します。ポリシーアクションの名前は通常、関連する AWS APIオペレーションと同じです。一致するAPIオペレーションを持たないアクセス許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは、依存アクションと呼ばれます。

このアクションは、関連付けられたオペレーションを実行するための権限を付与するポリシーで使用されます。

WorkSpaces Secure Browser アクションのリストを確認するには、「サービス認証リファレンス」の「Amazon WorkSpaces Secure Browser で定義されるアクション」を参照してください。

WorkSpaces Secure Browser のポリシーアクションは、アクションの前に次のプレフィックスを使用します。

```
workspaces-web
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

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

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

WorkSpaces Secure Browser のアイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAmazon WorkSpaces Secure Browser のアイデンティティベースのポリシーの例。

WorkSpaces Secure Browser のポリシーリソース

ポリシーリソースのサポート: あり

管理者はポリシーを使用して AWS JSON、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Policy `Resource`JSON要素は、アクションが適用されるオブジェクトを指定します。ステートメントには、`Resource` または `NotResource` 要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

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

WorkSpaces Secure Browser のリソースタイプとその のリストを確認するにはARNs、「サービス認証リファレンス」の「Amazon WorkSpaces Secure Browser で定義されるリソース」を参照してください。各リソースARNの を指定できるアクションについては、「Amazon WorkSpaces Secure Browser で定義されるアクション」を参照してください。

WorkSpaces Secure Browser のアイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAmazon WorkSpaces Secure Browser のアイデンティティベースのポリシーの例。

WorkSpaces Secure Browser のポリシー条件キー

サービス固有のポリシー条件キーのサポート: あり

管理者はポリシーを使用して AWS JSON、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルが、どのリソースに対してどのような条件下でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成することで、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition 要素を指定する場合、または 1 つの Condition 要素に複数のキーを指定する場合、 AWS では AND 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理ORオペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば、リソースにIAMユーザー名でタグ付けされている場合にのみ、リソースへのアクセス許可をIAMユーザーに付与できます。詳細については、「 ユーザーガイド」のIAM「ポリシー要素: 変数とタグIAM」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートします。すべての AWS グローバル条件キーを確認するには、「 ユーザーガイド」のAWS 「 グローバル条件コンテキストキーIAM」を参照してください。

WorkSpaces Secure Browser の条件キーのリストを確認するには、「サービス認証リファレンス」の「Amazon WorkSpaces Secure Browser の条件キー」を参照してください。条件キーを使用できるアクションとリソースについては、「Amazon WorkSpaces Secure Browser で定義されるアクション」を参照してください。

WorkSpaces Secure Browser のアイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAmazon WorkSpaces Secure Browser のアイデンティティベースのポリシーの例。

WorkSpaces Secure Browser のアクセスコントロールリスト (ACLs)

をサポートACLs： いいえ

アクセスコントロールリスト (ACLs) は、リソースへのアクセス許可を持つプリンシパル (アカウントメンバー、ユーザー、またはロール) を制御します。ACLs はリソースベースのポリシーに似ていますが、JSONポリシードキュメント形式を使用しません。

WorkSpaces Secure Browser を使用した属性ベースのアクセスコントロール (ABAC)

サポート ABAC (ポリシー内のタグ): 部分的

属性ベースのアクセスコントロール (ABAC) は、属性に基づいてアクセス許可を定義する認可戦略です。では AWS、これらの属性はタグ と呼ばれます。タグは、IAMエンティティ (ユーザーまたはロール) および多くの AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、の最初のステップですABAC。次に、プリンシパルのタグがアクセスしようとしているリソースのタグと一致する場合に、オペレーションを許可するABACポリシーを設計します。

ABAC は、急速に成長している環境や、ポリシー管理が煩雑になる状況に役立ちます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

の詳細についてはABAC、「 IAMユーザーガイド」の「 とはABAC」を参照してください。をセットアップする手順を含むチュートリアルを表示するにはABAC、「 ユーザーガイド」の「属性ベースのアクセスコントロール (ABAC) を使用するIAM」を参照してください。

WorkSpaces Secure Browser での一時的な認証情報の使用

一時的な認証情報のサポート: あり

一部の は、一時的な認証情報を使用してサインインすると機能 AWS サービス しません。一時的な認証情報 AWS サービス を使用する機能などの詳細については、「 ユーザーガイド」のAWS サービス 「 と連携IAMする IAM 」を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合、一時的な認証情報を使用します。例えば、会社のシングルサインオン (SSO) リンク AWS を使用して にアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えの詳細については、「 IAMユーザーガイド」の「ロールへの切り替え (コンソール) 」を参照してください。

一時的な認証情報は、 AWS CLI または を使用して手動で作成できます AWS API。その後、これらの一時的な認証情報を使用して . AWS recommends にアクセスできます AWS。これは、長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成することを推奨しています。詳細については、「」の「一時的なセキュリティ認証情報IAM」を参照してください。

WorkSpaces Secure Browser のクロスサービスプリンシパル許可

転送アクセスセッションをサポート (FAS): はい

IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS サービス、ダウンストリームサービス AWS サービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS サービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するための権限が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

WorkSpaces Secure Browser のサービスロール

サービスロールのサポート: なし

サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受ける IAM ロールです。IAM 管理者は、 内からサービスロールを作成、変更、削除できますIAM。詳細については、「 ユーザーガイド」の「 にアクセス許可を委任するロールの作成 AWS サービスIAM」を参照してください。

> **Warning**
>
> サービスロールのアクセス許可を変更すると、 WorkSpaces Secure Browser の機能が破損する可能性があります。 WorkSpaces Secure Browser が指示する場合以外は、サービスロールを編集しないでください。

WorkSpaces Secure Browser のサービスにリンクされたロール

サービスリンクロールのサポート: あり

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS サービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

サービスにリンクされたロールの作成または管理の詳細については、「AWS と連携する のサービスIAM」を参照してください。表の中から、[Service-linked role] (サービスにリンクされたロール) 列に Yes と記載されたサービスを見つけます。サービスリンクロールに関するドキュメントをサービスで表示するには、はい リンクを選択します。

Amazon WorkSpaces Secure Browser のアイデンティティベースのポリシーの例

デフォルトでは、ユーザーとロールには WorkSpaces Secure Browser リソースを作成または変更するアクセス許可はありません。また、、 AWS Command Line Interface （ AWS CLI ） AWS Management Console、または を使用してタスクを実行することはできません AWS API。必要なリソースに対してアクションを実行するアクセス許可をユーザーに付与するために、IAM管理者はIAMポリシーを作成できます。その後、管理者はIAMポリシーをロールに追加し、ユーザーはロールを引き受けることができます。

これらのポリシードキュメント例を使用してIAMアイデンティティベースのJSONポリシーを作成する方法については、「 ユーザーガイド」のIAM「ポリシーの作成IAM」を参照してください。

各リソースタイプの の形式など、 WorkSpaces Secure Browser で定義されるアクションとリソースタイプの詳細については、「サービス認証リファレンスARNs」の「Amazon WorkSpaces Secure Browser のアクション、リソース、および条件キー」を参照してください。

トピック

- ポリシーのベストプラクティス
- WorkSpaces Secure Browser コンソールの使用
- 自分の権限の表示をユーザーに許可する

ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが WorkSpaces Secure Browser リソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可を付与するには、多くの一般的なユースケースにアクセス許可を付与する AWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カ

スタマー管理ポリシーを定義して、アクセス許可をさらに減らすことをお勧めします。詳細については、「 ユーザーガイド」の「 AWS 管理ポリシー」または「 ジョブ機能の 管理ポリシーIAM」を参照してください。 AWS

- 最小特権のアクセス許可を適用する – IAMポリシーでアクセス許可を設定する場合は、タスクの実行に必要なアクセス許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用してアクセス許可を適用する方法の詳細については、「 ユーザーガイド」の「 のポリシーとアクセス許可IAMIAM」を参照してください。
- IAM ポリシーの条件を使用してアクセスをさらに制限する – ポリシーに条件を追加して、アクションとリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを を使用して送信する必要があることを指定できますSSL。条件を使用して、 などの特定の を介してサービスアクションが使用される場合に AWS サービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「 ユーザーガイド」のIAMJSON「ポリシー要素: 条件IAM」を参照してください。
- IAM Access Analyzer を使用してIAMポリシーを検証し、安全で機能的なアクセス許可を確保する – IAM Access Analyzer は、ポリシーがポリシー言語 (JSON) とIAMベストプラクティスに準拠するように、新規および既存のIAMポリシーを検証します。IAM Access Analyzer には、安全で機能的なポリシーの作成に役立つ 100 を超えるポリシーチェックと実用的な推奨事項が用意されています。詳細については、「 ユーザーガイド」のIAM「Access Analyzer ポリシーの検証IAM」を参照してください。
- 多要素認証を要求する (MFA) – でIAMユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化MFAするために をオンにします。API オペレーションが呼び出されるMFAタイミングを要求するには、ポリシーにMFA条件を追加します。詳細については、「 IAMユーザーガイド」のMFA「 で保護されたAPIアクセスの設定」を参照してください。

のベストプラクティスの詳細についてはIAM、「 ユーザーガイド」の「 のセキュリティのベストプラクティスIAMIAM」を参照してください。

WorkSpaces Secure Browser コンソールの使用

Amazon WorkSpaces Secure Browser コンソールにアクセスするには、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、 の WorkSpaces Secure Browser リソースの詳細を一覧表示および表示できます AWS アカウント。最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

AWS CLI または のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません AWS API。代わりに、実行しようとしているAPIオペレーションに一致するアクションにのみアクセスを許可します。

ユーザーとロールが引き続き WorkSpaces Secure Browser コンソールを使用できるようにするには、Secure Browser `ConsoleAccess`または WorkSpaces `ReadOnly` AWS 管理ポリシーもエンティティにアタッチします。詳細については、「 ユーザーガイド」の「ユーザーへのアクセス許可の追加IAM」を参照してください。

自分の権限の表示をユーザーに許可する

この例では、IAMユーザーがユーザー ID にアタッチされているインラインポリシーと管理ポリシーを表示できるようにするポリシーを作成する方法を示します。このポリシーには、コンソールで、または AWS CLI または を使用してプログラムでこのアクションを実行するアクセス許可が含まれています AWS API。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
```

```
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS WorkSpaces Secure Browser の マネージドポリシー

ユーザー、グループ、ロールにアクセス許可を追加するには、自分でポリシーを記述するよりも、AWS 管理ポリシーを使用する方が簡単です。チームに必要な許可のみを提供する IAM カスタマーマネージドポリシーを作成するには、時間と専門知識が必要です。すぐに開始するには、 AWS マネージドポリシーを使用できます。これらのポリシーは一般的なユースケースを対象としており、 AWS アカウントで利用できます。 AWS 管理ポリシーの詳細については、「IAM ユーザーガイド」の「AWS 管理ポリシー」を参照してください。

AWS サービスは、 AWS マネージドポリシーを維持および更新します。 AWS 管理ポリシーのアクセス許可は変更できません。サービスは、 AWS マネージドポリシーに新しい機能をサポートするために追加のアクセス許可を追加する場合があります。この種類の更新は、ポリシーがアタッチされている、すべてのアイデンティティ (ユーザー、グループおよびロール) に影響を与えます。新しい機能が立ち上げられた場合や、新しいオペレーションが使用可能になった場合に、各サービスが AWS マネージドポリシーを更新する可能性が最も高くなります。サービスは AWS マネージドポリシーからアクセス許可を削除しないため、ポリシーの更新によって既存のアクセス許可が中断されることはありません。

さらに、 は、複数の サービスにまたがる職務機能の マネージドポリシー AWS をサポートします。例えば、 `ReadOnlyAccess` AWS 管理ポリシーは、すべての AWS サービスとリソースへの読み取り専用アクセスを提供します。サービスが新機能を起動すると、 は新しいオペレーションとリソースの読み取り専用アクセス許可 AWS を追加します。ジョブ機能のポリシーの一覧および詳細については、「IAM ユーザーガイド」の「AWS のジョブ機能のマネージドポリシー」を参照してください。

AWS マネージドポリシー： AmazonWorkSpacesWebServiceRolePolicy

IAM エンティティに AmazonWorkSpacesWebServiceRolePolicy ポリシーをアタッチすることはできません。このポリシーは、 WorkSpaces Secure Browser がユーザーに代わってアクションを実行できるようにするサービスにリンクされたロールにアタッチされます。詳細については、「the section called “サービスリンクロールの使用”」を参照してください。

このポリシーは、 WorkSpaces Secure Browser が使用または管理する AWS のサービスおよびリソースへのアクセスを許可する管理アクセス許可を付与します。

許可の詳細

このポリシーには、以下の許可が含まれています。

- workspaces-web – WorkSpaces Secure Browser が使用または管理する AWS のサービスおよびリソースへのアクセスを許可します。
- ec2 – プリンシパルが VPC、サブネット、アベイラビリティーゾーンの説明、ネットワークインターフェイスの作成、タグ付け、説明、削除、アドレスの関連付けまたは関連付け解除、ルートテーブル、セキュリティグループ、VPC エンドポイントの説明を行うことができます。
- CloudWatch – プリンシパルがメトリクスデータを入力できるようにします。
- Kinesis - プリンシパルが Kinesis データストリームの概要を記述し、レコードを Kinesis データストリームに入力してユーザーアクセスロギングを行うことができます。詳細については、「the section called “ユーザーアクセスロギングをセットアップする”」を参照してください。

```
{
    "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 マネージドポリシー: AmazonWorkSpacesSecureBrowserReadOnly

AmazonWorkSpacesSecureBrowserReadOnly ポリシーは IAM ID にアタッチできます。

このポリシーは、 AWS マネジメントコンソール、SDK、および CLI を介して WorkSpaces Secure Browser とその依存関係へのアクセスを許可する読み取り専用アクセス許可を付与します。このポリシーには、認証タイプとして IAM_Identity_Center を使用するポータルとのやり取りに必要なアクセス許可は含まれていません。これらのアクセス許可を取得するには、このポリシーを AWSSSOReadOnly と組み合わせてください。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- workspaces-web – AWS マネジメントコンソール、SDK、および CLI を介して、 WorkSpaces Secure Browser とその依存関係への読み取り専用アクセスを提供します。
- ec2 – プリンシパルが VPC、サブネット、およびセキュリティグループを記述できるようにします。これは、 WorkSpaces Secure Browser の AWS マネジメントコンソールで使用され、サービスで使用できる VPCsサブネット、およびセキュリティグループを表示します。
- Kinesis - プリンシパルが Kinesis データストリームをリストできるようにします。これは、WorkSpaces Secure Browser の AWS マネジメントコンソールで使用され、サービスで使用できる Kinesis データストリームを表示します。

```
{
    "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 マネージドポリシー: AmazonWorkSpacesWebReadOnly

AmazonWorkSpacesWebReadOnly ポリシーは IAM ID にアタッチできます。

このポリシーは、 AWS マネジメントコンソール、SDK、および CLI を介して WorkSpaces Secure Browser とその依存関係へのアクセスを許可する読み取り専用アクセス許可を付与します。このポリシーには、認証タイプとして IAM_Identity_Center を使用するポータルとのやり取りに必要なアクセス許可は含まれていません。これらのアクセス許可を取得するには、このポリシーを AWSSSOReadOnly と組み合わせてください。

> **Note**
>
> 現在このポリシーを使用している場合は、新しいAmazonWorkSpacesSecureBrowserReadOnlyポリシーに切り替えます。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- workspaces-web – AWS マネジメントコンソール、SDK、および CLI を介して、 WorkSpaces Secure Browser とその依存関係への読み取り専用アクセスを提供します。
- ec2 – プリンシパルが VPC、サブネット、およびセキュリティグループを記述できるようにします。これは、 WorkSpaces Secure Browser の AWS マネジメントコンソールで使用され、サービスで使用できる VPCsサブネット、およびセキュリティグループを表示します。
- Kinesis - プリンシパルが Kinesis データストリームをリストできるようにします。これは、 WorkSpaces Secure Browser の AWS マネジメントコンソールで使用され、サービスで使用できる Kinesis データストリームを表示します。

```
{
    "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 AWS マネージドポリシーへのセキュアブラウザの更新

WorkSpaces Secure Browser の AWS マネージドポリシーの更新に関する詳細を、このサービスがこれらの変更の追跡を開始した以降の分について表示します。このページへの変更に関する自動アラートについては、ドキュメント履歴 ページの RSS フィードを購読してください。

変更	説明	日付
AmazonWorkSpacesSecureBrowserReadOnly - 新しいポリシー	WorkSpaces Secure Browser は、AWS マネジメントコンソール、SDK、および CLI を介して WorkSpaces Secure Browser とその依存関係への読み取り専用アクセスを提供する新しいポリシーを追加しました。	2024 年 6 月 24 日
AmazonWorkSpacesWebServiceRolePolicy - ポリシーを更新	WorkSpaces Secure Browser はポリシーを更新して、aws:RequestTag/WorkSpacesWebManaged: true でタグ付け CreateNetworkInterface するように制限し、サブネットとセキュリティグループのリソー	2022 年 12 月 15 日

変更	説明	日付
	スに対してアクションを実行し、aws:ResourceTag/WorkSpacesWebManaged: true でタグ付けされた ENIs DeleteNetworkInterface に制限しました。	
AmazonWorkSpacesWebReadOnly - ポリシーを更新	WorkSpaces Secure Browser は、ユーザーアクセスのログ記録と Kinesis データストリームの一覧表示のための読み取りアクセス許可を含めるようにポリシーを更新しました。詳細については、「the section called “ユーザーアクセスロギングをセットアップする”」を参照してください。	2022 年 11 月 2 日
AmazonWorkSpacesWebServiceRolePolicy - ポリシーを更新	WorkSpaces Secure Browser は、ポリシーを更新して Kinesis データストリームの概要を記述し、ユーザーアクセスのログ記録のためにレコードを Kinesis データストリームに配置しました。詳細については、「the section called “ユーザーアクセスロギングをセットアップする”」を参照してください。	2022 年 10 月 17 日
AmazonWorkSpacesWebServiceRolePolicy - ポリシーを更新	WorkSpaces Secure Browser は、ENI の作成時にタグを作成するようにポリシーを更新しました。	2022 年 9 月 6 日

変更	説明	日付
AmazonWorkSpacesWebServiceRolePolicy - ポリシーを更新	WorkSpaces Secure Browser は、AWS/Usage 名前空間を PutMetricData API アクセス許可に追加するようにポリシーを更新しました。	2022 年 4 月 6 日
AmazonWorkSpacesWebReadOnly - 新しいポリシー	WorkSpaces Secure Browser は、AWS マネジメントコンソール、SDK、および CLI を介して WorkSpaces Secure Browser とその依存関係への読み取り専用アクセスを提供する新しいポリシーを追加しました。	2021 年 11 月 30 日
AmazonWorkSpacesWebServiceRolePolicy - 新しいポリシー	WorkSpaces Secure Browser は、 WorkSpaces Secure Browser が使用または管理する AWS のサービスとリソースへのアクセスを許可する新しいポリシーを追加しました。	2021 年 11 月 30 日
WorkSpaces Secure Browser が変更の追跡を開始しました	WorkSpaces Secure Browser が AWS マネージドポリシーの変更の追跡を開始しました。	2021 年 11 月 30 日

Amazon WorkSpaces Secure Browser のアイデンティティとアクセスのトラブルシューティング

次の情報は、 WorkSpaces Secure Browser と の使用時に発生する可能性がある一般的な問題の診断と修正に役立ちますIAM。

トピック

- WorkSpaces Secure Browser でアクションを実行する権限がない
- iam を実行する権限がありません。PassRole
- AWS アカウント外のユーザーに WorkSpaces Secure Browser リソースへのアクセスを許可したい

WorkSpaces Secure Browser でアクションを実行する権限がない

「I am not authorized to perform an action in Amazon Bedrock」というエラーが表示された場合、そのアクションを実行できるようにポリシーを更新する必要があります。

次の例のエラーは、mateojacksonIAMユーザーが コンソールを使用して架空の*my-example-widget*リソースの詳細を表示しようとしているが、架空のworkspaces-web:*GetWidget*アクセス許可がない場合に発生します。

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

この場合、workspaces-web:*GetWidget* アクションを使用して *my-example-widget*リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

iam を実行する権限がありません。PassRole

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して Secure Browser WorkSpaces にロールを渡すことができるようにする必要があります。

一部の AWS サービス では、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

次の例のエラーは、 というIAMユーザーがコンソールを使用して WorkSpaces Secure Browser marymajor でアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

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

この場合、Mary のポリシーを更新してメアリーに `iam:PassRole` アクションの実行を許可する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

AWS アカウント外のユーザーに WorkSpaces Secure Browser リソースへのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACLs) をサポートするサービスでは、これらのポリシーを使用して、ユーザーにリソースへのアクセスを許可できます。

詳細については、以下を参照してください。

- WorkSpaces Secure Browser がこれらの機能をサポートしているかどうかを確認するには、「」を参照してくださいAmazon WorkSpaces Secure Browser と の連携方法 IAM。
- 所有している のリソースへのアクセスを提供する方法については、 AWS アカウント 「 ユーザーガイド」の「所有 AWS アカウント している別の のIAMユーザーへのアクセスを提供するIAM」を参照してください。
- リソースへのアクセスをサードパーティー に提供する方法については AWS アカウント、 IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを通じてアクセスを提供する方法については、 IAMユーザーガイドの「外部認証されたユーザーへのアクセスの提供 (ID フェデレーション)」を参照してください。
- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いについては、「 ユーザーガイド」の「 でのクロスアカウントリソースアクセスIAMIAM」を参照してください。

WorkSpaces Secure Browser のサービスにリンクされたロールの使用

Amazon WorkSpaces Secure Browser は AWS Identity and Access Management 、 (IAM) サービスにリンクされたロール を使用します。サービスにリンクされたロールは、 WorkSpaces Secure Browser に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは、WorkSpaces Secure Browser によって事前定義されており、サービスがユーザーに代わって他の AWS のサービスを呼び出すために必要なすべてのアクセス許可が含まれています。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がないため、 WorkSpaces Secure Browser の設定が簡単になります。 WorkSpaces Secure Browser は、サービスにリンクされたロールのアクセス許可を定義します。特に定義されている場合を除き、Secure Browser WorkSpaces のみがそのロールを引き受けることができます。定義された許可には、信頼ポリシーとアクセス許可ポリシーが含まれます。アクセス許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスリンクロールを削除するには、まずその関連リソースを削除します。これにより、リソースにアクセスするためのアクセス許可を誤って削除することがないため、 WorkSpaces Secure Browser リソースが保護されます。

サービスリンクロールをサポートする他のサービスについては、「IAM と連携するAWS のサービス」を参照して、[サービスリンクロール] 列が [はい] のサービスを探してください。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[はい] リンクを選択します。

WorkSpaces Secure Browser のサービスにリンクされたロールのアクセス許可

WorkSpaces Secure Browser は、 という名前のサービスにリンクされたロールを使用しますAWSServiceRoleForAmazonWorkSpacesWeb。 WorkSpaces Secure Browser は、このサービスにリンクされたロールを使用して、カスタマーアカウントの Amazon EC2 リソースにアクセスし、インスタンスと CloudWatch メトリクスをストリーミングします。

AWSServiceRoleForAmazonWorkSpacesWeb サービスにリンクされたロールは、ロールの引き受けについて以下のサービスを信頼します。

- workspaces-web.amazonaws.com

という名前のロールアクセス許可ポリシーAmazonWorkSpacesWebServiceRolePolicyにより、WorkSpaces Secure Browser は指定されたリソースに対して次のアクションを実行できます。詳細については、「the section called “AmazonWorkSpacesWebServiceRolePolicy”」を参照してください。

- アクション: all AWS resources 上で ec2:DescribeVpcs
- アクション: all AWS resources 上で ec2:DescribeSubnets
- アクション: all AWS resources 上で ec2:DescribeAvailabilityZones
- アクション: サブネットリソースとセキュリティグループリソース上の ec2:CreateNetworkInterface で aws:RequestTag/WorkSpacesWebManaged: true
- アクション: all AWS resources 上で ec2:DescribeNetworkInterfaces

- アクション: aws:ResourceTag/WorkSpacesWebManaged: true とのネットワークインターフェースで ec2:DeleteNetworkInterface
- アクション: all AWS resources 上で ec2:DescribeSubnets
- アクション: all AWS resources 上で ec2:AssociateAddress
- アクション: all AWS resources 上で ec2:DisassociateAddress
- アクション: all AWS resources 上で ec2:DescribeRouteTables
- アクション: all AWS resources 上で ec2:DescribeSecurityGroups
- アクション: all AWS resources 上で ec2:DescribeVpcEndpoints
- アクション: aws:TagKeys: ["WorkSpacesWebManaged"] を使った ec2:CreateNetworkInterface オペレーションでの ec2:CreateTags
- アクション: all AWS resources 上で cloudwatch:PutMetricData
- アクション: 名前が amazon-workspaces-web- で始まる Kinesis データストリーム上で kinesis:PutRecord
- アクション: 名前が amazon-workspaces-web- で始まる Kinesis データストリーム上で kinesis:PutRecords
- アクション: 名前が amazon-workspaces-web- で始まる Kinesis データストリーム上で kinesis:DescribeStreamSummary

サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、アクセス許可を設定する必要があります。詳細については、「IAM ユーザーガイド」の「サービスリンクロール権限」を参照してください。

WorkSpaces Secure Browser のサービスにリンクされたロールの作成

サービスリンクロールを手動で作成する必要はありません。、 AWS Management Console、 AWS CLIまたは AWS API で最初のポータルを作成すると、 WorkSpaces Secure Browser によってサービスにリンクされたロールが作成されます。

> **Important**
>
> このサービスリンクロールは、このロールでサポートされている機能を使用する別のサービスでアクションが完了した場合にアカウントに表示されます。

このサービスリンクロールを削除した後に、そのロールを再作成する必要がある場合は、同じプロセスを使用してアカウントでロールを再作成することができます。最初のポータルを作成すると、WorkSpaces Secure Browser によってサービスにリンクされたロールが再度作成されます。

IAM コンソールを使用して、WorkSpaces Secure Browser ユースケースでサービスにリンクされたロールを作成することもできます。 AWS CLI または AWS API で、サービス名を使用してworkspaces-web.amazonaws.comサービスにリンクされたロールを作成します。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの作成」を参照してください。このサービスリンクロールを削除しても、同じ方法でロールを再作成できます。

WorkSpaces Secure Browser のサービスにリンクされたロールの編集

WorkSpaces Secure Browser では、AWSServiceRoleForAmazonWorkSpacesWebサービスにリンクされたロールを編集することはできません。サービスリンクロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロール記述の編集はできます。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの編集」を参照してください。

WorkSpaces Secure Browser のサービスにリンクされたロールの削除

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、積極的にモニタリングまたは保守されていない未使用のエンティティを排除できます。ただし、手動で削除する前に、サービスリンクロールのリソースをクリーンアップする必要があります。

> **Note**
>
> リソースを削除しようとしたときに WorkSpaces Secure Browser サービスがロールを使用している場合、削除が失敗する可能性があります。失敗した場合は、数分待ってから操作を再試行してください。

で使用される WorkSpaces Secure Browser リソースを削除するには AWSServiceRoleForAmazonWorkSpacesWeb

- 以下のオプションから 1 つ選択してください。
  - コンソールを使用する場合は、コンソール上のポータルをすべて削除してください。

- CLI または API を使用する場合は、すべてのリソース (ブラウザ設定、ネットワーク設定、ユーザー設定、信頼ストア、ユーザーアクセスロギング設定を含む) をポータルから切り離し、これらのリソースを削除してからポータルを削除します。

サービスにリンクされたロールを IAM で手動削除するには

IAM コンソール、、または AWS API を使用して AWS CLI、サービスにリンクされたロールを削除します AWSServiceRoleForAmazonWorkSpacesWeb。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの削除」を参照してください。

WorkSpaces Secure Browser サービスにリンクされたロールでサポートされているリージョン

WorkSpaces Secure Browser は、サービスが利用可能なすべてのリージョンで、サービスにリンクされたロールの使用をサポートします。詳細については、「AWS リージョンとエンドポイント」を参照してください。

Amazon WorkSpaces Secure Browser でのインシデント対応

`SessionFailure` Amazon CloudWatch メトリクスをモニタリングすることで、インシデントを検出できます。インシデントのアラートを受信するには、 `SessionFailure` メトリクスの CloudWatch アラームを使用します。詳細については、「Amazon による Amazon WorkSpaces Secure Browser のモニタリング CloudWatch」を参照してください。

Amazon WorkSpaces Secure Browser のコンプライアンス検証

AWS サービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、コンプライアンスプログラムAWS サービス による対象範囲内のコンプライアンスプログラムを参照し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS「コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「 でのレポートのダウンロード AWS Artifact」の」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS サービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 は、コンプライアンスに役立つ以下のリソース AWS を提供しています。

- セキュリティとコンプライアンスのクイックスタートガイド – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境 AWS を にデプロイする手順について説明します。
- アマゾン ウェブ サービスHIPAAのセキュリティとコンプライアンスのためのアーキテクチャ – このホワイトペーパーでは、企業が AWS を使用して HIPAA対象アプリケーションを作成する方法について説明します。

> **Note**
>
> すべての AWS サービス がHIPAA対象となるわけではありません。詳細については、HIPAA「対象サービスリファレンス」を参照してください。

- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS カスタマーコンプライアンスガイド — コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、ガイダンスを保護し AWS サービス 、複数のフレームワーク (米国国立標準技術研究所 (NIST) 、Payment Card Industry Security Standards Council ()、PCI国際標準化機構 (ISO) など) のセキュリティコントロールにマッピングするためのベストプラクティスをまとめています。
- 「 デベロッパーガイド」の「 ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – これにより AWS サービス 、 内のセキュリティ状態を包括的に確認できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、Security Hub のコントロールリファレンスを参照してください。
- Amazon GuardDuty – これにより AWS アカウント、疑わしいアクティビティや悪意のあるアクティビティがないか環境を監視することで、、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS サービス を検出します。 GuardDuty は、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことでDSS、 PCI などのさまざまなコンプライアンス要件への対応に役立ちます。
- AWS Audit Manager – これにより AWS サービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

Amazon WorkSpaces Secure Browser の耐障害性

AWS グローバルインフラストラクチャは、 AWS リージョン およびアベイラビリティーゾーンを中心に構築されています。 は、低レイテンシー、高スループット、および高度に冗長なネットワークで接続された、物理的に分離および分離された複数のアベイラビリティーゾーン AWS リージョン を提供します。アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性が高く、フォールトトレラントで、スケーラブルです。

AWS リージョン およびアベイラビリティーゾーンの詳細については、AWS 「 グローバルインフラストラクチャ」を参照してください。

現在、 WorkSpaces Secure Browser では、以下の機能はサポートされていません。

- AZ またはリージョン間のコンテンツのバックアップ
- 暗号化されたバックアップ
- AZ 間またはリージョン間の転送中コンテンツの暗号化
- デフォルトバックアップまたは自動バックアップ

高いインターネット可用性を実現するように設定するには、VPC 設定を調整できます。API の可用性を高めるためには、適切な量の TPS をリクエストします。

Amazon WorkSpaces Secure Browser のインフラストラクチャセキュリティ

マネージドサービスである Amazon WorkSpaces Secure Browser は、 AWS グローバルネットワークセキュリティで保護されています。 AWS セキュリティサービスと がインフラストラクチャ AWS を保護する方法については、AWS 「 クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、「 Security Pillar AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

が AWS 公開したAPI呼び出しを使用して、ネットワーク経由で Amazon WorkSpaces Secure Browser にアクセスします。クライアントは以下をサポートする必要があります:

- Transport Layer Security (TLS) 。1TLS.2 が必要で、1.3 TLS をお勧めします。

- (Ephemeral Diffie-HellmanPFS) や DHE (Elliptic Curve Ephemeral Diffie-Hellman) などの完全前方秘匿性 ECDHE () を備えた暗号スイート。これらのモードは、Java 7 以降など、ほとんどの最新システムでサポートされています。

さらに、リクエストは、アクセスキー ID とプリンIAMシパルに関連付けられたシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token Service (AWS STS) を使用して、一時セキュリティ認証情報を生成し、リクエストに署名することもできます。

WorkSpaces Secure Browser は、すべてのサービスに標準 AWS SigV4 認証と認可を適用することで、サービストラフィックを分離します。カスタマーリソースエンドポイント (またはウェブポータルエンドポイント) は ID プロバイダーによって保護されています。ID プロバイダー (IdP) の多要素認証やその他のセキュリティメカニズムを使用することで、トラフィックをさらに分離できます。

、VPCサブネット、セキュリティグループなどのネットワーク設定を設定することで、すべてのインターネットアクセスを制御できます。マルチテナンシーとVPCエンドポイント (PrivateLink) は現在サポートされていません。

Amazon WorkSpaces Secure Browser での設定と脆弱性の分析

WorkSpaces Secure Browser は、Chrome や Linux など、ユーザーに代わって必要に応じてアプリケーションやプラットフォームを更新およびパッチ適用します。パッチや再構築は不要です。ただし、仕様とガイドラインに従って WorkSpaces Secure Browser を設定し、ユーザーによる Secure Browser WorkSpaces の使用状況をモニタリングするのはユーザーの責任です。サービス関連の設定と脆弱性分析はすべて WorkSpaces 、Secure Browser の責任です。

ウェブポータルの数やユーザー数など、 WorkSpaces Secure Browser リソースの制限の引き上げをリクエストできます。 WorkSpaces Secure Browser は、サービスと SLA の可用性を保証します。

Amazon WorkSpaces Secure Browser のセキュリティのベストプラクティス

Amazon WorkSpaces Secure Browser には、独自のセキュリティポリシーを開発および実装する際に使用できるさまざまなセキュリティ機能が用意されています。以下のベストプラクティスは一般的なガイドラインであり、完全なセキュリティソリューションを説明するものではありません。これらのベストプラクティスはお客様の環境に必ずしも適切または十分でない可能性があるので、処方箋ではなく、あくまで有用な考慮事項とお考えください。

Amazon WorkSpaces Secure Browser のベストプラクティスは次のとおりです。

- WorkSpaces Secure Browser の使用に関連する潜在的なセキュリティイベントを検出するには、または Amazon CloudWatch を使用して AWS CloudTrail アクセス履歴を検出して追跡し、ログを処理します。詳細については、「Amazon による Amazon WorkSpaces Secure Browser のモニタリング CloudWatch」および「を使用した WorkSpaces Secure Browser API コールのログ記録 AWS CloudTrail」を参照してください。
- 検出コントロールを実装し、異常を特定するには、 CloudTrail ログと CloudWatchメトリクスを使用します。詳細については、「Amazon による Amazon WorkSpaces Secure Browser のモニタリング CloudWatch」および「を使用した WorkSpaces Secure Browser API コールのログ記録 AWS CloudTrail」を参照してください。
- ユーザーアクセスロギングを設定して、ユーザーイベントを記録できます。詳細については、「the section called “ユーザーアクセスロギングをセットアップする”」を参照してください。

WorkSpaces Secure Browser の使用に関連する潜在的なセキュリティイベントを防ぐには、以下のベストプラクティスに従ってください。

- 最小特権アクセスを実装し、 WorkSpaces Secure Browser アクションに使用する特定のロールを作成します。IAM テンプレートを使用して、フルアクセスまたは読み取り専用ロールを作成します。詳細については、「AWS WorkSpaces Secure Browser の マネージドポリシー」を参照してください。
- ポータルのドメインとユーザー認証情報を共有する場合は注意が必要です。インターネット上の誰でもウェブポータルにアクセスできますが、ポータルへの有効なユーザー認証情報がないとセッションを開始できません。ウェブポータルの認証情報をどのように、いつ、誰と共有するかには注意が必要です。

Amazon WorkSpaces Secure Browser のモニタリング

モニタリングは、Amazon WorkSpaces Secure Browser およびその他の AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。 は、 WorkSpaces Secure Browser ポータルとそのリソースを監視し、問題が発生した場合に報告し、必要に応じて自動アクションを実行するために、以下のモニタリングツール AWS を提供します。

- Amazon CloudWatch は、 AWS リソースと で実行しているアプリケーションを AWS リアルタイムでモニタリングします。メトリクスの収集と追跡、カスタマイズしたダッシュボードの作成、および指定したメトリクスが指定されたしきい値に達したときに通知またはアクションを実行するアラームの設定を行うことができます。例えば、 で Amazon EC2 インスタンスの CPU 使用率やその他のメトリクス CloudWatch を追跡し、必要に応じて新しいインスタンスを自動的に起動できます。詳細については、「Amazon ユーザーガイド CloudWatch 」を参照してください。
- Amazon CloudWatch Logs を使用すると、Amazon EC2 インスタンスやその他のソースからログファイルをモニタリング、保存 CloudTrail、アクセスできます。 CloudWatch Logs はログファイル内の情報をモニタリングし、特定のしきい値に達したときに通知できます。高い耐久性を備えたストレージにログデータをアーカイブすることもできます。詳細については、「Amazon CloudWatch Logs ユーザーガイド」を参照してください。
- AWS CloudTrail は、 AWS アカウントによって、またはアカウントに代わって行われた API コールおよび関連イベントをキャプチャし、指定した Amazon S3 バケットにログファイルを配信します。を呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、呼び出しが発生した日時を特定できます。詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

トピック

- Amazon による Amazon WorkSpaces Secure Browser のモニタリング CloudWatch
- を使用した WorkSpaces Secure Browser API コールのログ記録 AWS CloudTrail
- ユーザーアクセスロギング

Amazon による Amazon WorkSpaces Secure Browser のモニタリング CloudWatch

を使用して Amazon WorkSpaces Secure Browser をモニタリングすることで CloudWatch、raw データを収集し、読み取り可能なほぼリアルタイムのメトリクスに加工できます。これらの統計は

15 か月間保持されるため、履歴情報にアクセスし、ウェブアプリケーションまたはサービスの動作をより的確に把握できます。また、特定のしきい値を監視するアラームを設定し、これらのしきい値に達したときに通知を送信したりアクションを実行したりできます。詳細については、「Amazon ユーザーガイド CloudWatch 」を参照してください。

AWS/WorkSpacesWeb 名前空間には、次のメトリクスが含まれます。

CloudWatch Amazon WorkSpaces Secure Browser の メトリクス

メトリクス	説明	ディメンション	統計	単位
SessionAttempt	Amazon WorkSpaces Secure Browser セッションの試行回数。	PortalId	Average、Sum、Maximum、Minimum	カウント
SessionSuccess	成功した Amazon WorkSpaces Secure Browser セッションの開始回数。	PortalId	Average、Sum、Maximum、Minimum	カウント
SessionFailure	失敗した Amazon WorkSpaces Secure Browser セッションの開始回数。	PortalId	Average、Sum、Maximum、Minimum	カウント
GlobalCpuPercent	Amazon WorkSpaces Secure Browser セッションインスタンスの CPU 使用率。	PortalId	Average、Sum、Maximum、Minimum	割合 (%)

メトリクス	説明	ディメンション	統計	単位
GlobalMemoryPercent	Amazon WorkSpaces Secure Browser セッションインスタンスのメモリ (RAM) 使用量。	PortalId	Average、Sum、Maximum、Minimum	割合 (%)

> **Note**
>
> GlobalCpuPercent または のSampleCount「」メトリクス統計を表示GlobalMemoryPercentして、ポータルでアクティブな同時セッションの数を判断できます。データポイントは、各セッションによって 1 分に 1 回出力されます。

を使用した WorkSpaces Secure Browser API コールのログ記録 AWS CloudTrail

WorkSpaces Secure Browser は AWS CloudTrail、Amazon WorkSpaces Secure Browser のユーザー、ロール、または サービスによって実行されたアクションを記録する AWS サービスである と統合されています。 は、Amazon Secure Browser のすべての API WorkSpaces コールをイベントとして CloudTrail キャプチャします。これには、Amazon WorkSpaces Secure Browser コンソールからの呼び出しと、Amazon WorkSpaces Secure Browser API オペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、Amazon WorkSpaces Secure Browser の CloudTrail イベントなど、Amazon S3 バケットへのイベントの継続的な配信を有効にすることができます。 Amazon S3 証跡を設定しない場合でも、 CloudTrail コンソールのイベント履歴 で最新のイベントを表示できます。で収集された情報を使用して CloudTrail、Amazon WorkSpaces Secure Browser に対して行われたリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

の詳細については CloudTrail、「 AWS CloudTrail ユーザーガイド」を参照してください。

WorkSpaces でブラウザ情報を保護する CloudTrail

CloudTrail AWS アカウントを作成すると、 がアカウントで有効になります。Amazon WorkSpaces Secure Browser でアクティビティが発生すると、そのアクティビティは CloudTrail イベント履歴 の他の AWS サービスイベントとともにイベントに記録されます。イベント履歴 では、 AWS アカウント内の最近のイベントを表示、検索、ダウンロードできます。詳細については、「イベント履歴 で CloudTrail イベントを表示する」を参照してください。

Amazon WorkSpaces Secure Browser のイベントなど、 AWS アカウント内のイベントの継続的な記録については、証跡を作成できます。証跡により CloudTrail 、 はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成すると、すべての AWSリージョンに証跡が適用されます。証跡は、 AWS パーティション内のすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、 CloudTrail ログで収集されたイベントデータをより詳細に分析し、それに基づいて行動するように、他の AWS サービスを設定できます。詳細については、次を参照してください:

- 「証跡作成の概要」
- CloudTrail がサポートするサービスと統合
- の Amazon SNS 通知の設定 CloudTrail
- 複数のリージョンからの CloudTrail ログファイルの受信と複数のアカウントからの CloudTrail ログファイルの受信

すべての Amazon WorkSpaces Secure Browser アクションは によってログに記録 CloudTrail され、Amazon WorkSpaces API リファレンス に記載されています。例えば、、、および `ListBrowserSettings`アクションを呼び出す`DeleteUserSettings`と`CreatePortal`、CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。同一性情報は次の判断に役立ちます。

- リクエストが、ルートと IAM ユーザー認証情報のどちらを使用して送信されたか。
- リクエストがロールまたはフェデレーションユーザーの一時的なセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の AWS サービスによって行われたかどうか。

詳細については、CloudTrail userIdentity 要素」を参照してください。

WorkSpaces Secure Browser ログファイルエントリについて

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信できるようにする設定です。 CloudTrail ログファイルには 1 つ以上のログエントリが含まれます。イベントは任意のソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータ、およびその他の details. CloudTrail log ファイルはパブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

次の例は、 `ListBrowserSettings`アクションを示す CloudTrail ログエントリを示しています。


```
{
   "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"
    }]
}
```


ユーザーアクセスロギング

Amazon WorkSpaces Secure Browser を使用すると、お客様は開始、停止、URL 訪問などのセッションイベントを記録できます。これらのログは、ウェブポータルに指定した Amazon Kinesis Data Streams に配信されます。詳細については、「the section called “ユーザーアクセスロギングをセットアップする”」を参照してください。

WorkSpaces Secure Browser ユーザー向けのガイダンス

管理者は WorkSpaces Secure Browser を使用して、内部ウェブサイト、 software-as-a-service (SAAS) ウェブアプリケーション、インターネットなどの企業ウェブサイトに接続するウェブポータルを作成します。エンドユーザーは、セッションを開始してコンテンツにアクセスするために、既存のウェブブラウザを使用してこれらのウェブポータルにアクセスします。

以下のコンテンツは、 WorkSpaces Secure Browser へのアクセス、セッションの起動と設定、ツールバーとウェブブラウザの使用についてさらに詳しく知りたいエンドユーザーのガイドに役立ちます。

トピック

ブラウザとデバイスの互換性

Amazon WorkSpaces Secure Browser は、ウェブブラウザ内で実行される NICE DCV ウェブブラウザクライアントを使用するため、インストールは必要ありません。ウェブブラウザクライアントは、Chrome や Firefox などのウェブブラウザや、Windows、macOS、Linux などのデスクトップオペレーティングシステムに対応しています。

ウェブブラウザクライアントのサポート up-to-date の詳細については、「ウェブブラウザクライアント」を参照してください。

> **Note**
>
> ウェブカメラは現在、Google Chrome や Microsoft Edge などの Chromium ベースのブラウザでのみサポートされています。現在、Apple Safari と Mozilla FireFox はウェブカメラをサポートしていません。

ウェブポータルアクセス

管理者は以下のオプションでウェブポータルへのアクセスを提供できます。

- メールまたはウェブサイトからリンクを選択し、SAML ID 認証情報を使用してサインインできます。
- SAML ID プロバイダー (Okta、Ping、Azure など) にサインインし、SAML プロバイダーのアプリケーションホームページ (Okta エンドユーザーダッシュボードや Azure Myapps ポータルなど) からワンクリックでセッションを開始できます。

セッションガイダンス

ウェブポータルにサインインすると、セッションを開始して、セッション中にさまざまなアクションを実行できます。

トピック

セッションを開始する

ログインしてセッションを開始すると、[セッションを開始しています] というメッセージと進行状況バーが表示されます。これは、Amazon WorkSpaces Secure Browser がユーザーに代わってセッションを作成していることを示します。バックグラウンドで、Amazon WorkSpaces Secure Browser はインスタンスを作成し、マネージドウェブブラウザを起動し、管理者設定とブラウザポリシーを適用しています。

ウェブポータルに初めてサインインする場合、ツールバーに青い [+] アイコンが表示されます。このアイコンは、ツールバーの利用可能な機能を説明するチュートリアルが存在することを示しています。これらのアイコンを使うと、以下の方法を学ぶことができます。

- マイク、ウェブカメラ、クリップボードに対してブラウザのアクセス許可を与えるには、ローカルブラウザの横にあるロックアイコンを選択し、クリップボード、マイク、カメラの横にあるスイッチを [オン] に設定します。

> **Note**
>
> 最初のセッションの開始時にウェブカメラのアクセス許可を有効にすると、ウェブカメラは短時間有効になり、コンピュータのライトが点滅します。これにより、ローカルブラウザからウェブカメラへのアクセスが許可されます。

- ブラウザのロックアイコンを選択し、「ポップアップを常に許可する」を設定することで、Amazon WorkSpaces Secure Browser が追加のモニターウィンドウを起動できるようにします。

チュートリアルを再開したい場合は、ツールバーの [プロファイル]、[ヘルプ]、[チュートリアルを開始] を選択できます。

ツールバーを使用する

ツールバーを移動するには、ツールバーの上部にある明るい色のバーを選択し、目的の場所にドラッグしてから離してドロップします。

ツールバーを折りたたむには、ツールバーにカーソルを合わせ、上矢印ボタンを選択するか、上部のセクションにある明るいバーをダブルクリックします。折りたたんだビューでは画面のスペースが広がり、よく使用するアイコンにワンクリックでアクセスできます。

ディスプレイのサイズを増やすには、ブラウザウィンドウを選択してズームインします。ツールバーのアイコンとテキストの表示サイズを増やすには、ツールバーを選択してズームインします。

Windows デバイスでズームインまたはズームアウトするには、次の手順に従います。

1. ツールバーまたはウェブコンテンツを選択します。
2. Ctrl + + を押してズームインするか、Ctrl + - を押してズームアウトします。

Mac デバイスでズームインまたはズームアウトするには、次の手順に従います。

1. ツールバーまたはウェブコンテンツを選択します。
2. Cmd + + を押してズームインするか、Cmd + - を押してズームアウトします。

ツールバーを画面の上部にドッキングするには、ツールバーモード で 設定 、一般 、ドッキング を選択します。

以下の表には、ツールバーで使用できるすべてのアイコンの説明が含まれています。

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

> **Note**
>
> クリップボードアイコンとファイルアイコンは、管理者がこれらにアクセス許可を付与しない限り、デフォルトでは非表示になっています。ウェブポータル上のクリップボードとファイルを有効または無効にできるのは管理者だけです。これらのアイコンが非表示になっており、アクセスする必要がある場合は、管理者に連絡してください。

ブラウザを使用する

セッションを開始すると、管理者が選択した URL であるスタートアップURL がブラウザに表示されます。管理者がスタートアップ URL を選択していない場合は、Google Chrome のデフォルトの新しいタブエクスペリエンスが表示されます。

ブラウザでは、タブを開いたり、(Windows ツールバーアイコンまたはブラウザの 3 ドットメニューから) 別のブラウザウィンドウを開始したり、URL バーに URL を入力するか、または検索したり、管理されたブックマークからウェブサイトにアクセスすることができます。ウェブポータルのブックマークにアクセスするには、ブックマークバー (URL バーの下) の [マネージドブックマーク] フォルダーを開くか、URL バーの右側にある 3 ドットメニューからブックマークマネージャーを開きます。

ブラウザウィンドウのサイズを変更または移動するには、Chrome タブストリップを下にドラッグします。これにより、セッション中に複数のブラウザウィンドウの画面スペースを増やすことができます。

> **Note**
>
> シークレットモードなどのブラウザ機能は、管理者が無効にしていると、セッション中は使用できない場合があります。

セッションを終了する

セッションを終了するには、[プロフィール] と [セッションの終了] を選択します。セッションが終了すると、Amazon WorkSpaces Secure Browser はセッションからすべてのデータを削除します。セッションが終了すると、開いているウェブサイトや履歴などのブラウザデータ、または File Explorer からのファイルやデータは使用できなくなります。

アクティブなセッション中にタブを閉じた場合、管理者が設定した時間が経過するとセッションが終了します。このタイムアウトが有効になる前にタブを閉じてウェブポータルに再度アクセスすると、現在のセッションに参加して、開いているウェブサイトやファイルなど、以前のセッションデータをすべて表示できます。

トラブルシューティング

Amazon WorkSpaces Secure Browser ポータルではサインインできません。「ウェブポータルはまだ設定されていません。貴社の IT 管理者にお問い合わせください。」というエラーメッセージが表示されました。

ユーザーがサインインできるようにするには、管理者が SAML 2.0 ID プロバイダーを使用してポータルの作成を完了する必要があります。対処方法については、貴社の 管理者に問い合わせてください。

ポータルがセッションを開始できません。「セッションを予約できませんでした。内部エラーが発生しました。もう一度試してください。」というエラーメッセージが表示されました。

ウェブポータルセッションの開始に発生しました。セッションをもう一度開始してみてください。問題が解決しない場合は、管理者にお問い合わせください。

クリップボード、マイク、ウェブカメラを使えません。

ブラウザのアクセス許可を与えるには、URL の横にあるロックアイコンを選択し、[クリップボード]、[マイク]、[カメラ]、[ポップアップとリダイレクト] の横にある青色のスイッチを切り替えて、これらの機能を有効にしてください。

> **Note**
>
> ウェブブラウザがビデオまたはオーディオからの入力をサポートしていない場合、これらのオプションはツールバーに表示されません。

Amazon WorkSpaces Secure Browser のリアルタイムオーディオビデオ (AV) は、ローカルウェブカメラのビデオとマイクのオーディオ入力をブラウザストリーミングセッションにリダイレクトします。これにより、Google Chrome や Microsoft Edge などの Chromium ベースのウェブブラウザを使用して、ストリーミングセッション内で、ローカルデバイスを使用したビデオ会議や音声会議を行うことができます。ウェブカメラは Chromium 以外のブラウザでは現在サポートされていません。

Google Chrome の設定方法の詳細については、「カメラとマイクを使用する」を参照してください。

ウェブポータルで追加のモニターウィンドウが開始されません。

デュアルモニターを起動しようとして、上部ブラウザのアドレスバーの端にポップアップブロックアイコンが表示されている場合は、そのアイコンを選択し、[ポップアップとリダイレクトを常に許可する] の横にあるラジオボタンを選択します。ポップアップが許可されたら、ツールバーのデュアルモニターアイコンを選択して新しいウィンドウを起動し、モニター上のウィンドウの位置を変更して、ブラウザタブをウィンドウにドラッグします。

[ファイル] ペインからファイルをダウンロードしようとしても、何も起こりません。

[ファイル] ペインからファイルをダウンロードしようとして、上部ブラウザのアドレスバーの端にポップアップブロックアイコンが表示されている場合は、そのアイコンを選択し、[ポップアップとリダイレクトを常に許可する] の横にあるラジオボタンを選択します。ポップアップが許可されたら、ファイルをもう一度ダウンロードしてみます。

シングルサインオンの拡張機能

Amazon WorkSpaces Secure Browser は、デスクトップコンピュータで Chrome および Firefox ブラウザを使用したシングルサインオン用の拡張機能を提供します。管理者が拡張機能を有効にしている場合、ログイン時にウェブポータルから拡張機能のインストールを求められます。

Amazon WorkSpaces Secure Browser は、セッション中にウェブサイトへのシングルサインオンを有効にする拡張機能を構築しました。例えば、SAML 2.0 ID プロバイダー (Okta や Ping など) を使用してウェブポータルにサインインし、セッション中に同じ ID プロバイダーを使用するウェブサイトにアクセスした場合、拡張機能によって追加のサインインプロンプトが削除され、ウェブサイトにアクセスしやすくなります。

ウェブポータルにアクセスするために拡張機能をインストールする必要はありませんが、ユーザー名とパスワードの入力を求める回数が減るため、使いやすくなります。

ログインすると、管理者がセッションに対してリストした Cookie が拡張機能によって検索されます。拡張機能が検索するデータはすべて、保存中および転送中に暗号化されます。このデータはいずれもローカルブラウザには保存されません。セッションを終了すると、セッションデータ (開いているタブ、ダウンロードしたファイル、セッション中に配信または作成された Cookie など) はすべて削除されます。

互換性

この拡張機能は以下のデバイスで動作します。

- ノートパソコン
- デスクトップコンピュータ

この拡張機能は以下のブラウザで動作します。

- Chrome
- Firefox

インストール

ポータルにサインインしたら、プロンプトに従って Chrome または Firefox ブラウザの拡張機能をインストールします。この操作は、ウェブブラウザごとに 1 回だけ行う必要があります。

デバイスを切り替えたり、同じデバイスで別のブラウザに切り替えたり、ローカルブラウザから拡張機能を削除したりすると、次のセッションを開始したときに拡張機能をインストールするように求めるメッセージが表示されます。

拡張機能が期待どおりに動作するようにするには、Incognito (Chrome) または Private Browsing (Firefox) の代わりに、通常のブラウジングウィンドウで拡張機能を使用します。

トラブルシューティング

拡張機能をインストールしているのにセッション中にログインを求められる場合は、以下の手順に従ってください。

1. Amazon WorkSpaces Secure Browser 拡張機能がブラウザにインストールされていることを確認します。ブラウザデータを削除した場合、その拡張機能を誤って削除した可能性があります。
2. シークレット (Chrome) やプライベートブラウジング (Firefox) ではないことを確認してください。これらのモードは拡張機能で問題を引き起こす可能性があります。
3. 問題が解決しない場合は、ポータル管理者に問い合わせてください。

Amazon WorkSpaces Secure Browser 管理ガイドのドキュメント履歴

次の表に、Amazon WorkSpaces Secure Browser のドキュメントリリースを示します。

変更	説明	日付
ディープリンクを許可する	ポータルがセッション中にユーザーを特定のウェブサイトに接続するディープリンクを受信できるようにします。	2024 年 6 月 25 日
マネージドポリシーの更新	AmazonWorkSpacesSecureBrowserReadOnly 管理ポリシーを追加	2024 年 6 月 24 日
ツールバーを使用してズームする	ツールバーを使用すると、表示、アイコン、テキストのサイズを増やすことができます。	2024 年 5 月 1 日
新しいウェブポータル設定	ウェブポータルのインスタンスタイプと最大同時ユーザー制限を指定できるようになりました。	2024 年 4 月 22 日
CloudWatch メトリクス	GlobalCpuPercent および GlobalMemoryPercent メトリクスを追加しました。	2024 年 2 月 26 日
URL フィルタリングを設定する	Chrome ポリシーを使用して、ユーザーがリモートブラウザからアクセスできる URLs をフィルタリングできます。	2024 年 2 月 21 日

IdP 認証タイプ	標準または IAM Identity Center 認証タイプを選択できます。	2024 年 2 月 5 日
シングルサインオンの拡張機能を有効にする	エンドユーザーがポータルのサインオンをより快適に行えるように、拡張機能を有効にできます。	2023 年 8 月 28 日
Amazon WorkSpaces Secure Browser のユーザーガイダンス	Amazon WorkSpaces Secure Browser へのアクセス、セッションの起動と設定、ツールバーとウェブブラウザの使用に関する詳細を知りたいエンドユーザー向けのガイドとなるコンテンツを追加しました。	2023 年 7 月 17 日
IP アクセスコントロール	WorkSpaces Secure Browser を使用すると、ウェブポータルにアクセスできる IP アドレスを制御できます。	2023 年 5 月 31 日
マネージドポリシーの更新	AmazonWorkSpacesWebReadOnly 管理ポリシーの更新	2023 年 5 月 15 日
ID プロバイダーの更新を設定する	WorkSpaces Secure Browser には、Standard と の 2 つの認証タイプがあります。 AWS IAM Identity Center	2023 年 3 月 15 日
ブラウザポリシーの更新	ブラウザポリシーセクションの更新と再構築	2023 年 1 月 31 日
マネージドポリシーの更新	AmazonWorkSpacesWebServiceRolePolicy 管理ポリシーの更新	2022 年 12 月 15 日

許可リストとブロックリスト	[許可リスト] と [ブロックリスト] を指定して、ユーザーがアクセスできる、またはアクセスできないドメインのリストを指定します。	2022 年 11 月 14 日
マネージドポリシーの更新	AmazonWorkSpacesWebReadOnly 管理ポリシーの更新	2022 年 11 月 2 日
マネージドポリシーの更新	AmazonWorkSpacesWebServiceRolePolicy 管理ポリシーの更新	2022 年 10 月 24 日
ユーザーアクセスロギング	ユーザーイベントを記録するユーザーアクセスロギングを設定します	2022 年 10 月 17 日
ネットワークの更新	「ネットワークとアクセス」セクションの各種更新	2022 年 9 月 22 日
マネージドポリシーの更新	AmazonWorkSpacesWebServiceRolePolicy 管理ポリシーの更新	2022 年 9 月 6 日
ユーザーセッションの構成	Input Method Editor (IME) とインセッションローカリゼーションを構成します	2022 年 7 月 28 日
ネットワークの更新	「ネットワークとアクセス」セクションの各種更新	2022 年 7 月 7 日
タイムアウト値	切断タイムアウトを分単位で指定し、アイドル切断タイムアウトを分単位で指定します。	2022 年 5 月 16 日

マネージドポリシーの更新	AmazonWorkSpacesWebServiceRolePolicy マネージドポリシーを更新して、AWS/Usage 名前空間を PutMetricData API アクセス許可に追加しました。	2022 年 4 月 6 日
サービスリンクロール	新しい AWSServiceRoleForAmazonWorkSpacesWeb サービスにリンクされたロール	2021 年 11 月 30 日
マネージドポリシー	新しい AmazonWorkSpacesWebReadOnly マネージドポリシー	2021 年 11 月 30 日
マネージドポリシー	新しい AmazonWorkSpacesWebServiceRolePolicy マネージドポリシー	2021 年 11 月 30 日
初回リリース	WorkSpaces Secure Browser 管理ガイドの初回リリース	2021 年 11 月 30 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。