aws

管理ガイド

Amazon WorkSpaces セキュアブラウザ

Amazon WorkSpaces セキュアブラウザ: 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 という名称でした。

Amazon WorkSpaces Secure Browser は、プライベートウェブサイトおよび 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、使い捨てコンテナからのインターネットの参照に使用される、フルマネージドのクラウドネイティブのホステッドブラウザサービスです。WorkSpaces Secure Browser は、IT 部門にアプライアンス、インフラストラクチャ、専用のクライアントソフトウェア、または仮想プライベートネットワーク (VPN) 接続の管理の負担をかけることなく、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流出のリスクを軽減します。HTML やドキュメントオブジェクトモデル (DOM)、機密性の高い企業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。

すべてのセッションで企業ブラウザポリシー (URL の許可/ブロックを含む) を適用でき、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も可能です。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 は設定や運用が容易です。各セッションは、最新のパッチが適用された最新の Chrome ブラウザで開始され、会社のポリシーと設定が適用されます。

Amazon WorkSpaces Secure Browser のリリース履歴

2024 年 5 月 20 日、Amazon WorkSpaces Web は Amazon WorkSpaces Secure Browser に名称が変更されました。既存のお客様の場合、このサービスを使用してユーザーやリソースを管理する方法に変更はありません。以下のリストでは、この名称変更に伴って行われた該当する更新について説明しています。

下位互換性のために、workspaces-web API 名前空間は変更されていません。その結果、以下のリソースは変更なく引き続き使用できます。

- CLI コマンド。
- Amazon CloudWatch メトリクス。詳細については、「the section called “CloudWatch によるモニタリング”」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 endpoints and quotas」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 resource type reference」を参照してください。
- workspaces-web を含むサービスリンクロール。詳細については、「the section called “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。
- Workspaces-web を含むコンソール URL。
- Workspaces-web を含むドキュメント URL。詳細については、Amazon WorkSpaces Secure Browser のドキュメントを参照してください。
- 既存の読み取り専用マネージドロール。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 グラント名。
- 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 URL は変更されません。2024 年 5 月 20 日より前に作成されたポータルの URL は <UUID>.workspaces-web.com の形式を使用していました。WorkSpaces Secure Browser ポータルは、引き続きこの形式と workspaces-web.com ドメインを使用します。

Amazon WorkSpaces Secure Browser を使用する際の基本用語

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。既存の IdP を設定して WorkSpaces Secure Browser と連携させることができます。

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。IdP 内のユーザーに WorkSpaces Secure Browser を使用するための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へ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)

既存または新しい VPC、対応するサブネット、セキュリティグループを使用して、社内コンテンツを WorkSpaces Secure Browser にリンクすることができます。

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 とサブネットが社内ウェブサイトや Software as a Service (SaaS) ウェブサイトへの安定した接続を備えている必要があります。

一覧表示される VPC、サブネット、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のものです。

信頼ストア

WorkSpaces Secure Browser 経由で Web サイトにアクセスしているユーザーが 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でウェブサイトを読み込む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、その証明書を信頼スト

アに追加して、ユーザーが WorkSpaces Secure Browser 内の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社内ウェブサイトや 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。

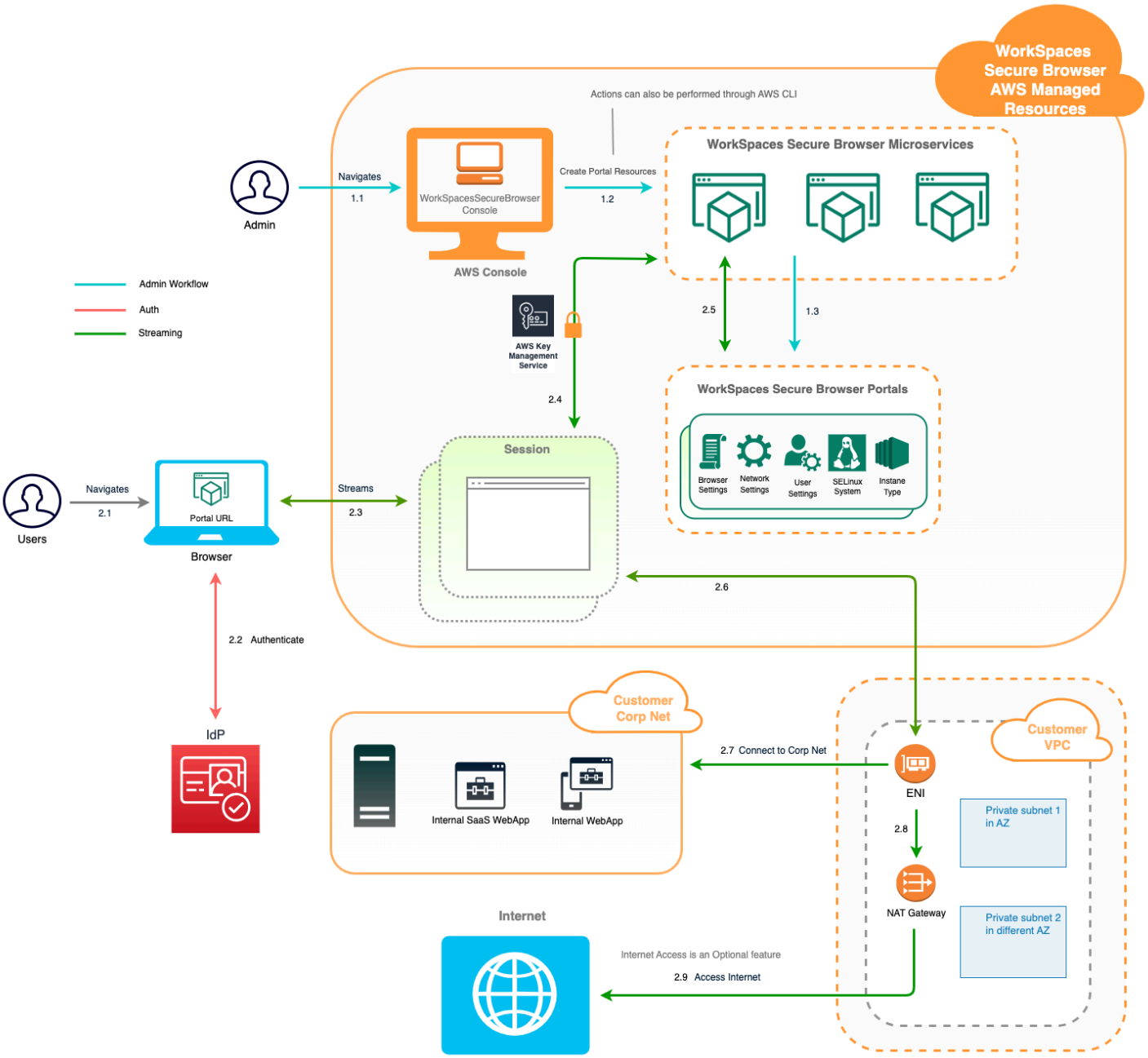
AWS Amazon WorkSpaces Secure Browser に関連する のサービス

WorkSpaces Secure Browser に関連する AWS サービスがいくつかあります。

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の Amazon WorkSpaces の機能です。WorkSpaces や 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促進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、容量、スケーリング、イメージは AWS によってオンデマンドで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開発者には永続的な Workspace Desktop を提供し、デスクトップコンピュータ上の少数の社内ウェブサイトや SaaS ウェブサイト (ネットワーク外でホストされているものを含む) へのアクセスを必要とするコンタクトセンターのユーザーには WorkSpaces Secure Browser を提供するように選択できます。

Amazon WorkSpaces Secure Browser のアーキテクチャ

WorkSpaces Secure Browser のアーキテクチャを以下の図に示します。



Amazon WorkSpaces Secure Browser へのアクセス

WorkSpaces Secure Browser にはいくつかの方法でアクセスできます。

管理者は、WorkSpaces Secure Browser コンソール、SDK、CLI、または API を使用して WorkSpaces Secure Browser にアクセスします。ユーザーは WorkSpaces Secure Browser エンドポイントを通じてアクセスします。

Amazon WorkSpaces Secure Browser の設定

WorkSpaces Secure Browser が社内のウェブサイトおよび SaaS アプリケーションに到達するように設定するには、以下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部では、電話またはテキストメッセージを受信し、電話のキーパッドに検証コードを入力します。

   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 のサービス とリソースへのアクセス権があります。セキュリティベストプラクティスとして、ユーザーに管理アクセス権を割り当て、ルートユーザーアクセスが必要なタスクの実行にはルートユーザーのみを使用するようにしてください。

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 [マイアカウント] 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、日常的なタスクにルートユーザーを使用しないように AWS アカウントのルートユーザー、 を保護し AWS IAM Identity Center、 を有効にして管理ユーザーを作成します。

を保護する 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 (コンソール) の仮想 MFA デバイスを有効にする」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、「 AWS IAM Identity Center ユーザーガイド」の「デフォルトを使用して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」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「グループの結合」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、 が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 アイデンティティセンター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 CLI、、 AWS SDKs、または AWS APIs。	使用するインターフェイスの指示に従ってください。 • については AWS CLI、「 AWS Command Line Interface ユーザーガイド」の「 を使用する AWS CLI ように AWS IAM Identity Centerを設定する」を参照してください。 • AWS SDKs、ツール、API については、 AWS APIs「 SDK およびツールリファ

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
		レンスガイド」の「IAM アイデンティティセンター認証」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 CLI、、 AWS SDKs、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 CLI、 AWS SDKs、または AWS APIs。	使用するインターフェイスの指示に従ってください。 • 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 とツールリファレンスガイド」の「長期認証情報を使用した認証」を参照してください。 AWS SDKs • API AWS APIs「IAM ユーザーのアクセスキーの管理」を参照してください。

Amazon WorkSpaces Secure Browser のネットワーク

以下のトピックでは、ユーザーが接続できるように WorkSpaces Secure Browser ストリーミング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 リソースや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

Amazon WorkSpaces Secure Browser 用の VPC の設定

WorkSpaces Secure Browser 用に VPC を設定するには、以下の手順に従います。

トピック

Amazon WorkSpaces Secure Browser 用の 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、「Amazon WorkSpaces Secure Browser 用の新しい VPC の作成」を参照してください。
- すべてのサブネットには、ユーザーが WorkSpaces Secure Browser でアクセスする内部コンテンツ AWS クラウド への安定した接続が必要です。

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、「Amazon WorkSpaces Secure Browser 用の新しい VPC の作成」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、「Amazon WorkSpaces Secure Browser での無制限のインターネットブラウジングの有効化 (推奨)」の手順に従ってください。

Amazon WorkSpaces Secure Browser 用の新しい VPC の作成

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。

トピック

- Elastic IP アドレスの割り当て
- 新しい VPC の作成
- 2 つ目のプライベートサブネットの追加
- サブネットルートテーブルの確認と名前付け

Elastic IP アドレスの割り当て

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 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
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。

新しい VPC の作成

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`**。
- 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`**。
- 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. Service 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。

2 つ目のプライベートサブネットの追加

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、[サブネット] を選択してください。
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`**。
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. [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。

サブネットルートテーブルの確認と名前付け

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 と指定します。
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

送信先	ターゲット	説明
		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、[サブネット] を選択してください。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、[サブネット] を選択してください。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。

Amazon WorkSpaces Secure Browser のインターネットブラウジングの有効化

無制限のインターネットブラウジングを有効にするか (推奨)、制限付きインターネットブラウジングを有効にするかを選択できます。

トピック

- Amazon WorkSpaces Secure Browser での無制限のインターネットブラウジングの有効化 (推奨)
- Amazon WorkSpaces Secure Browser での制限付きインターネットブラウジングの有効化
- Amazon WorkSpaces Secure Browser のインターネット接続ポート

Amazon WorkSpaces Secure Browser での無制限のインターネットブラウジングの有効化 (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、WorkSpaces Secure Browser は、パブリックインターネット上のサイト、および VPC 内でホストされている、または VPC に接続されているプライベートサイトへのアクセスを許可します。

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、以下の手順に従ってください。

> **Note**
>
> 既に VPC を設定している場合は、以下の手順に従って 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、「Amazon WorkSpaces Secure Browser 用の新しい VPC の作成」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 “2 つ目のプライベートサブネット”」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するには、パブリックサブネットを WorkSpaces Secure Browser ポータルに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。

Amazon WorkSpaces Secure Browser での制限付きインターネットブラウジングの有効化

WorkSpaces Secure Browser ポータルの推奨されるネットワーク設定は、NAT ゲートウェイに接続したプライベートサブネットを使用して、ポータルが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るようにすることです。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ことが必要になる場合があります。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的な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プログラム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、帯域幅の使用量を削減し、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。

管理対象デバイスや仮想環境のイメージでのプロキシ設定は多くの管理者にとって一般的です。しかし、デバイスを管理できない場合 (例えば、ユーザーが企業によって所有または管理されていないデバイスを使用している場合) や、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 では、ウェブブラウザに組み込まれた 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。そのためには、WorkSpaces Secure Browser の HTTP アウトバウンドプロキシを設定します。

この実装は、推奨されるアウトバウンド VPC プロキシ設定に基づいています。プロキシ実装は、オープンソースの HTTP プロキシ Squid に基づいています。そのため、WorkSpaces Secure Browser のブラウザ設定を使用して、WorkSpaces Secure Browser ポータルがプロキシエンドポイントに接続するように設定します。詳細については、「How to set up an outbound VPC proxy with domain whitelisting and content filtering」を参照してください。

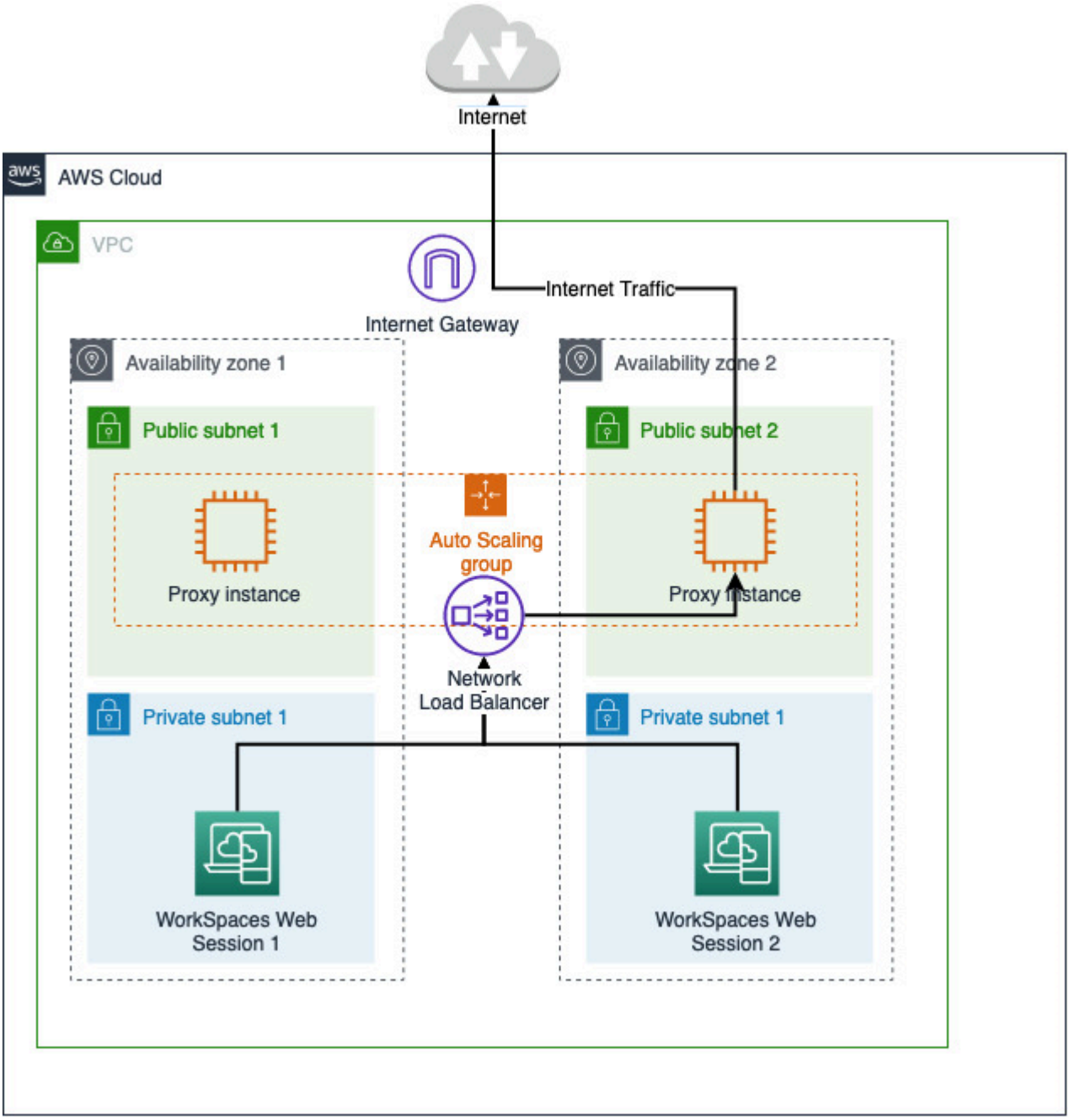
この実装には以下の利点があります。

- アウトバウンドプロキシが、Network Load Balancer によってホストされる自動スケールする Amazon EC2 インスタンスのグループで構成されている。プロキシインスタンスはパブリックサブネット内に配置され、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。
- WorkSpaces Secure Browser ポータルがプライベートサブネットにデプロイされている。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がありません。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経由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も、WorkSpaces Secure Browser ポータルの設定は同様になります。

トピック

Amazon WorkSpaces Secure Browser での制限付きインターネットブラウジングアーキテクチャ

VPC での一般的なプロキシ設定の例を以下に示します。プロキシ Amazon EC2 インスタンスはパブリックサブネットに配置され、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が自動的にスケールアップできるようになり、Network Load Balancer が単一のプロキシエンドポイントとなり、WorkSpaces Secure Browser セッションで使用できるようになります。



Amazon WorkSpaces Secure Browser の制限付きインターネットブラウジングの前提条件

開始する前に、以下の前提条件を満たしていることを確認してください。

- 複数のアベイラビリティーゾーン (AZ) にまたがるパブリックサブネットとプライベートサブネットを配置した VPC が既にデプロイされている必要があります。VPC 環境の設定方法の詳細については、「デフォルト VPC」を参照してください。

- WorkSpaces Secure Browser セッションが存在するプライベートサブネットからアクセスできる 1 つのプロキシエンドポイント (Network Load Balancer の DNS 名など) が必要です。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できる 1 つのエンドポイントがあることを確認してください。

Amazon WorkSpaces Secure Browser での HTTP アウトバウンドプロキシ

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

1. サンプルのアウトバウンドプロキシを VPC にデプロイするには、「How to set up an outbound VPC proxy with domain whitelisting and content filtering」の手順に従います。
   a. 「インストール (1 回限りの設定)」の手順に従って、CloudFormation テンプレートをお客様のアカウントにデプロイします。CloudFormation テンプレートのパラメータとして適切な VPC とサブネットを選択してください。
   b. デプロイ後、CloudFormation の出力パラメータである OutboundProxyDomain と OutboundProxyPort を確認します。これがプロキシの DNS 名とポートです。
   c. 独自のプロキシが既にある場合は、このステップをスキップし、そのプロキシの 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以下の ProxySettings ポリシーを追加します。`ProxyServer` フィールドには、プロキシの DNS 名とポートを設定する必要があります。ProxySettings ポリシーの詳細については、「ProxySettings」を参照してください。

```
{
    "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、プロキシが Chrome の設定に適用されていることが「Chrome は管理者により指定されたプロキシ設定を使用しています」として表示されます。
4. chrome://policy に移動し、[Chrome ポリシー] タブでこのポリシーが適用されていることを確認します。
5. WorkSpaces Secure Browser セッションで、NAT ゲートウェイを使用せずに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 Logs で、Squid プロキシのアクセスログが記録されていることを確認します。

Amazon WorkSpaces Secure Browser の制限付きインターネットブラウジングのトラブルシューティング

Chrome ポリシーが適用された後も WorkSpaces Secure Browser セッションで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の解決を試みてください。

- WorkSpaces Secure 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。そのためには、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` フィールドの形式が次のようになっていることを確認します: `<Proxy DNS name>:<Proxy port>`。プレフィックスに `http://` や `https://` が含まれていてはいけません。
  - 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。

Amazon WorkSpaces Secure Browser のインターネット接続ポート

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を可能に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。また、NAT ゲートウェイを含むプライベートサブネットが設定されている場合は、インターネットへの接続も可能にします。

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

WorkSpaces Secure Browser の VPC に関するベストプラクティス

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 のサービスクォータ (上限) が、予想される需要に対応するのに十分であることを確認します。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。WorkSpaces Secure Browser のデフォルトクォータについては、「the section called “サービスクォータの管理”」を参照してください。
- 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で NAT ゲートウェイを含む 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

- ストリーミング中は、WorkSpaces Secure Browser セッションごとに独自の Elastic Network Interface が必要です。WorkSpaces Secure Browser はフリートの希望最大容量に応じた数の Elastic Network Interface (ENI) 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

- ユーザー数をスケールアップする計画を立てる際には、WorkSpaces Secure Browser セッションごとに、設定したサブネットからの固有のクライアント 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、希望するリージョンの WorkSpaces Secure Browser がサポートする各アベイラビリティーゾーン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”」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。

Amazon WorkSpaces Secure Browser でサポートされているアベイラビリティーゾーン

WorkSpaces Secure Browser で使用する仮想プライベートクラウド (VPC) を作成する場合、VPC のサブネットは WorkSpaces Secure Browser を起動するリージョン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。たとえば、 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利用できます。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

リージョン名	リージョンコード	サポートされる AZ ID
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 ID の詳細については、Amazon 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、およびローカルゾーン」を参照してください。

Amazon WorkSpaces Secure Browser のユーザー接続の有効化

WorkSpaces Secure Browser は、パブリックインターネットを介してストリーミング接続を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ためには、インターネットに接続できることが必須です。このトラフィックを許可するには、「Amazon WorkSpaces Secure Browser の許可ドメイン」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

- Amazon WorkSpaces Secure Browser の IP アドレスとポートの要件

- Amazon WorkSpaces Secure Browser の許可ドメイン

Amazon WorkSpaces Secure Browser の 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以下のポートでアウトバウンドのアクセスが必要です。

- 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、Amazon WorkSpaces Secure Browser の許可ドメイン 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 ドメインと 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-AWSPublicIpAddressRangePowerShell 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。

Amazon WorkSpaces Secure Browser の許可ドメイン

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、以下のドメインを追加する必要があります。

以下の表で、*{region}* は運用中のウェブポータルのリージョンコードに置き換えてください。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 となります。リージョンコードのリストについては、「Amazon WorkSpaces Secure Browser endpoints and quotas」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 の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 Secure Browser の静的アセット	*.workspaces-web.com di5ry4hb4263e.cloudfront.net
WorkSpaces Secure Browser の認証	*.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するために許可リストに追加する必要があるドメインを特定してください。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。

Amazon WorkSpaces Secure Browser の開始方法

以下の手順に従って WorkSpaces Secure Browser ウェブポータルを作成し、ユーザーが既存のブラウザから社内ウェブサイトや 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。

> **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 の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費用はかかりません。WorkSpaces Secure Browser では、サービスを積極的に利用するユーザーに低額の月額料金を含め、従量制料金を提供しています。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、「Amazon WorkSpaces Secure Browser の設定」を参照してください。

トピック

- Amazon WorkSpaces Secure Browser でのウェブポータルの作成
- Amazon WorkSpaces Secure Browser でのウェブポータルのテスト
- Amazon WorkSpaces Secure Browser でのウェブポータルの配布

Amazon WorkSpaces Secure Browser でのウェブポータルの作成

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

- Amazon WorkSpaces Secure Browser のネットワーク設定の実行

- Amazon WorkSpaces Secure Browser のポータル設定の実行
- Amazon WorkSpaces Secure Browser のユーザー設定の実行
- Amazon WorkSpaces Secure Browser の ID プロバイダーの設定
- Amazon WorkSpaces Secure Browser でのウェブポータルの起動

Amazon WorkSpaces Secure Browser のネットワーク設定の実行

WorkSpaces Secure Browser のネットワーク設定を行うには、以下の手順に従います。

1. https://console.aws.amazon.com/workspaces-web/home で WorkSpaces Secure Browser コンソールを開きます。
2. [WorkSpaces Secure Browser]、[ウェブポータル] の順に選択した後、[ウェブポータルを作成] 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] では、WorkSpaces Secure Browser でユーザーにアクセスを許可するコンテンツに接続されている 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、「Amazon WorkSpaces Secure Browser のネットワーク」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。

Amazon WorkSpaces Secure Browser のポータル設定の実行

[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数を入力します。詳細については、「the section called “サービスクォータの管理”」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、月間のアクティブユーザーあたりのコストが変わります。料金の詳細については、「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グの設定”」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 “ブラウザポリシーの管理”」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グの設定”」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 URL を設定できます。詳細については、「the section called “URL フィルタリングの設定”」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管理”」を参照してください。
6. [次へ] を選択して続行します。

Amazon WorkSpaces Secure Browser のユーザー設定の実行

[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. アクセス許可 で、シングルサインオン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拡張機能の管理”」を参照してください。
2. [ユーザーにウェブポータルからローカルデバイスへの印刷を許可する] で、[許可] または [許可しない] を選択します。
3. [ユーザーにウェブポータルへのディープリンクを許可する] で、[許可] または [許可しない] を選択します。ディープリンクの詳細については、「the section called “ディープリンク”」を参照してください。
4. ツールバーコントロールで、 機能で必要な設定を選択します。

5. 設定 で、ツールバーの状態 (ドッキングまたはデタッチ) 、テーマ (ダークモードまたはライトモード) 、アイコンの可視性、セッションの最大表示解像度など、セッション開始時のツールバー表示ビューを管理します。これらのオプションを完全に制御できるように、これらの設定を未設定のままにします。詳細については、「the section called “ツールバーコントロール”」を参照してください。
6. セッションタイムアウトには、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。

Amazon WorkSpaces Secure Browser の ID プロバイダーの設定

以下の手順に従って、ID プロバイダー (IdP) を設定します。

トピック

Amazon WorkSpaces Secure Browser の ID プロバイダータイプの選択

WorkSpaces Secure Browser には、スタンダードと AWS IAM Identity Center の 2 つの認証タイプがあります。[ID プロバイダーの設定] ページで、ポータルで使用する認証タイプを選択します。

- [スタンダード] (デフォルトオプション) では、サードパーティーの SAML 2.0 ID プロバイダー (Okta や Ping など) とポータルを直接フェデレーションするように設定します。詳細については、「the section called “スタンダード認証タイプ”」を参照してください。スタンダードタイプでは、SP 開始と IdP 開始の両方の認証フローがサポートされています。
- [IAM アイデンティティセンター] (詳細オプション) では、IAM アイデンティティセンターとポータルがフェデレーションするように設定します。この認証タイプを使用するには、IAM アイデンティティセンターと WorkSpaces Secure Browser ポータルの両方が同じ AWS リージョンに存在する必要があります。詳細については、「the section called “IAM アイデンティティセンター認証タイプ”」を参照してください。

トピック

Amazon WorkSpaces Secure Browser のスタンダード認証タイプの設定

スタンダード認証タイプはデフォルトの認証タイプです。SAML 2.0 準拠の IdP を利用して、サービスプロバイダー開始 (SP 開始) と ID プロバイダー開始 (IdP 開始) のサインインフローをサポートできます。スタンダード認証タイプでは、以下の手順に従って、サードパーティーの SAML 2.0 IdP (Okta や Ping など) とポータルが直接フェデレーションするように設定します。

トピック

- 独自の IdP での IdP の設定
- Amazon WorkSpaces Secure Browser での IdP 設定の完了
- Amazon WorkSpaces Secure Browser での特定の IdP の使用に関するガイダンス

Amazon WorkSpaces Secure Browser での ID プロバイダーの設定

ID プロバイダーを設定するには、以下の手順に従います。

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ます。個々のメタデータ値のタブは開いたままにしておきます。
   - SP メタデータファイルを使用できる場合は、[メタデータファイルをダウンロード] 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、次の手順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。この操作を行わないと、ユーザーはサインインできません。
   - 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 および IdP によって開始された SAML アサーション] または [SP によって開始された SAML アサーションのみ] を選択します。
   - [SP および IdP によって開始された SAML アサーション] を選択すると、ポータルで両方のタイプのサインインフローがサポートされます。IdP 開始フローをサポートするポータルでは、ユーザーがポータル URL にアクセスしてセッションを開始する必要はなく、IdP から直接 SAML アサーションをサービス ID フェデレーションエンドポイントに送信できます。
     - このオプションを選択すると、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ようになります。
     - 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状態] を設定する必要があります。ポータルのリレー状態パラメータは、コンソールの [IdP によって開始された SAML サインイン] で確認できます。または、SP メタデータファイルの `<md:IdPInitRelayState>` からコピーすることもできます。
     - メモ
       - 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=Ex
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、& を & に変更してください。& は XML エスケープ文字です。

- ポータルで SP 開始のサインインフローのみをサポートするように設定するには、[SP によって開始された SAML アサーションのみ] を選択します。このオプションでは、IdP 開始のサインインフローからの未承諾の SAML アサーションは拒否されます。

> **Note**
>
> 一部のサードパーティー IdP では、SP 開始フローを活用して IdP 開始の認証エクスペリエンスを提供するカスタム 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 リクエストに署名する] を有効にするかどうかを選択します。SP 開始の認証により、IdP は認証リクエストがポータルから送信されていることを検証できるため、他のサードパーティーからのリクエストを受け付けないようにできます。

   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。同じ署名証明書をシングル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。名称は 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署名アルゴリズムであり、デフォルトのリクエスト署名アルゴリズムでもあります。

6. [暗号化された SAML アサーションが必要] を有効にするかどうかを選択します。有効にすると、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。この証明書は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、IdP にアップロードします。次に、IdP でアサーションの暗号化を有効にします (名称は 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。シングルサインアウトを有効にすると、エンドユーザーは 1 アクションで IdP と WorkSpaces Secure Browser の両方のセッションからサインアウトできるようになります。

   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] で確認できます。または、SP メタデータファイルの `<md:SingleLogoutService>` からも確認できます。

   c. IdP で [シングルログアウト] を有効にします。名称は IdP によって異なる場合があります。

独自の IdP での IdP の設定

独自の IdP で IdP を設定するには、以下の手順に従います。

1. ブラウザで新しいタブが開きます。
2. 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 の適切な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。IdP の設定にポータルの詳細を追加する方法については、the section called “特定の IdP に関するガイダンス” でプロバイダーのドキュメントを参照してください。
3. SAML アサーションの [NameID] を確認します。

   SAML IdP によって SAML アサーションの [NameID] にユーザー E メールフィールドが設定されていることを確認します。NameID とユーザーの E メールアドレスは、ポータルで SAML フェデレーション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 Name ID 形式を使用します。
4. オプション: IdP 開始の認証の [リレー状態] を設定します。

   前のステップで [SP および IdP によって開始された SAML アサーションを受け入れる] を選択した場合は、「the section called “WorkSpaces Secure Browser での IdP の設定” 」のステップ 2 に従って、IdP アプリケーションのデフォルトのリレー状態を設定します。

5. 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 リクエストに署名する] を選択した場合は、「the section called “WorkSpaces Secure Browser での IdP の設定”」のステップ 3 に従って署名証明書を IdP にアップロードし、リクエスト署名を有効にします。Okta などの一部の IdP では、[リクエスト署名] を使用するために [NameID] が「永続的」タイプであることが必要になる場合があります。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。
6. オプション: [アサーションの暗号化] を設定します。[このプロバイダーに暗号化された SAML アサーションをリクエストする] 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「メタデータをアップロードする」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、アサーションの暗号化を有効にします。
7. 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、「the section called “WorkSpaces Secure Browser での IdP の設定”」のステップ 5 のステップに従って、署名証明書を IdP にアップロードし、[シングルログアウト URL] に入力して、[シングルログアウト] を有効にします。
8. IdP 内のユーザーに WorkSpaces Secure Browser を使用するためのアクセス権を付与します。
9. IdP からメタデータ交換ファイルをダウンロードします。次のステップで、このメタデータを WorkSpaces Secure Browser にアップロードします。

Amazon WorkSpaces Secure Browser での IdP 設定の完了

WorkSpaces Secure Browser で IdP 設定を完了するには、以下の手順に従います。

1. WorkSpaces Secure Browser コンソールに戻ります。作成ウィザードの [ID プロバイダーを設定] ページに移動し、[IdP メタデータ] の下で、メタデータファイルをアップロードするか、IdP のメタデータ 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。
2. 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 [ファイルを選択] を選びます。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。
3. 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] で IdP から取得したメタデータ URL を入力します。
4. 終了したら、[Next] (次へ) を選択します。

5. [このプロバイダーに暗号化された SAML アサーションをリクエストする] オプションを有効にしたポータルの場合、ポータルの IdP 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、その IdP でこの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 アサーションにサブジェクトまたは NameID がマッピングされ、設定されている必要があります。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 レスポンスに以下のクレームが含まれている必要があります。*<Your SP Entity ID>* と *<Your SP ACS URL>* は、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やメタデータドキュメントから確認できます。
>
> - `AudienceRestriction` クレームの `Audience` 値で 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。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>">
> ```
>
> - `SubjectConfirmationData` クレームの `Recipient` 値で SP ACS URL を設定し、`InResponseTo` 値で元の SAML リクエスト ID を設定。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 開始の SAML アサーションの場合、リクエストの詳細は HTTP POST リクエストの本文内で `RelayState` パラメータの形式になっている必要があります。リクエスト

本文には、SAML アサーションを SAMLResponse パラメータとして含める必要があります。これらの両方が含まれていれば、前の手順が正しく完了しています。
IdP 開始の SAML プロバイダーの POST 本文の例を以下に示します。

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

Amazon WorkSpaces Secure Browser での特定の IdP の使用に関するガイダンス

ポータルの SAML フェデレーションを正しく設定するには、以下のリンクの先で、一般的に利用されている IdP のドキュメントを参照してください。

IdP	SAML アプリケーションの設定	ユーザー管理	IdP 開始の認証	リクエスト署名	アサーションの暗号化	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	アプリケーション統合ウィザード SAML フィールドリファレンス	アプリケーション統合ウィザード SAML フィールドリファレンス	アプリケーション統合ウィザード SAML フィールドリファレンス	アプリケーション統合ウィザード 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 開始の SSO の有効化	PingOne for Enterprise での認証リ	PingOne for Enterprise は暗号化をサポート	SAML 2.0 シングルログアウト

IdP	SAML アプリケーションの設定	ユーザー管理	IdP 開始の認証	リクエスト署名	アサーションの暗号化	シングルログアウト
				クエスト署名の設定	していますか?	
OneLogin	SAML Custom Connector (Advanced) (4266907)	OneLogin にユーザーを手動で追加	SAML Custom Connector (Advanced) (4266907)	SAML Custom Connector (Advanced) (4266907)	SAML Custom Connector (Advanced) (4266907)	SAML Custom Connector (Advanced) (4266907)
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設定	独自の SAML 2.0 アプリケーションを設定	独自の SAML 2.0 アプリケーションを設定	該当なし	該当なし	該当なし

Amazon WorkSpaces Secure Browser の IAM アイデンティティセンター認証タイプの設定

IAM アイデンティティセンタータイプ (詳細) では、IAM アイデンティティセンターとポータルをフェデレーションします。以下の条件に該当する場合のみ、このオプションを選択します。

- IAM アイデンティティセンターは、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ています。
- 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 アイデンティティセンター認証タイプでウェブポータルを作成する前に、IAM アイデンティティセンター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 アイデンティティセンター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 アイデンティティセンター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 アイデンティティセンターを使用している場合は、プロバイダーのタイプとして IAM アイデンティティセンターを選択し、以下の手順に従ってウェブポータルからユーザーやグループを追加、表示、削除できます。

> **Note**
>
> この認証タイプを使用するには、IAM アイデンティティセンターが 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 アイデンティティセンターが別の 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 “スタンダード認証タイプ”」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 アイデンティティセンターと統合された WorkSpaces Secure Browser ポータルのみを作成できます。

トピック

- IAM アイデンティティセンターでのウェブポータルの作成
- IAM アイデンティティセンターでのウェブポータルの管理
- ウェブポータルへのユーザーとグループの追加
- ウェブポータルのユーザーとグループの表示または削除

IAM アイデンティティセンターでのウェブポータルの作成

IAM アイデンティティセンターでウェブポータルを作成するには、以下の手順に従います。

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」でポータル作成時に [AWS IAM Identity Center] を選択します。
2. [IAM アイデンティティセンターで続行] を選択します。
3. [ユーザーとグループを割り当てる] ページで、[ユーザー]/[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またはグループの横にあるチェックボックスをオンにします。
5. ポータルの作成後、関連付けたユーザーは IAM アイデンティティセンター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 アイデンティティセンターでのウェブポータルの管理

IAM アイデンティティセンターでウェブポータルを管理するには、以下の手順に従います。

IAM Identity Center でウェブポータルを管理するには

1. ポータルが作成されると、IAM アイデンティティセンターコンソールで設定済みアプリケーションとして表示されます。
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。

ウェブポータルへのユーザーとグループの追加

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、以下の手順に従います。

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. 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]、[ウェブポータル] の順に選択し、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の表示または削除

ウェブポータルのユーザーやグループを表示または削除するには、[割り当てられたユーザー] の表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の管理」を参照してください。

> **Note**
>
> WorkSpaces Secure Browser ポータルの編集ページでは、ユーザーやグループを表示したり削除したり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。

Amazon WorkSpaces Secure Browser の ID プロバイダータイプの変更

ポータルの認証タイプはいつでも変更できます。これを実行するには、次の手順を実行します。

- [IAM アイデンティティセンター] から [スタンダード] に変更するには、「the section called “スタンダード認証タイプ”」の手順に従います。
- [スタンダード] から [IAM アイデンティティセンター] に変更するには、「the section called “IAM アイデンティティセンター認証タイプ”」の手順に従います。

ID プロバイダータイプの変更は反映されるまでに最大 15 分かかる場合がありますが、進行中のセッションが自動的に終了されることはありません。

`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。

Amazon WorkSpaces Secure Browser でのウェブポータルの起動

設定が完了したウェブポータルは以下の手順に従って起動できます。

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。

Amazon WorkSpaces Secure Browser でのウェブポータルのテスト

ウェブポータルを作成したら、WorkSpaces Secure Browser エンドポイントにサインインして、接続されているウェブサイトをエンドユーザーと同じように閲覧できます。

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 Amazon WorkSpaces Secure Browser でのウェブポータルの配布 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]、[ウェブポータル] の順に選択し、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 サインインページで、[サインイン]、[SAML] の順に選択し、SAML 認証情報を入力します。
5. [セッションは準備中です] ページが表示されたら、WorkSpaces Secure Browser セッションが開始されます。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。

Amazon WorkSpaces Secure Browser でのウェブポータルの配布

ユーザーが WorkSpaces Secure Browser を使用開始する準備ができたら、以下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開始できるようにします。そのためには、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、「the section called “スタンダード認証タイプ”」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。または、SP 開始のフローを使用して IdP 開始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を作成する」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。

Amazon WorkSpaces Secure Browser でのウェブポータルの管理

ウェブポータルを設定したら、以下のアクションを実行して管理できます。

トピック

Amazon WorkSpaces Secure Browser でのウェブポータルの詳細の表示

ウェブポータルの詳細を表示するには、以下の手順に従います。

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]、[ウェブポータル] の順に選択し、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。

Amazon WorkSpaces Secure Browser でのウェブポータルの編集

ウェブポータルを編集するには、以下の手順に従います。

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]、[ウェブポータル] の順に選択し、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。

Amazon WorkSpaces Secure Browser でのウェブポータルの削除

ウェブポータルを削除するには、以下の手順に従います。

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]、[ウェブポータル] の順に選択し、ウェブポータルを選択してから、[削除] を選択します。

Amazon WorkSpaces Secure Browser でのポータルのサービスクォータの管理

を作成すると AWS アカウント、 でリソースを使用するため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 のサービス。管理者は、ユースケースをサポートす

るために引き上げが必要になる可能性がある 2 つのクォータを把握しておく必要があります。これらの 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、各リージョンで利用できる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の数です。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。

以下の表に、デフォルトのサービスクォータの上限を示します。

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

各リージョンのアカウントに割り当てられているサービスクォータはいつでも Service Quotas ページで確認できます。

> **Important**
>
> サービスクォータは AWS リージョン 、一度に 1 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 endpoints and quotas」を参照してください。

トピック

- Amazon WorkSpaces Secure Browser でのサービスクォータ引き上げのリクエスト
- Amazon WorkSpaces Secure Browser でのポータル引き上げのリクエスト
- Amazon WorkSpaces Secure Browser での最大同時セッション数引き上げのリクエスト
- Amazon WorkSpaces Secure Browser でのサービスクォータ例
- Amazon WorkSpaces Secure Browser のその他のサービスクォータ

Amazon WorkSpaces Secure Browser でのサービスクォータ引き上げのリクエスト

サービスクォータ引き上げをリクエストするには、以下の手順に従います。

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 の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。

Amazon WorkSpaces Secure Browser でのポータル引き上げのリクエスト

ポータルはこの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を関連付けます。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適用できるため、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で複数のポータルを作成します。例えば、グループ A には制限付きポリシー (クリップボードとファイル転送を無効にするなど) により特定のウェブサイトへのアクセスのみを提供し、グループ B には 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提供できます。サポートされている任意の AWS リージョンでポータルを作成できます。現在のサービス提供状況については、「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. 目的のリージョンの 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する] を選択します。
4. [クォータ値を引き上げる] に、クォータに設定する合計数を入力します。

Amazon WorkSpaces Secure Browser での最大同時セッション数引き上げのリクエスト

最大同時セッション数クォータは、ポータルに同時に接続できるユーザーの最大数です。最大同時セッション数のサービスクォータ上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を使用できない可能性があります。このサービスクォータを引き上げることに加えて、お客様は VPC とサブネットに最大同時セッション数をサポートするのに十分な IP スペースがあることを確認する必要があります。

最大同時セッション数の引き上げをリクエストするには

1. 目的のリージョンの Service Quotas ページを開きます。
2. 引き上げが必要な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する] を選択します。
4. [クォータ値を引き上げる] に、クォータに設定する合計数を入力します。

> **Note**
>
> 大規模または緊急の引き上げが必要な場合は、Service Quotas 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てサポートケースにリンクし、ユースケースや緊急性に関する詳細を返信として追加してください。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。

Amazon WorkSpaces Secure Browser でのサービスクォータ例

例えば、管理者が米国東部 (バージニア北部) で合計 125 人のユーザー向けに 2 つのウェブポータルを設定するとします。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 人のユーザーをサポート予定であ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したところ、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 番目のウェブポータル (ポータル B) は、カスタマーの 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したところ、管理者はスタンダードインスタンスタイプで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 について、管理者は XL インスタンスの上限をリージョンのデフォルト値 (5) から 100 に引き上げるために、サービスクォータの引き上げリクエストを送信する必要があります。リクエストが承認されると、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 については、管理者はクォータの引き上げをリクエストせずに進めることができます (リージョンのスタンダードインスタンスタイプのデフォルトクォータが 25 であるため)。

Amazon WorkSpaces Secure Browser のその他のサービスクォータ

Service Quotas ページのリストにあるその他のクォータを表示し、引き上げをリクエストできます。ほとんどのお客様はこれらの上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とレートの 2 タイプに大きく分類されます。

数のクォータについては、ウェブポータル数のサービスクォータ引き上げをリクエストすると、固有のポータルを作成するために必要なサブリソースの数も自動的に引き上げられます。この変更は Service Quotas ページに反映されます。例えば、ポータル数の上限を 3 から 5 に引き上げることをリクエストすると、ブラウザ設定とユーザー設定の両方のサービスクォータも自動的に 3 から 5 に引き上げられます。必要に応じて、サブリソースを再利用するか、新規に作成するかを選択できます。

まれに、その他のリソースクォータの数やレートを引き上げる必要があるユースケースが発生する場合があります。例えば、追加のポータル設定をテストするために、ブラウザ設定のサービスクォータの数を増やしたいと考える管理者もいるでしょう。これらのサービスクォータリクエストはケースバイケースで審査され、対応されます。

レートクォータについては、アカウントのポータル数の上限に関係なく、Service Quotas で公開されているレートの上限を調整する必要はありません。

Amazon WorkSpaces Secure Browser での 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ケーションにサインインして SAML IdP トークンを既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、そのユーザーは 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。
   - 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タイムアウト値とアイドルタイムアウト値を設定します。これらの値は、ユーザーが最後に操作してから、非アクティブ状態のため WorkSpaces Secure Browser セッションが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 “ウェブポータルの作成”」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、ユーザーがまだ有効な SAML IdP トークンを持っている場合、ユーザーはユーザー名とパスワードを入力して新しい

WorkSpaces Secure Browser セッションを開始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。

Amazon WorkSpaces Secure Browser でのユーザーアクセスログの設定

以下の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できます。

- 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

カスタマーは、WorkSpaces Secure Browser の使用に伴って生じる潜在的な法的問題を理解し、WorkSpaces Secure Browser の使用が、適用されるすべての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。これらには、従業員による WorkSpaces Secure Browser の使用状況 (アプリケーション内で行われるアクティビティなど) をモニタリングする雇用主の権限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有効にすると、Amazon Kinesis Data Streams からの請求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ギングを有効にするには、[ユーザーアクセスロギング] で、データの受信に使用する 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。

トピック

- Amazon WorkSpaces Secure Browser のユーザーアクセスログの例

Amazon WorkSpaces Secure Browser のユーザーアクセスログの例

以下は、Validation、StartSession、VisitPage、EndSession を含む利用可能な各イベントの例です。

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"
}
```

Amazon WorkSpaces Secure Browser でのブラウザポリシーの管理

WorkSpaces Secure Browser では、最新の安定した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 “チュートリアル: カスタムブラウザポリシーの設定” 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、「入門」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、ベースラインのブラウザポリシー設定をすべてのポータルに適用します。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の編集”」を参照してください。

トピック

- チュートリアル: Amazon WorkSpaces Secure Browser でのカスタムブラウザポリシーの設定
- Amazon WorkSpaces Secure Browser でのベースラインブラウザポリシーの編集

チュートリアル: Amazon WorkSpaces Secure Browser でのカスタムブラウザポリシーの設定

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。

この後のチュートリアルでは、以下のポリシーコントロールを設定した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 ポリシーの 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 “ウェブポータルの作成”」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 – 特定の拡張機能をインストールできるようにします。
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どのウェブページを開くかを設定します。
   - 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. 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] を選択し、次に [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. [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. [Save] を選択します。

Amazon WorkSpaces Secure Browser でのベースラインブラウザポリシーの編集

サービスを提供するために、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。

Amazon WorkSpaces Secure Browser の IME (Input Method Editor) の設定

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 Secure Browser セッションには、デフォルトで IME の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 サポート。

Amazon WorkSpaces Secure Browser のセッション内ローカリゼーションの設定

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、それらを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。

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にある ForcedLanguages ポリシー。詳細については、「ForcedLanguages」を参照してください。
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 (読み込みメッセージとエラーを含む)
- 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

トピック

Amazon WorkSpaces Secure Browser でサポートされている言語コード

以下のリストでは、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)

ユーザーブラウザ設定での言語の選択

ユーザーのローカルブラウザ設定を行うには、適切な手順に従ってください。

- 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。

Amazon WorkSpaces Secure Browser での IP アクセスコントロールの管理

WorkSpaces Secure Browser では、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。接続すると、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、ユーザーが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 の使用に伴って生じる潜在的な法的問題を理解し、WorkSpaces Secure Browser の使用が、適用されるすべての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。これらには、従業員による WorkSpaces Secure Browser の使用状況 (アプリケーション内で行われるアクティビティなど) をモニタリングする雇用主の権限を規制する法律が含まれます。

トピック

Amazon WorkSpaces Secure Browser での IP アクセスコントロールグループの作成

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. 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. 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。

Amazon WorkSpaces Secure Browser での IP アクセス設定とウェブポータルの関連付け

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. 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. 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. [Save] 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” 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。

Amazon WorkSpaces Secure Browser での IP アクセスコントロールグループの編集

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. 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. 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。

Amazon WorkSpaces Secure Browser での IP アクセスコントロールグループの削除

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. 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. 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。

Amazon WorkSpaces Secure Browser でのシングルサインオン拡張機能の管理

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。

デフォルトでは、Chrome のシークレットウィンドウや Firefox のプライベートブラウジングウィンドウで拡張機能は有効になりません。ユーザーはそれらの拡張機能を手動で有効にできます。Chrome の詳細については、「シークレットモードでの拡張機能」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での拡張機能」を参照してください。

ユーザーがポータルにサインインすると、拡張機能をインストールするように求められます。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拡張機能”」を参照してください。

トピック

- Amazon WorkSpaces Secure Browser でのシングルサインオン拡張機能のドメインの特定
- Amazon WorkSpaces Secure Browser での新しいウェブポータルへのシングルサインオン拡張機能の追加
- Amazon WorkSpaces Secure Browser での既存のウェブポータルへのシングルサインオン拡張機能の追加
- Amazon WorkSpaces Secure Browser でのシングルサインオン拡張機能の編集または削除

Amazon WorkSpaces Secure Browser でのシングルサインオン拡張機能のドメインの特定

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。

Cookie を同期させる適切なドメインをテストして特定するのはお客様の責任です。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。

よく利用される IdP が使用するドメインを確認するには、以下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
OneLogin	onelogin.com
Duo	duosecurity.com

Amazon WorkSpaces Secure Browser での新しいウェブポータルへのシングルサインオン拡張機能の追加

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、以下の手順に従います。

1. the section called “ユーザー設定” に到達するまで、the section called “ウェブポータルの作成” の手順に従います。
2. the section called “ユーザー設定” 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” の手順と the section called “ウェブポータルの作成” 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。

Amazon WorkSpaces Secure Browser での既存のウェブポータルへのシングルサインオン拡張機能の追加

既存のウェブポータルに拡張機能を追加するには、以下の手順に従います。

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。

Amazon WorkSpaces Secure Browser でのシングルサインオン拡張機能の編集または削除

ドメインを編集したり、拡張機能を削除したりするには、以下の手順に従います。

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. 削除すると、ユーザーのブラウザに WorkSpaces Secure Browser 拡張機能がインストールされていても、セッションで Cookie が同期されなくなります。

Amazon WorkSpaces Secure Browser での URL フィルタリングの設定

Chrome ポリシーを使用して、リモートブラウザからユーザーがアクセスできる URL をフィルタリングできます。Chrome ポリシーには、URL をフィルタリングするための 2 つのメカニズム、URLAllowlist と URLBlocklist が用意されています。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か、カスタム JSON ステートメントの一部として追加できます (インラインエディタまたは JSON ファイルのアップロードのいずれかで)。

トピック

- Amazon WorkSpaces Secure Browser でのコンソールを使用した URL フィルタリングの設定
- Amazon WorkSpaces Secure Browser での JSON エディタまたはファイルアップロードを使用した URL フィルタリングの設定

Amazon WorkSpaces Secure Browser でのコンソールを使用した URL フィルタリングの設定

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、以下の手順に従います。

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]、[ウェブポータル] の順に選択し、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、以下のオプションから選択します。

   - すべての URL 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 URL 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することで、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設定できます。例えば、www.anycorp.com を BlockURL リストに追加すると、セッション中にユーザーが www.anycorp.com に移動できなくなります。
   - すべての URL 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。特定のウェブサイトを URL 許可リストに追加して、ユーザーがアクセスできるウェブサイトのリストを管理し、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 1 クリックで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 と blockURL のリストが作成されて併用されます。URL 許可リスト は URL ブロックリスト よりも優先されます。このオプションを選択すると、パスによる URL フィルタリングが有効になります。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、その他の URL パス (www.anycorp.com/finance など) にはアクセスできなくなります。

ブロック URL と許可 URL の使用に関する詳細なガイダンスについては、「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。最適な結果を得るには、Chrome のブロックリストフィルタ形式に従って URL をこれらのリストに追加します。詳細については、「URL ブロックリストフィルタ形式」を参照してください。

Amazon WorkSpaces Secure Browser での JSON エディタまたはファイルアップロードを使用した URL フィルタリングの設定

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、以下の手順に従います。

1. [ポリシー設定] モジュールから [JSON エディタ] を選択して、コンソール UI モジュールの代わりに [エディタ] または [ファイルアップロード] ビューが使用されるようにします。
   - [エディタ] では、お客様はコンソールでインラインでカスタムポリシーステートメントを作成できます。ポリシーの作成中に JSON ステートメントのエラーが強調表示されます。
   - [ファイルアップロード] では、お客様はコンソール外で作成された JSON ファイル (既存の Chrome ブラウザからエクスポートしたものなど) を追加できます。
2. ウェブポータルの allow/denyURL リストを適切な形式にするには、URLAllowlist と URLBlocklist について Chrome ポリシーの詳細を参照してください。詳細については、「URLAllowlist」と「URLBlocklist」を参照してください。

Amazon WorkSpaces Secure Browser のディープリンク

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、セッション中に特定のウェブサイトにユーザーを接続する、ディープリンクをポータルで受信するように設定することもできます。ディープリンクが選択されると、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。リンクが新しいタブで表示され、セッション開始用に設定されたホームページが別のタブで表示されます。セッションが既に進行中の場合は、リンクが新しいタブで表示されるだけです。この機能を使用すると、管理者は WorkSpaces Secure Browser でより動的なユーザーエクスペリエンスを提供できます。

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。セッションが既に実行中の場合、ディープリンクは新しいタブで開かれます。セッションがまだ実行されていない場合は、ディープリンクの URL が新しいタブで開かれ、ポータルのデフォルトのホームページが別のタブで開かれます。ディープリンクに複数の URL が含まれる場合、リスト内の最初のディープリンクの URL がフォーカスされた状態で新しいタブで開かれ、後続の各 URL (デフォルトホームページを含む) はそれぞれ別のタブで開かれます。

トピック

- Amazon WorkSpaces Secure Browser でのディープリンクの設定
- Amazon WorkSpaces Secure Browser でのディープリンクの URL フィルタリングの使用

Amazon WorkSpaces Secure Browser でのディープリンクの設定

ディープリンクに対するアクセス許可を設定するには、ユーザー設定の作成時に [許可] を選択します。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。

ディープリンクには、最大 10 個の URL をカンマで区切って含めることができます。以下に例を示します。

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。

ディープリンクに対するアクセス許可の詳細については、「the section called “ユーザー設定”」を参照してください。

Amazon WorkSpaces Secure Browser でのディープリンクの URL フィルタリングの使用

このポータルリンクを共有したユーザーは、ディープリンクの値を操作して任意のウェブサイトにアクセスできます。ただし、そのウェブサイトのドメインがポータルからアクセス可能で、かつ URL ブロックリストに含まれていない場合に限ります。ユーザーがポータルで意図しないドメインにアクセスするのを防ぐために制限付き許可リストまたはブロックリストを作成するには、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。そのためには、許可リストに登録されているポータル URL に次の形式で URL を追加します。ここで uuid はポータル ID です。https://<uuid>.workspaces-web.com/?deepLinks=https%3A%2F%2Fwww.example.com%2F%3Fquery%3Dtrue。

詳細については、「the section called “URL フィルタリングの設定”」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 でのセッション管理ダッシュボードの使用

WorkSpaces Secure Browser コンソールのセッション管理ダッシュボードを使用して、アクティブなセッションと完了したセッションをモニタリングおよび管理します。

ダッシュボードへのアクセス

ダッシュボードにアクセスするには、以下の手順に従います。

ダッシュボードにアクセスするには

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]、[ウェブポータル] の順に選択し、対象のウェブポータルを選択します。
3. [セッション] タブを選択するか、[セッションを表示] を選択して、下部の分割パネルでダッシュボードを開きます。

ダッシュボードフィルター

セッションパネルで、以下のプロパティまたは値でセッションをフィルタリングできます。

- ステータス
  - アクティブ - セッションが現在実行中であることを示します。セッションを終了するには、以下を参照してください。
  - 終了済み - セッションがアクティブでなくなったことを示します。
- セッション ID
- ユーザー名
- セッション開始時刻

セッションの終了

セッションを終了するには、以下の手順に従います。

セッションを終了するには

1. セッションダッシュボードで、停止するセッションを選択します。
2. [Terminate] (終了) を選択します。
3. 切断されたユーザーはセッションのすべての状態を失います。開いていたすべてのタブは閉じられ、ブラウザ履歴、Secure Browser にダウンロードされたファイルは消去されます。

セッション履歴

ダッシュボードには、過去 35 日間のセッションが含まれています。CLI を使用して、フィルターあり/なしで、セッションを一覧表示できます。セッション履歴は JSON として配信され、管理者は個別のリポジトリで処理、管理、保存できます。

US-West-2 (オレゴン) リージョンでセッションを管理するための CLI コマンドの例を以下に示します。

ウェブポータルのすべてのセッションを一覧表示するには、以下のコマンドを実行します。

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

ウェブポータルの特定のユーザーのすべてのセッションを一覧表示するには、以下のコマンドを実行します。

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

FIPS エンドポイントと Amazon WorkSpaces Secure Browser を使用した転送中のデータの保護

デフォルトでは、コンソール、コマンドラインインターフェイス (AWS CLI)、または AWS SDK AWS を使用して、またはユーザーのセッション中に、管理者として WorkSpaces Secure Browser サービスと通信する場合、転送中のすべてのデータは TLS 1.2 を使用して暗号化されます。

コマンドラインインターフェイスまたは API を使用して 「 AWS 」 にアクセスする際に FIPS 140-3 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。FIPS エンドポイントを使用すると、すべての転送中のデータは、Federal Information Processing Standard

(FIPS) 140-3 に準拠した暗号化標準を使用して暗号化されます。WorkSpaces Secure Browser エンドポイントのリストを含め FIPS エンドポイントの詳細については、「https://aws.amazon.com/compliance/fips」を参照してください。

FIPS エンドポイントでポータルが作成されると、すべてのユーザーセッションと管理上の変更は、FIPS 140-3 エンドポイントを使用して自動的に行われます。AWS_USE_FIPS_ENDPOINT=true 環境変数を使用して FIPS エンドポイントを特定し、SDK を使用してリクエストを送信できます。以下に例を示します。

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

–endpoint-url オプションを使用して FIPS エンドポイントに直接リクエストを送信することもできます。US-West-2 (オレゴン) リージョンでポータルを一覧表示する呼び出しの例を以下に示します。

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

Amazon WorkSpaces Secure Browser でのデータ保護設定の管理

データ保護設定は、セッション中にデータを共有しないように保護するために使用されます。設定を作成して複数のポータルに適用できます。

トピック

- Amazon WorkSpaces Secure Browser でのインラインデータ秘匿化
- Amazon WorkSpaces Secure Browser のデフォルトの秘匿化設定
- Amazon WorkSpaces Secure Browser の基本インラインリダクション
- Amazon WorkSpaces Secure Browser でのカスタムインラインリダクション
- Amazon WorkSpaces Secure Browser でデータ保護設定を作成する
- Amazon WorkSpaces Secure Browser でデータ保護設定を関連付ける
- Amazon WorkSpaces Secure Browser でデータ保護設定を編集する

- Amazon WorkSpaces Secure Browser でデータ保護設定を削除する

Amazon WorkSpaces Secure Browser でのインラインデータ秘匿化

インラインデータリダクションをポータルに追加することで、ウェブページに表示されるテキスト文字列から特定のデータを自動的に予測および編集できます。秘匿化ポリシーを作成するには、組み込みパターン (社会保障番号やクレジットカード番号など) から選択するか、正規表現とキーワードを使用して独自のカスタムデータ型を作成できます。ポリシーには、秘匿化を適用する必要がある URLs の設定可能なレベルの適用とコントロールが含まれます。

以下のコンポーネントは、データが秘匿化されるタイミングを決定します。

- データ保護設定 - データ保護設定は、データ型と適用基準を含むリソースの名前です。このリソースを使用するには、まず設定を作成し、ポータルに関連付けます。ユーザーがセッションを起動すると、セッション中に設定が適用されます。
- セッション内ブラウザ拡張機能 - 秘匿化設定をポータルに関連付けると、セッションブラウザは、設定を適用するシステム強制ブラウザ拡張機能で起動します。データ保護設定では、信頼度と URL の適用設定に従って、パターンマッチング (正規表現) とキーワード検索によって秘匿化を適用します。コンテンツはテキスト文字列から予測され、画面に表示される前に編集されます。拡張機能は、秘匿化 (無効化されたプライベートブラウジング、デベロッパーツールへのアクセス、ネットワーク検査など) を回避するユーザーの機能を管理する関連するブラウザポリシーも設定します。

次の Chrome ブラウザポリシーの変更は、セッション内ブラウザ拡張機能によって適用されます。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。

- ブラウザポリシーを適用して、ユーザーが編集せずにセッションを表示できないようにします。
  - IncognitoModeAvailability = 1
  - DeveloperToolsAvailability = 2
  - BrowserAddPersonEnabled = false
  - BrowserGuestModeEnabled = false
- また、 拡張機能は、ダウンロードイベントをキャンセルすることで、データ保護設定を適用している URLs からユーザーが HTML ファイルをダウンロードできないようにします。

一般に、構造化されていないパブリックブラウジング (Facebook や Google など) ではなく、構造化されたプライベートウェブサイト (カスタマー管理ツール、チケットシステム、Wiki など) で秘匿化

を使用する必要があります。組み込みのデータ型から選択することも (完全なリストについては以下を参照) 、独自の正規表現の値とキーワードを使用してカスタムデータ型を定義することもできます。管理者は、各データ型、信頼度、URL の適用が期待どおりに機能していることをテストおよび検証する責任があります。 AWS は、サードパーティーが提供するカスタムウェブサイトやアプリケーションとの互換性を保証することはできません。

WorkSpaces Secure Browser は現在、以下の形式のテキストを含む、テキスト以外の形式のサポートされているデータ型またはカスタムデータ型の秘匿化をサポートしていません。

- JPEG、PNG、GIF などのイメージ
- Google ドキュメントやシートなど、ユーザーが動的な単語処理や編集を使用できるようにするウェブページ
- YouTube 動画など、ブラウザでアクセスされるオーディオストリームまたはビデオストリーム
- Chrome ブラウザで表示される PDFs

サポートされていない形式のコンテンツには秘匿化を使用しないでください。管理者は、秘匿化する予定のコンテンツへのアクセス権をユーザーに付与する前に、サイトとコンテンツの互換性を検証する責任があります。

Amazon WorkSpaces Secure Browser のデフォルトの秘匿化設定

デフォルトの秘匿化設定では、データ保護設定のすべての組み込みデータ型に信頼レベルと URL 適用が自動的に適用されます。組み込みデータ型を追加するときに、デフォルト設定を上書きするオプションがあります。

信頼度レベルを使用すると、形式、キーワード、およびフォーマットされていないテキストを組み合わせて、組み込みデータ型の秘匿化ロジックを微調整できます。高、中、低など、秘匿化の適用方法の厳格度を選択します。データ型レベルでオーバーライドが適用されない限り、デフォルト値はすべてのデータ型に適用されます。一般的に、デフォルト設定の Medium から始めて、サイトに期待どおりに秘匿化が適用されていることを検証して絞り込みます。

信頼度	説明	例
高	コンテンツを秘匿化するには、フォーマットされたテキストパターンの一致が必要です。	123-45-6798 の SSN は秘匿化されますが、123456789 は秘匿化されません。

信頼度	説明	例
Medium	リダクションでは、フォーマットされたテキストとフォーマットされていないテキストの両方が考慮され、ロジックにキーワードの関連付けが追加されます。	123-45-6798 の SSN は編集されます。123456789 は、キーワード (「社会保障番号」など) の近くで検出された場合に編集されます。
低	フォーマットされたパターン + キーワードなしのフォーマットされていないパターンの両方に適用されるリダクション。	SSN 形式 - 123-45-6798 および 123456789 - キーワードを必要とせずに編集されます。

すべてのデータ型にデフォルトの秘匿化設定を設定する必要があります。次のオプションから選択できます。

- すべての URLs
- 特定の URLs
- 高度な設定

データ型レベルでオーバーライドが適用されない限り、デフォルト値はすべてのデータ型に適用されます。URL の適用では、許可リストとブロックリストを管理するために Chrome ポリシーと同様のロジックを使用します。ブロック URL と許可 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形式」を参照してください。

Amazon WorkSpaces Secure Browser の基本インラインリダクション

インラインデータリダクションでは、組み込みパターン (社会保障番号やクレジットカード番号など) がサポートされています。このパターンは、「基本インラインリダクション」に記載されています。ドロップダウンメニューからデータ型 (複数可) を選択し、各データ型の置換値を指定します。すべてのデータ型は上記のデフォルトの設定適用パターンに従いますが、信頼レベルを上書きし、各データ型のドメイン適用パターンを微調整することを選択できます。

デフォルト設定の代替値を入力するには、信頼レベルのオーバーライドを選択します。例えば、デフォルト設定を Medium に設定すると、テスト中に、いずれかのデータ型が確実に編集されていないことに気付くことがあります。オーバーライドを低に設定すると、他のデータ型に使用される口ジックを調整することなく、秘匿化の可能性を高めることができます。

デフォルト設定を変更せずに URLs 間でリダクションを適用する方法を微調整するには、URL 適用オーバーライドを適用します。例えば、URL オーバーライドを使用して、企業ディレクトリウェブサイトやウェブベースの E メールの E メールアドレスへのユーザーアクセスを損なうことなく、顧客関係管理システムで E メールアドレスの秘匿化を適用できます。

以下は、データ型とそれに対応する組み込みパターン IDs。

builtInPatternId	データ型
awsAccessKey:	AWS アクセスキー
awsSecretKey:	AWS シークレットキー
cardNumbers:	クレジットカード番号
暗号：	暗号通貨アドレス
cusipNum:	CUSIP 番号
日付：	日付
deaNum:	米国 DEA 番号
dob:	生年月日
driversLicense:	米国運転免許証
emailAddress:	E メールアドレス
ein:	米国の雇用主識別番号
expDate:	クレジットカードの有効期限
healthInsuranceNum:	メディケア健康保険請求番号
hipaaCode:	HIPAA ICD-10 コード

builtInPatternId	データ型
indivTaxId:	米国個人税 ID
ipAddr:	IP アドレス
isin:	国際証券識別番号
jwt:	JSON ウェブトークン
locationCoord:	位置座標
macAddr:	MAC アドレス
medicareBeneficiaryId:	メディケア受取人番号
npi:	国内プロバイダー識別番号
ndc:	国民医薬品コード (NDC)
passportNum:	米国のパスポート番号
phoneNum:	電話番号
routingNumber:	ABA ルーティング番号
ssn:	米国の社会保障番号
swiftCode:	SWIFT コード
時間：	時間
ビン：	米国車両識別番号

Amazon WorkSpaces Secure Browser でのカスタムインラインリダクション

お客様は、カスタムの内部アプリケーション IDs などの正規表現を使用して独自のパターンを定義できます。カスタムインラインリダクションパターンを作成するには、次の手順に従います。

1. データ保護設定に移動します。
2. カスタムインラインリダクションを選択して追加します。
3. カスタムデータ型の名前を入力します。
4. 正規表現の値を入力します。
   - 正規表現の値は、JavaScript 正規表現リテラル構文と一致する必要があります。詳細については、「正規表現」を参照してください。正規表現の例は です`/ex[am]+ple/i`。
   - サポートする予定のウェブサイトでカスタムパターンをテストしてください。カスタムパターンが エラーで書き込まれると、意図しないパフォーマンスの問題が発生する可能性があります。
5. 置換値を指定します。
6. その他のオプションカスタマイズには、以下を含むその他のオプションを選択します。
   - キーワードを追加して、秘匿化ロジックを微調整します。キーワードを使用すると、適用の精度を高めることができます。Javascript 正規表現リテラル構文にキーワードを追加します。詳細については、「正規表現」を参照してください。

     たとえば、内部システムで使用されるクライアント IDs のカスタムリダクションパターンを作成する場合は、`/client name/i`キーワードフィールドに を追加して、スキャンと検出の ロジックを通知できます。
   - URL 適用オーバーライドを適用して、デフォルト設定を変更せずに URLs URL 間で秘匿化を適用する方法を微調整します。

     例えば、URL オーバーライドを使用して、企業ディレクトリウェブサイトやウェブベースの E メールの E メールアドレスへのユーザーアクセスを損なうことなく、顧客関係管理システムで E メールアドレスの秘匿化を適用できます。
   - データ型の説明 (オプション) を入力します。

Amazon WorkSpaces Secure Browser でデータ保護設定を作成する

WorkSpaces Secure Browser でデータ保護設定を作成できます。

データ保護設定を作成するには

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. 左側のナビゲーションペインで、データ保護設定を選択します。

3. データ保護設定の作成 を選択します。
4. 設定の表示名 (必須) と説明 (オプション) を入力します。
5. インラインリダクションのデフォルト設定を選択します。以下を設定できます。
   - すべてのデータ型の厳密性のレベル
   - 秘匿化を適用するドメイン
6. サポートされている型からベースインラインリダクションデータ型を選択するか、カスタムデータ型を作成します。厳格度やドメイン例外のレベルなど、各データ型にオーバーライドを設定できます。
7. レポート用のタグ (オプション) を追加します。
8. 完了したら、[Save] を選択します。

Amazon WorkSpaces Secure Browser でデータ保護設定を関連付ける

WorkSpaces Secure Browser でデータ保護設定を関連付けることができます。

データ保護設定を既存のポータルに関連付けるには

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. 左側の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. データ保護設定で、ポータルの設定を選択します。
5. [Save] を選択します。

新しいポータルの作成時にデータ保護設定を関連付けるには、次の手順に従います。

新しいポータルの作成時にデータ保護設定を関連付けるには

1. the section called “ウェブポータルの作成” 「」の手順に従って、データ保護設定に到達するまでポータルを作成します。
2. ドロップダウンメニューからデータ保護設定を選択します。
3. のステップを完了the section called “ウェブポータルの作成”して、ポータルの作成を完了します。

新しいポータルの作成時にデータ保護設定を作成するには、次の手順に従います。

新しいポータルの作成時にデータ保護設定を作成するには

1. the section called “ウェブポータルの作成” 「」の手順に従って、データ保護設定に到達するまでポータルを作成します。
2. ドロップダウンメニューからデータ保護設定を選択します。
3. 設定の表示名 (必須) と説明 (オプション) を入力します。
4. インラインリダクションのデフォルト設定を選択します。以下を設定できます。
   - すべてのデータ型の厳密性のレベル
   - 秘匿化を適用するドメイン
5. サポートされている型からベースインラインリダクションデータ型を選択するか、カスタムデータ型を作成します。厳格度やドメイン例外のレベルなど、各データ型にオーバーライドを設定できます。
6. レポート用のタグ (オプション) を追加します。
7. 完了したら、[Save] を選択します。
8. データ保護設定の更新ボタンを選択し、ドロップダウンメニューからデータ保護設定を選択します。
9. ポータルの作成手順に引き続き従って、ポータルの作成を完了します。

Amazon WorkSpaces Secure Browser でデータ保護設定を編集する

WorkSpaces Secure Browser でデータ保護設定を編集できます。

データ保護設定を編集するには

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. リストビューから、データ保護設定と編集するデータ保護設定を選択します。
3. 名前、説明、デフォルト設定、データ型 (サポートまたはカスタム) を更新し、信頼レベルまたはドメインオーバーライドを適用できます。
4. [Save] を選択します。

Amazon WorkSpaces Secure Browser でデータ保護設定を削除する

WorkSpaces Secure Browser でデータ保護設定を削除できます。

データ保護設定を削除するには

1. データ保護設定に関連付けられたポータルがある場合は、データ保護設定を削除する前に、まず関連付けを削除する必要があります。
2. 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。
3. リストビューから、データ保護設定と削除するデータ保護設定を選択します。
4. [削除] を選択します。

Amazon WorkSpaces Secure Browser でのツールバーコントロールの管理

ツールバーコントロールを使用すると、以下のオプションを含め、エンドユーザーセッションのツールバー表示を設定できます。

- 特徴
  - クリップボード: 有効にすると、きめ細かなコントロール (コピーのみ、貼り付けのみ、またはその両方) によるコピー/貼り付けが許可されます。無効にすると、アイコンが非表示になり、ツールバーの使用が禁止されます。
  - ファイル転送: 有効にすると、きめ細かな制御 (アップロードのみ、ダウンロードのみ、またはその両方) によるファイルオペレーションが可能になります。無効にすると、アイコンが非表示になり、転送が禁止されます。
  - マイク: 有効にすると、マイクの使用が許可されます。無効にすると、アイコンが非表示になります。
  - ウェブカメラ: 有効にすると、カメラの使用が許可されます。無効にすると、アイコンが非表示になります。
  - デュアルモニター: 有効にすると、デュアルモニターの使用が許可されます。無効にすると、アイコンが非表示になります。
  - 全画面表示: 有効にすると、全画面表示モードが許可されます。無効にすると、アイコンが非表示になります。

  - Windows: 有効にすると、ウィンドウ間の移動が許可されます。無効にすると、アイコンが非表示になります。
- 設定
  - ツールバーテーマ: ライトモードまたはダークモードの表示を制御します。設定により、エンドユーザーテーマコントロールが削除されます。
  - ツールバーの状態: ツールバーのドッキング状態またはデタッチ状態を設定します。設定により、ツールバーの状態に対するエンドユーザーの制御が削除されます。
  - 最大解像度: 許容される最大表示解像度を定義します。ユーザーは、この定義された制限までの解像度のみを選択できます。

Amazon WorkSpaces Secure Browser でのセキュリティ

でのクラウドセキュリティが最優先事項 AWS です。 AWS のお客様は、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 とお客様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 – AWS 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 AWS 責任があります。 AWS また、 は、お客様が安全に使用できるサービスも提供します。AWS コンプライアンス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対象範囲内の AWS のサービス」を参照してください。
- クラウド内のセキュリティ – 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法を理解するのに役立ちます。ここでは、セキュリティとコンプライアンスの目標を満たすように 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 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 に関するセキュリティベストプラクティス

Amazon WorkSpaces Secure Browser におけるデータ保護

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。ユーザーは、このインフラストラクチャでホストされ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 のサービス 」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に関するよくある質問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に投稿された AWS 責任共有モデルおよび GDPR の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 (IAM) 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。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。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- で 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。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」のCloudTrail 証跡の使用」を参照してください。
- AWS 暗号化ソリューションと、その中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 のサービス。
- Amazon Macie などの高度な管理された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 API AWS を介して にアクセスするときに FIPS 140-3 検証済み暗号化モジュールが必要な場合は、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を、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含めないことを強くお勧めします。これは、コンソール、API、または SDK を使用して WorkSpaces Secure Browser AWS CLIまたは他の AWS のサービス を操作する場合も同様です。 AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する

場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

トピック

Amazon WorkSpaces Secure Browser でのデータ暗号化

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、信頼ストアデータ、信頼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)、および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 の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ます。これにより、WorkSpaces Secure Browser は保管中のデータを指定したキーで暗号化できます。
- 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、企業の社内ウェブサイトや SaaS アプリケーションにもアクセスできません。

Amazon WorkSpaces Secure Browser の保管時の暗号化

保管時の暗号化はデフォルトで設定され、WorkSpaces Secure Browser で使用されるすべての顧客データ (ブラウザポリシーステートメント、ユーザー名、ログ記録、IP アドレスなど) は を使用して暗号化されます AWS KMS。デフォルトでは、WorkSpaces Secure Browser は AWS所有キーによる暗号化を有効にします。リソースの作成時にカスタマーマネージドキー (CMK) を指定することで、CMK を使用することもできます。CMK は現在 CLI を通じてのみサポートされています。

CMK を渡すことを選択した場合、提供されるキーは対称暗号化 AWS KMS キーである必要があり、管理者には次のアクセス許可が必要です。

```
kms:DescribeKey

kms:GenerateDataKey

kms:GenerateDataKeyWithoutPlaintext

kms:Decrypt

kms:ReEncryptTo
kms:ReEncryptFrom
```

CMK を使用する場合は、キーにアクセスできるように、WorkSpaces Secure Browser 外部サービスプリンシパルを許可リストに追加する必要があります。
詳細については、「aws:SourceAccount を使用したスコープ付き CMK キーポリシーの例」を参照してください。

可能な場合、WorkSpaces Secure Browser は Forward Access Sessions (FAS) 認証情報を使用してキーにアクセスします。FAS の詳細については、「Forward Access Sessions」を参照してください。
WorkSpaces Secure Browser がキーに非同期にアクセスする必要がある場合があります。お客様のキーポリシーで WorkSpaces Secure Browser 外部サービスプリンシパルを許可リストに追加することで、WorkSpaces Secure Browser は許可リストに含まれる暗号化オペレーションをお客様のキーで実行できるようになります。

リソースの作成後は、キーを削除したり変更したりすることはできません。CMK を使用した場合、リソースにアクセスする管理者として、以下のアクセス許可が必要です。

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

kms:ReEncryptTo
kms:ReEncryptFrom
```

コンソール使用時にアクセス拒否エラーが表示される場合、コンソールにアクセスしているユーザーに、使用中のキーで CMK を使用するためのアクセス許可がない可能性があります。

WorkSpaces Secure Browser のキーポリシーとスコープの例

CMK には、以下のキーポリシーが必要です。

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

WorkSpaces Secure Browser には、以下のアクセス許可が必要です。

- `kms:DescribeKey` — 指定された AWS KMS キーが正しく設定されていることを確認します。

- kms:GenerateDataKeyWithoutPlaintext および kms:GenerateDataKey — オブジェクトの暗号化に使用されるデータ AWS KMS キーを作成するためのキーをリクエストします。
- kms:Decrypt — 暗号化されたデータ AWS KMS キーを復号するキーをリクエストします。これらのデータキーはデータの暗号化に使用されます。
- kms:ReEncryptTo および kms:ReEncryptFrom — KMS AWS KMS キーとの間での再暗号化を許可するキーをリクエストします。

AWS KMS キーに対する WorkSpaces Secure Browser アクセス許可の範囲設定

キーポリシーステートメントのプリンシパルが AWS のサービスプリンシパルである場合は、暗号化コンテキストに加えて、aws:SourceArn または aws:SourceAccount グローバル条件キーを使用することを強くお勧めします。

リソースに使用される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。

ソース ARN とソースアカウントの値は、リクエストが別の AWS サービス AWS KMS から に送信された場合にのみ、認可コンテキストに含まれます。この条件の組み合わせにより、最小特権のアクセス許可が実装され、可能性のある「混乱した代理」シナリオが回避されます。詳細については、「キーポリシーにおける AWS のサービスのアクセス許可」を参照してください。

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

> **Note**
>
> リソースの作成前は、完全なリソース ARN がまだ存在しないため、キーポリシーでは aws:SourceAccount Condition のみを使用する必要があります。リソースの作成後、キー

ポリシーを更新して aws:SourceArn および kms:EncryptionContext Condition を含めることができます。

aws:SourceAccount を使用したスコープ付き CMK キーポリシーの例

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

aws:SourceArn とリソースワイルドカードを使用したスコープ付き CMK キーポリシーの例

```
{
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
```

```
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:workspaces-web:<Region>:<AccountId>:*/*"
        }
      }
    }
  ]
}
```

aws:SourceArn を使用したスコープ付き CMK キーポリシーの例

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

```
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:workspaces-web:<Region>:<AccountId>:portal/*",
            "arn:aws:workspaces-web:<Region>:<AccountId>:browserSettings/*",
            "arn:aws:workspaces-web:<Region>:<AccountId>:userSettings/*",
            "arn:aws:workspaces-web:<Region>:<AccountId>:ipAccessSettings/*"
          ]
        }
    }
  ]
}
```

> **Note**
>
> リソースを作成した後、その SourceArn のワイルドカードを更新できます。WorkSpaces Secure Browser を使用して、CMK アクセスが必要な新しいリソースを作成する場合は、それに応じてキーポリシーを更新してください。

aws:SourceArn とリソース固有の **EncryptionContext** を使用したスコープ付き CMK キーポリシーの例

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

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

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

> **Note**
>
> 同じキーポリシーにリソース固有の EncryptionContext を含める場合は、個別のステートメントを作成してください。詳細については、kms:EncryptionContext:context-key で「複数の暗号化コンテキストペアの使用」セクションを参照してください。

Amazon WorkSpaces Secure Browser での転送中の暗号化

WorkSpaces Secure Browser は、HTTPS と TLS 1.2 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 呼び出しを使用して WorkSpaces 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、すべてを HTTPS または TLS 接続経由で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 から WorkSpaces Secure Browser に転送できます。

転送時の暗号化はデフォルトで構成され、安全な接続 (HTTPS、TLS) はデフォルトで構成されます。

Amazon WorkSpaces Secure Browser でのキー管理

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。 AWS SDK を使用してキーを設定できます。

Amazon WorkSpaces Secure Browser での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 VPC 内でブラウザセッションを開始します。オンプレミスアプリケーションへの接続は独自の VPC で設定され、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 はサービスリンクロールを使用してカスタマーアカウントに安全に接続し、カスタマー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、「Amazon WorkSpaces Secure Browser のサービスリンクロール」を参照してください。

Amazon WorkSpaces Secure Browser での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。ユーザーアクセスログからの閲覧情報は AWS、ログ記録が設定されていないセッションによって保存されたり、セッションから利用されたりすることはありません。シークレットモードでの URL 訪問、またはブラウザ履歴から削除された URL は、ユーザーアクセスロギングに記録されません。

Amazon WorkSpaces Secure Browser の ID およびアクセス管理

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 のサービス するのに役立つ です。IAM 管理者は、WorkSpaces Secure Browser リソースを使用するための認証 (サインイン) と認可 (アクセス許可の保有) ができる人を制御します。IAM は、追加料金なしで AWS のサービス 使用できる です。

トピック

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 - 作業を行うために WorkSpaces Secure Browser サービスを使用する場合は、管理者から必要な認証情報とアクセス許可が提供されます。WorkSpaces Secure Browser のさらに多くの機能を使用して作業を行う場合は、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解すると、管理者に適切なアクセス許可をリクエストするのに役に立ちます。WorkSpaces Secure Browser の機能にアクセスできない場合は、「Amazon WorkSpaces Secure Browser ID とアクセスのトラブルシューティング」を参照してください。

サービス管理者 - 会社で WorkSpaces Secure Browser リソースを担当している場合は、おそらく WorkSpaces Secure Browser へのフルアクセス権があります。サービスユーザーがアクセスすべき WorkSpaces Secure Browser の機能やリソースを決定するのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。会社で WorkSpaces Secure Browser とともに

IAM を使用する方法の詳細については、「Amazon WorkSpaces Secure Browser と IAM との連携方法」を参照してください。

IAM 管理者 - IAM 管理者であれば、WorkSpaces Secure Browser へのアクセスを管理するためのポリシーの作成方法について詳細を確認することが必要になる場合があります。IAM で使用できる WorkSpaces Secure Browser のアイデンティティベースのポリシーの例は、「Amazon WorkSpaces Secure Browser のアイデンティティベースのポリシーの例」で確認してください。

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 AWS アカウントのルートユーザー、IAM ユーザーとして、または IAM ロールを引き受けて認証 (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 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場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーションを使用して にアクセスすると、間接的 AWS 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、「 AWS サインイン ユーザーガイド」の「 にサインインする方法 AWS アカウント」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 Software Development Kit (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。リクエストに自分で署名する推奨方法の使用については、「IAM ユーザーガイド」の「API リクエストに対するAWS Signature Version 4」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、 では、アカウントのセキュリティを強化するために多要素認証 (MFA) を使用する AWS 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「IAM ユーザーガイド」の「IAM のAWS 多要素認証」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 の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「ルートユーザー認証情報が必要なタスク」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が、一時的な認証情報 AWS のサービス 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 ID ソースを通じて提供された認証情報 AWS のサービス 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、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、「AWS IAM Identity Center ユーザーガイド」の「What is IAM Identity Center?」(IAM Identity Center とは) 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、1 人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保有する IAM ユーザーを作成する代わりに、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 ユーザーでの長期的な認証情報が必要な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、「IAM 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のためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団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、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する許可を与えることができます。

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、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」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。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。で IAM ロールを一時的に引き受けるには AWS Management Console、ユーザーから IAM ロールに切り替えることができます (コンソール) 。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 URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールと一時的な認証情報は、次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については、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center User Guide」の「Permission sets」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで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、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、 (ロールをプロキシとして使用する代わりに) リソースに直接ポリシーをアタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。
- クロスサービスアクセス — 一部の では、他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2

でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。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と AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストリクエストを使用します。FAS リクエストは、サービスが他の AWS のサービス 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アクセス許可が必要です。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 - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除することができます。詳細については、「IAM ユーザーガイド」の「AWS のサービスに許可を委任するロールを作成する」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 のサービス。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、サービスリンク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 EC2 で実行されているアプリケーション – 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 リクエストを実行している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 インスタンス内でのアクセスキーの保存に推奨されます。EC2 インスタンスに AWS ロールを割り当て、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、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、「IAM ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与する」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には AWS 、ポリシーを作成し、ID AWS またはリソースにアタッチします。ポリシーは のオブジェクト AWS であり、アイデンティティまたはリソースに関連付けられると、

そのアクセス許可を定義します。 は、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) がリクエストを行うときに、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、IAM ユーザーガイドの JSON ポリシー概要を参照してください。

管理者は JSON AWS ポリシーを使用して、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。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、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方法を問わず、アクションの許可を定義します。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 API からロール情報を取得できます。

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ポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 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ポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」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。マネージドポリシーまたはインラインポリシーのいずれ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いずれかを選択する」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、リソースに添付する 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には例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。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制御できます。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 のサービス。

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では、IAM の AWS マネージド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 (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL 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は使用しません。

Amazon S3、 AWS WAF、および Amazon VPC は、ACLs。ACL の詳細については、「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ています。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ポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限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) の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、ビジネスが所有する複数の AWS アカウント 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 (SCP) を一部またはすべてのアカウントに適用できます。SCP 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を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー (SCP)」を参照してください。

- リソースコントロールポリシー (RCP) – RCP は、所有する各リソースにアタッチされた IAM ポリシーを更新することなく、アカウント内のリソースに利用可能な最大数のアクセス許可を設定するために使用できる JSON ポリシーです。RCP は、メンバーアカウントのリソースのアクセス許可を制限し、組織に属しているかどうかにかかわらず AWS アカウントのルートユーザー、 を含む ID の有効なアクセス許可に影響を与える可能性があります。RCP をサポートする のリストを含む Organizations と RCP の詳細については、AWS Organizations RCPs「リソースコントロールポリシー (RCPs」を参照してください。 AWS のサービス
- 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、「IAM ユーザーガイド」の「セッションポリシー」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係する場合に が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、「IAM ユーザーガイド」の「ポリシー評価ロジック」を参照してください。

Amazon WorkSpaces Secure Browser と IAM との連携方法

IAM を使用して WorkSpaces Secure Browser へのアクセスを管理する前に、WorkSpaces Secure Browser で使用できる IAM の機能を理解しておきましょう。

Amazon WorkSpaces Secure Browser で使用できる IAM 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ポリシー	はい
リソースベースのポリシー	いいえ
ポリシーアクション	はい
ポリシーリソース	あり

IAM 機能	WorkSpaces Secure Browser のサポート
ポリシー条件キー	Yes
ACL	いいえ
ABAC (ポリシー内のタグ)	部分的
一時的な認証情報	はい
プリンシパル権限	はい
サービスロール	いいえ
サービスリンクロール	はい

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 「IAM と連携する のサービス」を参照してください。

トピック

- WorkSpaces Secure Browser のアイデンティティベースのポリシー
- WorkSpaces Secure Browser のリソースベースのポリシー
- WorkSpaces Secure Browser のポリシーアクション
- WorkSpaces Secure Browser のポリシーリソース
- WorkSpaces Secure Browser のポリシー条件キー
- WorkSpaces Secure Browser のアクセスコントロールリスト (ACL)
- WorkSpaces Secure Browser での属性ベースのアクセス制御 (ABAC)
- WorkSpaces Secure Browser での一時的な認証情報の使用
- WorkSpaces Secure Browser のクロスサービスプリンシパルアクセス許可
- WorkSpaces Secure Browser のサービスロール
- WorkSpaces Secure Browser のサービスリンクロール

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

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 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。ID ベースのポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」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、許可または拒否するアクションとリソース、およびアクションを許可または拒否す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学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」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は、「Amazon WorkSpaces Secure Browser のアイデンティティベースのポリシーの例」で確認してください。

WorkSpaces Secure Browser 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、リソースに添付する 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には例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。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制御できます。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 のサービス。

クロスアカウントアクセスを有効にするには、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。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場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、リソースにアクセスするためのアクセス許可をプリンシパルエンティティ (ユーザーまたはロール) に付与する必要もあります。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、「IAM ユーザーガイド」の「IAM でのクロスアカウントリソースアクセス」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 JSON AWS ポリシーを使用して、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` 要素にはポリシー内の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が記述されます。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 オペレーションのない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アクセス許可を付与するポリシーで使用されます。

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

WorkSpaces Secure Browser のポリシーアクションは、アクションの前に以下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は、「Amazon WorkSpaces Secure Browser のアイデンティティベースのポリシーの例」で確認してください。

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 JSON AWS ポリシーを使用して、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。

`Resource` JSON ポリシー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 リソースのタイプとその ARN のリストを確認するには、サービス認可リファレンスの「Amazon WorkSpaces Secure Browser で定義されているリソース」を参照してください。各リソースの ARN を指定できるアクションについては、「Amazon WorkSpaces Secure Browser で定義されているアクション」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は、「Amazon WorkSpaces Secure Browser のアイデンティティベースのポリシーの例」で確認してください。

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 JSON AWS ポリシーを使用して、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して、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 IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、「IAM ユーザーガイド」の「IAM ポリシーの要素: 変数およびタグ」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ています。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「 グローバル条件コンテキストキー」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、サービス認可リファレンスの「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 で定義されているアクション」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は、「Amazon WorkSpaces Secure Browser のアイデンティティベースのポリシーの例」で確認してください。

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

ACL のサポート: なし

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL 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は使用しません。

WorkSpaces Secure Browser での属性ベースのアクセス制御 (ABAC)

ABAC (ポリシー内のタグ) のサポート: 一部

属性ベースのアクセス制御 (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、ABAC の最初の手順です。その後、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した場合にオペレーションを許可するように ABAC ポリシーをします。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

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。

ABAC の詳細については、「IAM ユーザーガイド」の「ABAC 認可でアクセス許可を定義する」を参照してください。ABAC の設定手順を説明するチュートリアルについては、IAM ユーザーガイドの「属性ベースのアクセス制御 (ABAC) を使用する」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 AWS のサービス は、一時的な認証情報を使用してサインインすると機能しません。一時的な認証情報 AWS のサービス を使用する機能などの詳細については、AWS のサービス「IAM ユーザーガイド」の「IAM と連携する」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。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「ユーザーから IAM ロールに切り替える (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 AWS API を使用して手動で作成できます。その後、これらの一時的な認証情報を使用してアクセスすることができます AWS。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 AWS を動的に生成することをお勧めします。詳細については、「IAM の一時的セキュリティ認証情報」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アクセス許可

転送アクセスセッション (FAS) のサポート: あり

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と AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストリクエストを使用します。FAS リクエストは、サービスが他の AWS のサービス 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アクセス許可が必要です。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

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスに許可を委任するロールを作成する」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 の機能が阻害され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 のサービスリンクロール

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 のサービス。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、「IAM と提携するAWS のサービス」を参照してください。表の「サービスリンクロール」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。

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、ユーザーおよびロールには、WorkSpaces Secure Browser リソースを作成または変更するための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 AWS API を使用してタスクを実行することはできません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

これらサンプルの JSON ポリシードキュメントを使用して、IAM 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、「IAM ユーザーガイド」の「IAM ポリシーを作成する (コンソール)」を参照してください。

WorkSpaces Secure Browser が定義するアクションとリソースタイプ (リソースタイプごとの ARN の形式を含む) の詳細については、サービス認可リファレンスの「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

- Amazon WorkSpaces Secure Browser のアイデンティティベースのポリシーに関するベストプラクティス
- Amazon WorkSpaces Secure Browser コンソールの使用
- ユーザーに Amazon WorkSpaces Secure Browser に対する自分のアクセス許可を表示できるようにする

Amazon WorkSpaces Secure Browser のアイデンティティベースのポリシーに関するベストプラクティス

アイデンティティ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、または削除できるか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、「IAM ユーザーガイド」の「AWS マネージドポリシー」または「ジョブ機能のAWS マネージドポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な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 を使用して許可を適用する

方法の詳細については、「IAM ユーザーガイド」の「IAM でのポリシーとアクセス許可」を参照してください。

- IAM ポリシーで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、アクションや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 SSL を使用して送信するように指定できます。条件を使用して、サービスアクションが などの特定の を通じて使用される場合に AWS のサービス、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、「IAM ユーザーガイド」の「IAM JSON ポリシー要素:条件」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、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer でポリシーを検証する」を参照してください。
- 多要素認証 (MFA) を要求する – 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するために MFA を有効にします。API オペレーションが呼び出されるときに MFA を必須にするには、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 を使用した安全な API アクセス」を参照してください。

IAM で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 IAM でのセキュリティのベストプラクティスを参照してください。

Amazon 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、 AWS アカウントの WorkSpaces Secure Browser リソースのリストと詳細を表示できます。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 AWS API 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。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のみへのアクセスが許可されます。

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、エンティティに WorkSpaces Secure Browser `ConsoleAccess`または `ReadOnly` AWS 管理ポ

リシーもアタッチします。詳細については、「IAM ユーザーガイド」の「ユーザーへのアクセス許可の追加」を参照してください。

ユーザーに Amazon WorkSpaces Secure Browser に対する自分のアクセス許可を表示できるようにする

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API 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。

```
{
    "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。チームに必要な権限のみを提供する 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 管理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 管理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破損す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管理ポリシー AWS をサポートします。例えば、 `ReadOnlyAccess` AWS マネージドポリシーは、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に読み取り専用アクセス許可 AWS を追加します。ジョブ機能ポリシーのリストと説明については、IAM ユーザーガイドのジョブ機能のAWS 管理ポリシーを参照してください。

トピック

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、ユーザーに代わって WorkSpaces Secure Browser がアクションを実行することを許可する、サービスリンクロールにアタッチされます。詳細については、「the section called “サービスにリンクされたロールの使用”」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 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。

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 – WorkSpaces Secure Browser が使用または管理する AWS サービスと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グの設定”」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 ポリシーを IAM アイデンティティ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、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、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 ポリシーを IAM アイデンティティ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、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、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 Secure Browser の AWS マネージドポリシーへの更新

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 で、AWS マネジメントコンソール、SDK、CLI を通じて WorkSpaces Secure Browser とその依存関係への読み取り専用アクセス権を与えるための、新しいポリシーが追加されました。	2024 年 6 月 24 日
AmazonWorkSpacesWebServiceRolePolicy – ポリシーの更新	WorkSpaces Secure Browser でポリシーが更新されて、CreateNetworkInterface の対象を aws:RequestTag/WorkSpacesWebManaged:	2022 年 12 月 15 日

変更	説明	日付
	true でタグ付けされたサブネットとセキュリティグループのリソースに制限するようになりました。また、DeleteNetworkInterface の対象を aws:ResourceTag/WorkSpacesWebManaged: true でタグ付けされた ENI に制限するようになりました。	
AmazonWorkSpacesWebReadOnly – ポリシーの更新	WorkSpaces Secure Browser で、ユーザーアクセスロギングの読み取りアクセス許可を付与し、Kinesis データストリームの一覧表示を許可するように、ポリシーが更新されました。詳細については、「the section called “ユーザーアクセスログの設定”」を参照してください。	2022 年 11 月 2 日
AmazonWorkSpacesWebServiceRolePolicy – ポリシーの更新	WorkSpaces Secure Browser で、Kinesis データストリームの概要を記述し、レコードをユーザーアクセスロギング用に Kinesis データストリームに入力するように、ポリシーが更新されました。詳細については、「the section called “ユーザーアクセスログの設定”」を参照してください。	2022 年 10 月 17 日

変更	説明	日付
AmazonWorkSpacesWebServiceRolePolicy – ポリシーの更新	WorkSpaces Secure Browser で、ENI の作成中にタグを作成するように、ポリシーが更新されました。	2022 年 9 月 6 日
AmazonWorkSpacesWebServiceRolePolicy – ポリシーの更新	WorkSpaces Secure Browser で、AWS/Usage 名前空間を PutMetricData API アクセス許可に追加するように、ポリシーが更新されました。	2022 年 4 月 6 日
AmazonWorkSpacesWebReadOnly – 新しいポリシー	WorkSpaces Secure Browser で、AWS マネジメントコンソール、SDK、CLI を通じて WorkSpaces Secure Browser とその依存関係への読み取り専用アクセス権を与えるための、新しいポリシーが追加されました。	2021 年 11 月 30 日
AmazonWorkSpacesWebServiceRolePolicy – 新しいポリシー	WorkSpaces Secure Browser で、WorkSpaces Secure Browser によって使用、管理される AWS のサービスやリソースへのアクセスを許可するための、新しいポリシーが追加されました。	2021 年 11 月 30 日
WorkSpaces Secure Browser での変更の追跡の開始	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 ID とアクセスのトラブルシューティング

以下の情報を使用すると、WorkSpaces Secure Browser および IAM での作業中に直面する可能性がある一般的な問題の診断や修正に役立ちます。

トピック

WorkSpaces Secure Browser でアクションを実行する権限がありません

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、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。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要なworkspaces-web:*GetWidget* アクセス許可を持っていない場合に発生するものです。

```
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:PassRole を実行する権限がありません

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 WorkSpaces Secure Browser 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 のサービス 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、既存のロールをそのサービスに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。

以下の例のエラーは、marymajor という名前の IAM ユーザーがコンソールを使用して WorkSpaces Secure Browser でアクションを実行しようとする際に発生します。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 (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

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については、「Amazon WorkSpaces Secure Browser と IAM との連携方法」を参照してください。
- 所有 AWS アカウント する 全体のリソースへの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「所有 AWS アカウント する別の の IAM ユーザーへのアクセスを提供する」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介し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「外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可」を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

Amazon WorkSpaces Secure Browser のサービスリンクロール

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。サービスリンクロールは、WorkSpaces Secure Browser に直接リンクされた特殊な 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 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。

必要なアクセス許可を手動で追加する必要がないため、サービスリンクロールは WorkSpaces Secure Browser のセットアップを容易にします。WorkSpaces Secure Browser は、サービスリンク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、WorkSpaces Secure Browser 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、WorkSpaces Secure Browser リソースに対するアクセス許可が誤って削除されることを防ぎ、それらのリソースを保護できます。

サービスにリンクされた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 サービス」を参照して、サービスにリンクされたロール列がはいになっているサービスを見つけてください。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。

トピック

- WorkSpaces Secure Browser のサービスリンクロールのアクセス許可
- WorkSpaces Secure Browser のサービスリンクロールの作成
- WorkSpaces Secure Browser のサービスリンクロールの編集
- WorkSpaces Secure Browser のサービスリンクロールの削除
- WorkSpaces Secure Browser のサービスリンクロールでサポートされているリージョン

WorkSpaces Secure Browser のサービスリンクロールのアクセス許可

WorkSpaces Secure Browser は、WorkSpaces Secure Browser は、`AWSServiceRoleForAmazonWorkSpacesWeb` という名前のサービスリンク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て、インスタンスや CloudWatch メトリクスをストリーミングします。

AWSServiceRoleForAmazonWorkSpacesWeb サービスリンクロールは、以下のサービスを信頼してロールを引き受けます。

- workspaces-web.amazonaws.com

AmazonWorkSpacesWebServiceRolePolicy という名前のロールアクセス許可ポリシーは、WorkSpaces Secure Browser に、指定されたリソースで以下のアクションを完了することを許可します。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: ec2:DescribeVpcs。対象リソース: all AWS resources
- アクション: all AWS resources 上で ec2:DescribeSubnets
- アクション: ec2:DescribeAvailabilityZones。対象リソース: all AWS resources
- 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: ec2:DescribeNetworkInterfaces。対象リソース: all AWS resources
- 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: ec2:DescribeSubnets。対象リソース: all AWS resources
- 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: ec2:DescribeVpcEndpoints。対象リソース: all AWS resources
- 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: cloudwatch:PutMetricData。対象リソース: all AWS resources
- 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

サービスリンク役割の作成、編集、削除を IAM エンティティ (ユーザー、グループ、役割など) 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の許可」を参照してください。

WorkSpaces Secure Browser のサービスリンクロールの作成

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役割はこの役割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、サービスリンク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リンク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 のサービスリンクロールの編集

WorkSpaces Secure Browser では、`AWSServiceRoleForAmazonWorkSpacesWeb` のサービスリンク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「サービスにリンクされたロールの編集」を参照してください。

WorkSpaces Secure Browser のサービスリンクロールの削除

サービスリンクロールを必要とする機能やサービスが不要になった場合は、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ているときに WorkSpaces Secure Browser サービスがロールを使用している場合は、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。

AWSServiceRoleForAmazonWorkSpacesWeb によって使用される WorkSpaces Secure Browser リソースを削除するには

- 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。

サービスリンクロールを IAM で手動削除するには

IAM コンソール、 AWS CLI、または AWS API を使用して、AWSServiceRoleForAmazonWorkSpacesWeb サービスリンクロールを削除します。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削除」を参照してください。

WorkSpaces Secure Browser のサービスリンクロールでサポートされているリージョン

WorkSpaces Secure Browser は、このサービスが利用可能なすべてのリージョンで、サービスリンク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 でのインシデントへの対応

`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` メトリックスの

CloudWatch アラームを使用します。詳細については、「Amazon CloudWatch を使用した Amazon WorkSpaces Secure Browser のモニタリング」を参照してください。

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

AWS のサービス 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AWS のサービス プログラムによる範囲内コンプライアンスを参照し、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 「 Compliance ProgramsAssurance」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、「Downloading AWS Artifact reports 」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 のサービス 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。 では、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。

- セキュリティのコンプライアンスとガバナンス – これらのソリューション実装ガイドでは、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の機能をデプロイする手順を示します。
- HIPAA 対応サービスのリファレンス – HIPAA 対応サービスの一覧が提供されています。すべてが HIPAA 対応 AWS のサービス であるわけではありません。
- 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。このガイドは、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) を含む) のセキュリティコントロールを保護し、そのガイダンスに AWS のサービス マッピングするためのベストプラクティスをまとめたものです。
- 「 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 のサービス 、セキュリティ状態を包括的に把握できます 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一覧については、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 – 環境をモニタリングして AWS アカウント不審なアクティビティや悪意のあるアクティビティがないか調べることで、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。GuardDuty を使用すると、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、PCI DSS などのさまざまなコンプライアンス要件に対応できます。
- AWS Audit Manager – これにより AWS のサービス 、 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 のレジリエンス

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、以下の機能は WorkSpaces Secure Browser によって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、「セキュリティの柱 AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

AWS が公開した API コールを使用して、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)。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。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。

また、リクエストにはアクセスキー ID と、IAM プリンシパルに関連付けられている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、一時的な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 Standard 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) の多要素認可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 などのアプリケーションやプラットフォームを、必要に応じてユーザーに代わって更新し、パッチを適用します。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 WorkSpaces Secure Browser の使用状況をモニタリングするのはお客様の責任です。サービス関連の設定と脆弱性の分析はすべて WorkSpaces Secure Browser が担当します。

ウェブポータルの数やユーザー数など、WorkSpaces Secure Browser リソースの上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 の可用性を担保します。

インターフェイス VPC エンドポイント (AWS PrivateLink) を使用して APIs にアクセスする

インターネット経由で接続するのではなく、プライベートクラウド (VPC) 内から Amazon WorkSpaces Secure Browser API エンドポイントを直接呼び出すことができます。これは、インターネットゲートウェイ、NAT デバイス、VPN 接続、または AWS Direct Connect 接続を使用せずに実行できます。

このプライベート接続を確立するには、 を使用するインターフェイス VPC エンドポイントを作成しますAWS PrivateLink。VPC から指定したサブネットごとに、サブネットにエンドポイントネットワークインターフェイスが作成されます。エンドポイントネットワークインターフェイスは、Amazon WorkSpaces Secure Browser API トラフィックのエントリポイントとして機能するリクエスタマネージドネットワークインターフェイスです。

詳細については、「 を介して AWS サービスにアクセスする AWS PrivateLink」を参照してください。

トピック

- Amazon WorkSpaces Secure Browser に関する考慮事項
- Amazon WorkSpaces Secure Browser 用のインターフェイス VPC エンドポイントの作成
- インターフェイス VPC エンドポイントのエンドポイントポリシーの作成
- トラブルシューティング

Amazon WorkSpaces Secure Browser に関する考慮事項

Amazon WorkSpaces Secure Browser APIs「Access AWS services through AWS PrivateLink」の「Prerequisites」を確認してください。Amazon WorkSpaces Secure Browser は、インターフェイス VPC エンドポイントを介したすべての API アクションの呼び出しをサポートしています。

デフォルトでは、エンドポイント経由で Amazon WorkSpaces Secure Browser へのフルアクセスが許可されます。詳細については、「Amazon VPC ユーザーガイド」の「VPC エンドポイントでサービスへのアクセスを制御する」を参照してください。

Amazon WorkSpaces Secure Browser 用のインターフェイス VPC エンドポイントの作成

Amazon WorkSpaces Secure Browser サービスのインターフェイス VPC エンドポイントは、Amazon VPC コンソールまたは AWS Command Line Interface () を使用して作成できますAWS CLI。詳細については、 Amazon VPC ユーザーガイド のインターフェイスエンドポイントの作成を参照してください。

次のサービス名を使用して、Amazon WorkSpaces Secure Browser のインターフェイス VPC エンドポイントを作成します。

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

FIPS がサポートされているリージョンの場合は、次のサービス名を使用して Amazon WorkSpaces Secure Browser のインターフェイス VPC エンドポイントを作成します。

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

インターフェイス VPC エンドポイントのエンドポイントポリシーの作成

エンドポイントポリシーは、インターフェイス VPC エンドポイントにアタッチできる IAM リソースです。デフォルトのエンドポイントポリシーでは、インターフェイス VPC エンドポイントを介して Amazon WorkSpaces Secure Browser APIs へのフルアクセスが許可されます。VPC から Amazon WorkSpaces Secure Browser に付与されるアクセスを制御するには、インターフェイス VPC エンドポイントにカスタムエンドポイントポリシーをアタッチします。

エンドポイントポリシーは以下の情報を指定します。

- アクションを実行できるプリンシパル (AWS アカウント、IAM ユーザー、IAM ロール)。
- 実行可能なアクション。
- アクションを実行できるリソース。

詳細については、「Amazon VPC ユーザーガイド」の「VPC エンドポイントでサービスへのアクセスを制御する」を参照してください。

例: Amazon WorkSpaces Secure Browser アクションの VPC エンドポイントポリシー

以下は、カスタムエンドポイントポリシーの例です。このポリシーをインターフェイス VPC エンドポイントにアタッチすると、すべてのリソースのすべてのプリンシパルに対して、リストされている Amazon WorkSpaces Secure Browser アクションへのアクセスが許可されます。

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

トラブルシューティング

Amazon WorkSpaces Secure Browser APIs への呼び出しがハングしている場合、VPC Endpoint Service セキュリティグループまたは IAM ロール設定の設定が間違っている可能性があります。これを解決するには、以下を試してください。

- インターフェイス VPC エンドポイントの作成中に、 が AWS アカウントデフォルトのセキュリティグループに自動的にアタッチされている可能性があります。別のセキュリティグループを使用し、インバウンドアクセス許可とアウトバウンドアクセス許可でデータを適切に転送できることを確認します。
- Amazon WorkSpaces Secure Browser APIs の呼び出しを許可する IAM ロールを使用していることを確認します。

詳細については、「Amazon VPC ユーザーガイド」の「What is AWS PrivateLink？」を参照してください。

Amazon WorkSpaces Secure Browser に関するセキュリティ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適切ではないか、十分ではない場合があるため、これらは指示ではなく、有用な考慮事項と見なしてください。

Amazon WorkSpaces Secure Browser に関するベストプラクティスには以下が含まれます。

- 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、AWS CloudTrail または Amazon CloudWatch を使用してアクセス履歴とプロセスログを検出および追跡します。詳細については、Amazon CloudWatch を使用した Amazon WorkSpaces Secure Browser のモニタリングおよびを使用した WorkSpaces Secure Browser API コールのログ記録 AWS CloudTrailを参照してください。
- 検出制御を実装して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 CloudWatch を使用した Amazon WorkSpaces Secure Browser のモニタリングおよびを使用した 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グの設定”」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 の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は報告し、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 AWS で実行されるアプリケーションを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、CloudWatch で Amazon EC2 インスタンスの CPU 使用率などのメトリクスを追跡し、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 CloudWatch ユーザーガイド」を参照してください。
- Amazon CloudWatch Logs は、Amazon EC2 インスタンス、CloudTrail、およびその他のソースからのログファイルをモニタリング、保存、およびアクセスするのに役立ちます。CloudWatch Logs は、ログファイル内の情報をモニタリングし、特定のしきい値が満たされたときに通知します。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可能です。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。が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、および呼び出しの発生日時を特定できます。詳細については、AWS CloudTrail ユーザーガイドをご参照ください。

トピック

Amazon CloudWatch を使用した 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、raw データを収集し、リアルタイムに近い読み取り可能なメトリクスに加工することができます。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 CloudWatch ユーザーガイド」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。

Amazon WorkSpaces Secure Browser の CloudWatch 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 のセッション試行回数。	PortalId	Average、Sum、Maximum、Minimum	カウント
SessionSuccess	Amazon WorkSpaces Secure Browser セッションが正常に開始された回数です。	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です。	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 GlobalMemoryPercent の「SampleCount」メトリクス統計を表示して、ポータルでアクティブな同時セッション数を確認できます。データポイントはセッションごとに 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。CloudTrail は、Amazon WorkSpaces Secure Browser へのすべての API コールをイベントとしてキャプチャします。これには、Amazon WorkSpaces Secure Browser コンソールの呼び出しと、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。証跡を作成すると、Amazon WorkSpaces Secure Browser のイベントを含め、Amazon S3 バケットへの CloudTrail イベントの継続的デリバリーを有効にすることができます。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。CloudTrail により収集された情報を使用して、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、リクエストが行われた日時、および追加の詳細を特定することができます。

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

トピック

- CloudTrail における WorkSpaces Secure Browser の情報

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

CloudTrail における WorkSpaces Secure Browser の情報

CloudTrail は、 AWS アカウントの作成時に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イベント履歴の他の AWS サービスイベントとともに CloudTrail 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、 CloudTrail イベント履歴でのイベントの表示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、ログファイルを CloudTrail で 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口グに記録し、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 ログで収集したイベントデータをより詳細に分析し、それに基づいて対応するため、他の AWS サービスを構成できます。詳細については、次を参照してください:

- 追跡を作成するための概要
- 「CloudTrail がサポートされているサービスと統合」
- 「CloudTrail の Amazon SNS 通知の設定」
- 「複数のリージョンから CloudTrail ログファイルを受け取る」および「複数のアカウントから CloudTrail ログファイルを受け取る」

Amazon WorkSpaces Secure Browser のすべてのアクションは CloudTrail によってログに記録されます。これらのアクションは Amazon WorkSpaces API リファレンスに記載されています。例えば、`CreatePortal`、`DeleteUserSettings`、`ListBrowserSettings` の各アクションを呼び出すと、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 エレメント」を参照してください。

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

「トレイル」は、指定した Simple Storage Service (Amazon S3) バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルには、ログエントリが 1 つ以上あります。イベントは任意の出典からの 1 つ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、リクエストのパラメータ、その他の詳細に関する情報が含まれます。CloudTrail ログファイルは、パブリック API 呼び出し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。

以下の例は、`ListBrowserSettings` アクションを示す CloudTrail ログエントリです。


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

Amazon WorkSpaces Secure Browser でのユーザーアクセスロギング

Amazon WorkSpaces Secure Browser では、カスタマーは、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グの設定”」を参照してください。

Amazon WorkSpaces Secure Browser ユーザー向けガイダンス

管理者は WorkSpaces Secure Browser を使用して、企業の社内ウェブサイトや Software as a Service (SaaS) ウェブアプリケーション、またはインターネッ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、セッションの開始と設定、ツールバーとウェブブラウザの使用について詳しく知りたいエンドユーザー向けのガイドとなります。

トピック

Amazon WorkSpaces Secure Browser での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 Amazon DCV ウェブブラウザクライアントを利用しているため、インストールは不要です。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サポートの最新情報については、「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。

Amazon WorkSpaces Secure Browser でのウェブポータルへのアクセス

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。

Amazon WorkSpaces Secure Browser でのセッションのガイダンス

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

Amazon WorkSpaces Secure Browser でのセッションの開始

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 がユーザー向けにセッションを作成していることを示しています。背後では、Amazon WorkSpaces Secure Browser が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、[常にポップアップを許可する] に設定することで、Amazon WorkSpaces Secure Browser は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。

Amazon WorkSpaces Secure Browser でのツールバーの使用

ツールバーの使用方法を理解するには、以下の手順に従います。

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、その上にカーソルを置いて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色の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。

画面の表示サイズを大きくするには、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大きくするには、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、以下の手順に従います。

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

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

1. ツールバーまたはウェブコンテンツを選択します。

2. ズームインするには Cmd + + を、ズームアウトするには Cmd + - を押します。

ツールバーを画面上部にドッキングするには、[詳細設定]、[全般] の順に選択し、[ツールバーモード] で [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. Use the down arrow to select from a list of available microphones.
	**Webcam**	Activate webcam for the session. Use the down arrow to select from a list of available webcams.
	**Preferences**	Access the **General** and **Keyboard** menus. From the **General** menu, toggle between light and dark mode, activate the keyboard input selector (for changing the keyboard language), and switch between streaming mode or display resolution. From the **Keyboard** menu, change the option and command key settings (on Mac devices), or activate **Functions** (see below).
	**Profile**	End your session, view performance metrics, access **Feedback** and **Help**, and learn about Amazon WorkSpaces Web. **End Session** ends the Amazon WorkSpaces Web session. **Performance metrics** displays the frame rate, network latency, and bandwidth usage graph. This information is useful for administrators when investigating issues with the service. **Feedback** provides you with an email address to share feedback to the Amazon WorkSpaces Web team. **Help** provides you with access to Frequently Asked Questions, such as how to use the clipboard, microphone, and webcam during the session, or how to troubleshoot launching an additional monitor window. From help, you can also launch the tutorial or user guide. **About** provides more information about Amazon WorkSpaces Web.
	**Notifications**	Get one-click access to session notifications.
	**Clipboard**	Access clipboard shortcut descriptions, links to set the command key preference, and troubleshoot clipboard permissions from the local web browser. You can use the content preview text box to test clipboard functionality. This icon only displays if clipboard permission is granted by your administator.
	**Files**	From the files menu, you can upload content to the remote browser. Once uploaded, you can rename, download, or delete, as well as create folders in the temporary file menu. All files and data in **Files** are deleted at the end of the session. This icon only displays if **Files** permission is granted by your administator.

> **Note**
>
> 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。

Amazon WorkSpaces Secure Browser でのブラウザの使用

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。

Amazon WorkSpaces Secure Browser でのセッションの終了

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。

Amazon WorkSpaces Secure Browser でのユーザーの問題のトラブルシューティング

WorkSpaces Secure Browser の使用中に次の問題が発生した場合は、以下の解決方法を試してください。

Amazon WorkSpaces Secure Browser ポータルに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 リアルタイムオーディオビデオ (AV) は、ローカルのウェブカメラビデオとマイクの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。

どのマイクやウェブカメラが使用されているか、またどのように変更すればよいですか？

マイクまたはカメラの横にある下矢印アイコンをクリックします。メニューには、使用可能なデバイスが表示され、現在のデバイスを示すチェックマークが表示されます。別のデバイスを選択して、セッションに使用するデバイスを変更します。

Amazon WorkSpaces Secure Browser のシングルサインオン拡張機能

Amazon WorkSpaces Secure Browser には、デスクトップコンピュータの Chrome ブラウザと Firefox ブラウザでシングルサインオンするための拡張機能が用意されています。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 には、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可能にする拡張機能が用意されています。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。

トピック

Amazon WorkSpaces Secure Browser のシングルサインオン拡張機能の互換性

シングルサインオン拡張機能は、以下のデバイスとブラウザで動作します。

- デバイス
  - ノートパソコン
  - デスクトップコンピュータ
- ブラウザ
  - Google Chrome
  - Mozilla Firefox

Amazon WorkSpaces Secure Browser のシングルサインオン拡張機能のインストール

シングルサインオン拡張機能をインストールするには、以下の手順に従います。

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 ブラウザ用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。

拡張機能が想定どおりに動作するようにするには、シークレットモード (Chrome) やプライベートブラウジング (Firefox) ではなく、通常のブラウジングウィンドウで拡張機能を使用してください。

Amazon WorkSpaces Secure Browser のシングルサインオン拡張機能のトラブルシューティング

シングルサインオン拡張機能の使用中に、以下の問題が発生する可能性があります。

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. ブラウザに Amazon WorkSpaces Secure Browser 拡張機能がインストールされていることを確認してください。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. シークレットモード (Chrome) またはプライベートブラウジング (Firefox) を使用してい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

以下の表に、Amazon WorkSpaces Secure Browser のドキュメントリリースについて説明します。

変更	説明	日付
ツールバーコントロール	ツールバーコントロールを使用すると、エンドユーザーセッションのツールバー表示を設定できます。	2025 年 2 月 21 日
インターフェイス VPC エンドポイント (AWS PrivateLink) を使用して APIs にアクセスする	インターネット経由で接続するのではなく、プライベートクラウド (VPC) 内から Amazon WorkSpaces Secure Browser API エンドポイントを直接呼び出します。	2025年1月10日
データ保護設定	データ保護設定を追加して、セッション中にデータが共有されないようにします。	2024 年 11 月 20 日
FIPS エンドポイント	FIPS エンドポイントを使用して転送中のデータを保護します。	2024 年 10 月 7 日
セッション管理ダッシュボード	セッション管理ダッシュボードを使用して、アクティブなセッションと完了したセッションをモニタリングおよび管理します。	2024 年 9 月 19 日
ディープリンクの許可	セッション中に特定のウェブサイトにユーザーを接続するディープリンクをポータルで受信することを許可します。	2024 年 6 月 25 日

マネージドポリシーの更新	AmazonWorkSpacesSecureBrowserReadOnly マネージドポリシーを追加しました。	2024 年 6 月 24 日
ツールバーを使用したズーム	ツールバーを使用して、画面表示、アイコン、テキストのサイズを拡大できます。	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数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 フィルタリングの設定	Chrome ポリシーを使用して、リモートブラウザからユーザーがアクセスできる URL をフィルタリングできます。	2024 年 2 月 21 日
IdP 認証タイプ	スタンダードまたは IAM アイデンティティセンターのいずれかの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 のユーザー向けガイダンス	Amazon WorkSpaces Secure Browser へのアクセス、セッションの開始と設定、ツールバーとウェブブラウザの使用について詳しく知りたいエンドユーザー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 では、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 マネージドポリシーの更新	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、スタンダードと AWS IAM Identity Center の 2 つの認証タイプがあります。	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 マネージドポリシーの更新	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 マネージドポリシーの更新	2022 年 11 月 2 日

マネージドポリシーの更新	AmazonWorkSpacesWebServiceRolePolicy マネージドポリシーの更新	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 マネージドポリシーの更新	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	PutMetricData API アクセス許可に AWS/Usage 名前空間を追加するように AmazonWorkSpacesWebServiceRolePolicy マネージドポリシーを更新しました	2022 年 4 月 6 日
サービスリンクロール	新しい AWSServiceRoleForAmazonWorkSpacesWeb サービスリンクロール	2021 年 11 月 30 日

マネージドポリシー	AmazonWorkSpacesWebReadOnly マネージドポリシーの更新	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。