入門ガイド

AWS マネジメントコンソール

Version 1.0

AWS マネジメントコンソール: 入門ガイド

Table of Contents

AWS マネジメントコンソールとは

AWS マネジメントコンソール はウェブベースのアプリケーションであり、すべての個々の AWS サービスコンソールに一元的にアクセスできます。で統合ナビゲーションを使用して、サービス AWS マネジメントコンソール の検索、通知の表示、 AWS CloudShell へのアクセス、アカウントと請求情報へのアクセス、一般的なコンソール設定のカスタマイズを行うことができます。のホームページ AWS マネジメントコンソール が呼び出されます AWS Console Home。から AWS Console Home、 AWS アプリケーションを管理し、他のすべての個々のサービスコンソールにアクセスできます。ウィジェットを使用して、 AWS と リソースに関するその他の役立つ情報を表示する AWS Console Home ように をカスタマイズすることもできます。[最近アクセスした] 、[AWS ヘルス] などのウィジェットを追加、削除、配置変更することができます。

トピック

- の機能 AWS マネジメントコンソール
- の個々の AWS サービスコンソール AWS マネジメントコンソール
- へのアクセス AWS マネジメントコンソール
- モバイルデバイスでの AWS マネジメントコンソール へのアクセス

の機能 AWS マネジメントコンソール

の重要な機能 AWS マネジメントコンソール は次のとおりです。

- AWS サービスコンソールに移動する – Unified Navigation を使用して、最近アクセスしたサービスコンソールへのアクセス、お気に入りリストへのサービスの表示と追加、コンソール設定へのアクセス、アクセスを行うことができます AWS User Notifications。
- AWS サービスやその他の AWS 情報の検索 – 統合検索を使用して、 AWS サービスや機能、マーケット AWS プレイス製品を検索します。
- コンソールのカスタマイズ – 統合設定を使用して、 AWS マネジメントコンソールのさまざまな側面をカスタマイズできます。これには、言語、デフォルトのリージョンなどが含まれます。
- CLI コマンドを実行する – コンソールから直接 AWS CloudShell アクセスできます。CloudShell を使用して、お気に入りのサービスに対して AWS CLI コマンドを実行できます。
- すべての AWS イベント通知へのアクセス – を使用して AWS マネジメントコンソール 、 AWS User Notifications および からの通知にアクセスできます AWS Health。

- カスタマイズ AWS Console Home – ウィジェットを使用して AWS Console Home エクスペリエンスを完全にカスタマイズできます。
- AWS アプリケーションの作成と管理 – で myApplications を使用して、アプリケーションのコスト、ヘルス、セキュリティ体制、パフォーマンスを管理およびモニタリングします AWS Console Home。
- Amazon Q とのチャット – 生成人工知能 (AI) アシスタントによる AWS のサービス 質問への回答は、 コンソールから直接取得できます。ライブエージェントに接続して、追加のサポートを受けることもできます。
- ネットワーク内の AWS アカウントアクセスを制御する – AWS マネジメントコンソール プライベートアクセスを使用して、トラフィックがネットワーク内から発信されたときに AWS マネジメントコンソール 、 へのアクセスを、指定された一連の既知の AWS アカウントに制限できます。

の個々の AWS サービスコンソール AWS マネジメントコンソール

各 AWS サービスには、 内でアクセスできる独自のサービスコンソールがあります AWS マネジメントコンソール。ビジュアルモードやデフォルト言語など AWS マネジメントコンソール、 の統合設定で選択した設定は、すべての個々の AWS コンソールに適用されます。 AWS サービスコンソールには、クラウドコンピューティング用の幅広いツールと、アカウントや請求に関する情報が用意されています。Amazon Elastic Compute Cloud など、特定のサービスとそのコンソールの詳細を確認するには、 AWS マネジメントコンソール ナビゲーションバーで統合検索を使用してコンソールに移動し、 AWS ドキュメントウェブサイトから Amazon EC2 ドキュメントにアクセスします。

個々の AWS サービスのコンソールに移動する場合でも、コンソールの上部にある統合ナビゲーション AWS マネジメントコンソール を使用して の機能にアクセスできます。個々のサービスのコンソールのフィードバックは、そのコンソールに移動し、ページのフッターで [フィードバック] を選択して残すことができます。

へのアクセス AWS マネジメントコンソール

には、https://console.aws.amazon.com/ AWS マネジメントコンソール からアクセスできます。

モバイルデバイスでの AWS マネジメントコンソール へのアクセス

AWS マネジメントコンソール はタブレットおよび他のモバイルデバイスで使用できるように設計されています。

- 横および縦のスペースは画面により多くの情報を表示するよう最大化できます。
- ボタンとセレクタはより大きく、タッチしやすくなっています。

モバイルデバイスで AWS マネジメントコンソール にアクセスするには、AWS Console Mobile Application を使用する必要があります。このアプリは Android および iOS で使用できます。このコンソールモバイルアプリは完全なウェブ体験の補助として、モバイル関連の作業を行うのに適しています。例えば、携帯電話から既存のAmazon EC2 インスタンスと Amazon CloudWatch アラームを閲覧し、管理できます。詳細については、AWS Console Mobile Application ユーザーガイドの「AWS Console Mobile Application とは」を参照してください。

Amazon Appstore、Google Play、または iOS App Store からコンソールモバイルアプリをダウンロードできます。

AWS マネジメントコンソール でサービスの使用を開始する

AWS マネジメントコンソール には、個々のサービスコンソールに移動する複数の方法があります。

サービスのコンソールを開くには

次のいずれかを行います:

- ナビゲーションバーで、サービスの名前の全部または一部を入力します。[サービス] で、検索結果のリストから必要なサービスを選択します。詳細については、「で統合検索を使用して製品、サービス、機能などを検索する AWS マネジメントコンソール」を参照してください。
- [最近アクセスしたサービス] ウィジェットで、サービス名を選択します。
- [最近アクセスしたサービス] ウィジェットで、[すべての AWS のサービスを表示] を選択します。次に、[すべての AWS のサービス] ページで、サービス名を選択します。
- ナビゲーションバーで、サービスの詳細なリストを開くには、[サービス] を選択します。次に、[最近アクセスした] または [すべてのサービス] でサービスを選択します。

統合ナビゲーションによる AWS マネジメントコンソール ナビゲーションバーの使用

このトピックでは、統合ナビゲーションの使用方法について説明します。統合ナビゲーションとは、コンソールのヘッダーおよびフッターとして機能するナビゲーションバーを指します。統合ナビゲーションを使用して以下が可能です。

- AWS サービス、機能、製品などを検索してアクセスする。
- AWS CloudShell を起動する。
- AWS 通知と AWS Health イベントにアクセスする。
- さまざまな AWS ナレッジソースからサポートを受ける。
- デフォルトの言語、ビジュアルモード、リージョンなどを選択して、AWS マネジメントコンソール を設定する。
- アカウント、組織、Service Quotas、請求情報にアクセスする。

トピック

AWS マネジメントコンソール のサービスメニューへのアクセス

検索バーの横にある [サービス] メニューを使用して、最近アクセスしたサービスへのアクセス、お気に入りリストの表示、すべての AWS サービスの表示ができます。また、[分析] や [アプリケーションの統合] などのサービスタイプを選択して、タイプ別にサービスを表示することもできます。

次の手順は、[サービス] メニューにアクセスする方法を示しています。

サービスメニューにアクセスするには

1. にサインインします。。AWS マネジメントコンソール
2. ナビゲーションバーで [サービス (⁝⁝⁝)] を選択します。
3. (オプション) [最近アクセスした] を選択して、最近操作したサービスとアプリケーションを表示します。
4. (オプション) [お気に入り] を選択して、お気に入りリストを表示します。
5. (オプション) [すべてのアプリケーション] を選択して、myApplications アプリケーションを表示します。
6. (オプション) [すべてのサービス] を選択して、すべての AWS サービスのアルファベット順のリストを表示します。
7. (オプション) サービスタイプを選択して、タイプ別に AWS サービスを表示します。

で統合検索を使用して製品、サービス、機能などを検索する AWS マネジメントコンソール

ナビゲーションバーの検索ボックスには、 AWS サービスと機能、サービスドキュメント、 AWS Marketplace 製品などを検索するための統合検索ツールが用意されています。数文字、または質問を入力するだけで、利用可能なすべてのコンテンツタイプから結果が生成され始めます。文字を入力する度に、結果をさらに絞り込むことができます。使用可能なコンテンツタイプは次のとおりです。

- サービス
- 機能
- ドキュメント
- ブログ
- ナレッジ記事
- Events
- チュートリアル
- Marketplace
- リソース

> **Note**
>
> フォーカス検索を実行することで、検索結果をリソースのみに絞り込むことができます。フォーカス検索を実行するには、検索バーでクエリの先頭に `/Resources` を入力し、ドロップダウンメニューから [/Resources] を選択します。次に、クエリの残りの部分を入力します。

トピック

で AWS 製品を検索する AWS マネジメントコンソール

次の手順では、検索ツールを使用して AWS 製品を検索する方法について詳しく説明します。

サービス、機能、ドキュメント、または AWS Marketplace 製品を検索するには

1. AWS マネジメントコンソール のナビゲーションバーの検索ボックスに、クエリを入力します。
2. 任意のリンクを選択して、目的の宛先に移動します。

> **Tip**
>
> キーボードを使用して、上位の検索結果にすばやく移動することもできます。まず、[Alt+s] (Windows) または[Option+s] (macOS) キーを押して検索バーにアクセスします。次に、検索する語句を入力します。意図した結果がリストの最上部に表示されたら、[Enter] キーを押します。例えば、Amazon EC2 コンソールにすばやく移動するには、「ec2」と入力し、[Enter] キーを押します。

での検索の絞り込み AWS マネジメントコンソール

コンテンツタイプ別に検索を絞り込み、検索結果に関する追加情報を表示できます。

検索を特定のコンテンツタイプに絞り込むには

1. AWS マネジメントコンソール のナビゲーションバーの検索ボックスに、クエリを入力します。
2. 検索結果の横にある任意のコンテンツタイプを選択します。
3. (オプション) 特定のカテゴリのすべての結果を表示するには
   - [さらに表示]を選択します。新しいタブが開き、結果が表示されます。
4. (オプション) 検索結果に関する追加情報を表示するには
   a. 検索結果で、検索結果の上にカーソルを合わせます。
   b. 利用可能な追加情報を表示します。

でのサービスの機能の表示 AWS マネジメントコンソール

検索結果内からサービスの機能を表示できます。

サービスの機能を表示するには

1. AWS マネジメントコンソール のナビゲーションバーの検索ボックスに、クエリを入力します。
2. 検索結果で、[サービス] 内のサービスにカーソルを合わせます。
3. [トップ機能] のリンクのいずれかを選択します。

のナビゲーションバー AWS CloudShell から起動する AWS マネジメントコンソール

AWS CloudShell はブラウザベースの事前認証済みシェルで、 AWS マネジメントコンソール ナビゲーションバーから直接起動できます。任意のシェル (Bash、PowerShell、または Z シェル) を使用して、 サービスに対して AWS CLI コマンドを実行できます。

CloudShell は、次の 2 つの方法のいずれか AWS マネジメントコンソール を使用して から起動できます。

- コンソールのフッターで CloudShell アイコンを選択します。
- コンソールナビゲーションバーで、CloudShell アイコンを選択します。

このサービスの詳細については、AWS CloudShell ユーザーガイドを参照してください。

AWS リージョン AWS CloudShell が利用可能な の詳細については、AWS 「リージョンサービスリスト」を参照してください。コンソールリージョンの選択は CloudShell リージョンと同期しています。選択したリージョンで CloudShell が利用できない場合、CloudShell は最も近いリージョンで実行されます。

AWS 通知とヘルスイベントへのアクセス

一部の AWS 通知にアクセスして、ナビゲーションバーからヘルスイベントを表示できます。AWS User Notifications にアクセスして、ナビゲーションバーからすべての AWS 通知と AWS Health ダッシュボードを表示することもできます。

詳細については、「AWS User Notifications ユーザーガイド」の「AWS User Notifications とは」と「AWS Health ユーザーガイド」の「AWS Health とは」をご覧ください。

次の手順では、AWS イベント情報にアクセスする方法について説明します。

AWS イベント情報にアクセスするには

1. にサインインします。。AWS マネジメントコンソール
2. ナビゲーションバーで、 ベルアイコンを選択します。
3. 通知とヘルスイベントを表示します。
4. (オプション) [すべての通知の表示] を選択して User Notifications コンソールに移動します。
5. (オプション) [すべてのヘルスイベントの表示] を選択して AWS Health コンソールに移動します。

サポート情報

ナビゲーションバーの疑問符アイコンを選択すると、サポートを受けることができます。サポートメニューから、以下を選択できます。

- サポートセンターのサービスコンソールに移動する
- AWS IQ から専門家のサポートを受ける
- コミュニティ記事と AWS re:Post のナレッジセンターから厳選されたナレッジを表示する
- AWS ドキュメントに移動する
- AWS トレーニングに移動する
- AWS 利用開始のためのリソースセンターに移動する

- 現在アクセスしているサービスコンソールのフィードバックを残す

> **Note**
>
> これは、コンソールのフッターで [フィードバック] を選択することでも実行できます。開くモーダルのタイトルは、フィードバックを残そうとしているコンソールを示しています。

コンソール内でいつでもサポートを受けることができ、ライブエージェントと接続して、AWS Q を使用して AWS に関する質問をチャットで行うことができます。詳細については、「???」を参照してください。

統合設定 AWS マネジメントコンソール を使用した の設定

このトピックでは、統合設定ページ AWS マネジメントコンソール を使用して を設定し、すべてのサービスコンソールに適用されるデフォルトを設定する方法について説明します。

トピック

- での統合設定の設定 AWS マネジメントコンソール
- リージョン選択
- のお気に入り AWS マネジメントコンソール
- でのパスワードの変更 AWS マネジメントコンソール
- の言語の変更 AWS マネジメントコンソール

での統合設定の設定 AWS マネジメントコンソール

表示、言語、リージョンなどの設定とデフォルトは、 AWS マネジメントコンソール 統一された設定ページから設定できます。統一されたナビゲーションのナビゲーションバーから統合設定にアクセスできます。ビジュアルモードとデフォルトの言語は、ナビゲーションバーから直接設定することもできます。これらの変更は、すべてのサービスコンソールに適用されます。

> **Important**
>
> 設定、お気に入りサービス、最近アクセスしたサービスがグローバルに保持されるように、このデータはデフォルトで無効になっているリージョンを含む AWS リージョンすべての に

保存されます。対象となるリージョンは、アフリカ (ケープタウン)、アジアパシフィック (香港)、アジアパシフィック (ハイデラバード)、アジアパシフィック (ジャカルタ)、欧州 (ミラノ)、欧州 (スペイン)、欧州 (チューリッヒ)、中東 (バーレーン)、および中東 (UAE) です。アクセスするには、引き続きリージョンを手動で有効にし、そのリージョンでリソースを作成して管理する必要があります。このデータをすべての に保存しない場合は AWS リージョン、すべてリセットを選択して設定をクリアし、設定管理で最近アクセスしたサービスの記憶をオプトアウトします。

トピック

- の統合設定へのアクセス AWS マネジメントコンソール
- の統合設定のリセット AWS マネジメントコンソール
- での統合設定の編集 AWS マネジメントコンソール
- のビジュアルモードの変更 AWS マネジメントコンソール

の統合設定へのアクセス AWS マネジメントコンソール

次の手順では、統一された設定にアクセスする方法を説明します。

統合設定にアクセスするには

1. AWS マネジメントコンソール にサインインします。
2. ナビゲーションバーで、 歯車アイコン (#) を選択します。
3. [統一された設定] ページを開くには、[すべてのユーザー設定の表示] を選択します。

の統合設定のリセット AWS マネジメントコンソール

統一された設定をリセットすると、統一された設定のすべての設定が削除され、デフォルト設定が復元されます。

> **Note**
>
> これは AWS、ナビゲーションやサービスメニューのお気に入りサービス、コンソールホームウィジェットや で最近アクセスしたサービス AWS Console Mobile Application、デフォルト言語、デフォルトリージョン、ビジュアルモードなど、サービス全体に適用されるすべての設定など、 の複数の領域に影響します。

すべての統一された設定をリセットするには

1. AWS マネジメントコンソール にサインインします。
2. ナビゲーションバーで、 歯車アイコン (#) を選択します。
3. [すべてのユーザー設定を見る] を選択して [統一された設定] ページを開きます。
4. [すべてをリセット] を選択します。

での統合設定の編集 AWS マネジメントコンソール

次の手順では、優先設定を編集する方法について説明します。

統一された設定を編集するには

1. AWS マネジメントコンソール にサインインします。
2. ナビゲーションバーで、 歯車アイコン (#) を選択します。
3. [すべてのユーザー設定を見る] を選択して [統一された設定] ページを開きます。
4. 目的の設定の横にある [編集] を選択します。

- ローカリゼーションとデフォルトのリージョン:
  - [言語] では、コンソールテキストのデフォルト言語を選択できます。
  - [デフォルトのリージョン] では、ログインするたびに適用されるデフォルトのリージョンを選択できます。アカウントで使用可能なリージョンはどれでも選択できます。デフォルトとして最後に使用したリージョンを選択することもできます。

    AWS マネジメントコンソールでのリージョンルーティングの詳細については、「リージョンの選択」を参照してください。
- [表示:]
  - [Visual mode] (ビジュアルモード) では、コンソールをライトモード、ダークモード、またはブラウザのデフォルトの表示モードに設定できます。

    ダークモードはベータ機能であり、 AWS のすべてのサービスコンソールに適用されるわけではありません。
  - [お気に入りのバーの表示] では、[お気に入り] バーの表示を切り替えて、完全なサービス名とアイコンを表示するか、サービスのアイコンのみを表示します。
  - [お気に入りバーのアイコンサイズ] は、[お気に入り] バーに表示されるサービスアイコンのサイズを、小 (16 x 16 ピクセル) と大 (24 x 24 ピクセル) の間で切り替えます。

- 設定管理:
  - 最近訪問したサービスでは、 が最近訪問したサービスを AWS マネジメントコンソール 記憶しているかどうかを選択できます。これをオフにすると、最近アクセスしたサービス履歴も削除されるため、最近アクセスしたサービスはサービスメニュー AWS Console Mobile Applicationやコンソールホームウィジェットに表示されなくなります。

5. [Save changes] (変更の保存) をクリックします。

のビジュアルモードの変更 AWS マネジメントコンソール

ビジュアルモードでは、コンソールをライトモード、ダークモード、またはブラウザのデフォルトの表示モードに設定できます。

ナビゲーションバーからビジュアルモードを変更するには

1. AWS マネジメントコンソール にサインインします。
2. ナビゲーションバーで、 歯車アイコン (#) を選択します。
3. [ビジュアルモード] で、ライトモードの場合は [ライト]、ダークモードの場合は [ダーク]、ブラウザのデフォルト表示モードの場合は [ブラウザのデフォルト] を選択します。

リージョン選択

多くのサービスでは、リソースを管理する場所 AWS リージョン を指定する を選択できます。リージョンは、同じ地理的エリアにある AWS リソースのセットです。AWS マネジメントコンソール や などの一部のサービスでは、リージョンを選択する必要はありません AWS Identity and Access Management。 AWS リージョンの詳細については、「AWS 全般のリファレンス」の「AWS リージョンの管理」を参照してください。

> **Note**
>
> AWS リソースを作成したが、それらのリソースがコンソールに表示されない場合、コンソールに別のリージョンのリソースが表示されている可能性があります。一部のリソース (Amazon EC2 インスタンスなど) は、そのリソースが作成されたリージョンに固有です。

トピック

- のナビゲーションバーからリージョンを選択する AWS マネジメントコンソール

- でのデフォルトリージョンの設定 AWS マネジメントコンソール

のナビゲーションバーからリージョンを選択する AWS マネジメントコンソール

次の手順では、ナビゲーションバーからリージョンを変更する方法について説明します。

ナビゲーションバーでリージョンを選択するには

1. AWS マネジメントコンソール にサインインします。
2. ナビゲーションバーで、現在表示されているリージョン名を選択します。
3. 切り替え先のリージョンを選択します。

でのデフォルトリージョンの設定 AWS マネジメントコンソール

次の手順では、統一された設定ページからデフォルトリージョンを変更する方法について説明します。

デフォルトージョンを設定するには

1. ナビゲーションバーで、 歯車アイコン (#) を選択します。
2. [すべてのユーザー設定を表示] を選択して、[統一された設定] ページに移動します。
3. [ローカリゼーションとデフォルトのリージョン] の横にある [編集] を選択します。
4. [デフォルトリージョン] で、リージョンを選択します。

> **Note**
>
> デフォルトのリージョンを選択しない場合、最後にアクセスしたリージョンがデフォルトになります。

5. [設定を保存] を選択します。
6. (オプション) [新しいデフォルトリージョンに移動] を選択して、すぐに新しいデフォルトリージョンに移動します。

のお気に入り AWS マネジメントコンソール

頻繁に使用するサービスにすばやくアクセスするには、サービスコンソールを [お気に入り] リストに保存できます。 AWS マネジメントコンソールを使用して、お気に入りを追加または削除できま

す。サービスまたはアプリケーションを [お気に入り] に追加すると、[お気に入り] クイックバーに表示されます。

トピック

- でのお気に入りの追加 AWS マネジメントコンソール
- でのお気に入りへのアクセス AWS マネジメントコンソール
- でのお気に入りの削除 AWS マネジメントコンソール

でのお気に入りの追加 AWS マネジメントコンソール

[サービス] メニューと [最近アクセスしたサービス] メニューから、サービスやアプリケーションをお気に入りに追加できます。検索ボックスの検索結果ページを使用して、サービスをお気に入りに追加することもできます。お気に入りに追加したサービスとアプリケーションは、[お気に入り] クイックバーに表示されます。

トピック

- のお気に入りクイックバー AWS マネジメントコンソール
- のお気に入りへのサービスの追加 AWS マネジメントコンソール
- のお気に入りへのアプリケーションの追加 AWS マネジメントコンソール

のお気に入りクイックバー AWS マネジメントコンソール

お気に入りに少なくとも 1 つの AWS サービスまたはアプリケーションが追加されると、お気に入りクイックバーが表示されます。お気に入りクイックバーはナビゲーションバーの後にあり、すべての AWS サービスコンソールに表示されるため、お気に入りのサービスとアプリケーションにすばやくアクセスできます。サービスまたはアプリケーションを左右にドラッグすることで、お気に入りクイックバー内のサービスおよびアプリケーションの順序を変更できます。

のお気に入りへのサービスの追加 AWS マネジメントコンソール

[サービス] メニューまたは検索ボックスの検索結果ページから、お気に入りにサービスを追加できます。

Services menu

サービスメニューからお気に入りを追加するには

1. AWS マネジメントコンソール を開きます。

2. ナビゲーションバーで [サービス (⋮⋮⋮)] を選択します。
3. (オプション) 次の手順で、最近アクセスしたサービスをお気に入りに追加します。

   a. [最近アクセスしたサービス] で、サービスの上にカーソルを置きます。

   b. サービス名の横にある星印を選択します。
4. [すべてのサービス] を選択します。
5. 選択したサービスにカーソルを合わせます。
6. サービス名の横にある星印を選択します。

Search box

検索ボックスからお気に入りを追加するには

1. AWS マネジメントコンソール を開きます。
2. 検索ボックスにサービス名を入力します。
3. 検索結果ページで、サービス名の横にある星印を選択します。

> **Note**
>
> お気に入りにサービスを追加すると、ナビゲーションバーの後にあるお気に入りクイックバーに追加されます。

のお気に入りへのアプリケーションの追加 AWS マネジメントコンソール

[サービス] メニューからお気に入りにアプリケーションを追加できます。

サービスメニューからお気に入りを追加するには

1. AWS マネジメントコンソール を開きます。
2. ナビゲーションバーで [サービス (⋮⋮⋮)] を選択します。
3. (オプション) 次の手順で、最近アクセスしたサービスをお気に入りに追加します。

   a. [最近アクセスした] で、アプリケーションにカーソルを合わせます。

   b. アプリケーション名の横にある星を選択します。
4. [Applications] (アプリケーション) を選択します。

5. 選択したアプリケーションにカーソルを合わせます。
6. アプリケーション名の横にある星を選択します。

> **Note**
>
> アプリケーションをお気に入りに追加すると、ナビゲーションバーの後にあるお気に入りクイックバーに追加されます。

でのお気に入りへのアクセス AWS マネジメントコンソール

お気に入りに追加したサービスおよびアプリケーションには、[サービス] メニュー、お気に入りクイックバー、[お気に入り] ウィジェットからアクセスできます。

Services menu

[サービス] メニューからお気に入りにアクセスするには

1. AWS マネジメントコンソール を開きます。
2. ナビゲーションバーで [サービス (⋮⋮⋮)] を選択します。
3. [お気に入り] を選択します。
4. お気に入りに追加したサービスおよびアプリケーションを表示します。
5. (オプション) アプリケーションリソースを表示します。
   a. アプリケーションを選択します。
   b. (オプション) [ビュー] を選択します。
   c. リソースを表示します。
   d. (オプション) フィルターを選択します。プロパティまたはタグでリソースをフィルタリングできます。詳細については、「AWS Resource Explorer ユーザーガイド」の「Resource Explorer の検索クエリ構文リファレンス」を参照してください。
   e. (オプション) リソースを選択して、関連するサービスコンソールで表示します。

> **Tip**
>
> [サービス (⋮⋮⋮)] を選択して、中断したところからリソースの閲覧を続けることができます。適用した検索フィルターも保持されます。

Favorites quickbar

お気に入りクイックバーからお気に入りにアクセスするには

1. AWS マネジメントコンソール を開きます。
2. お気に入りクイックバーでサービスおよびアプリケーションを表示します。

Favorites widget

お気に入りウィジェットからお気に入りにアクセスするには

1. AWS マネジメントコンソール を開きます。
2. (オプション) [お気に入り] ウィジェットにお気に入りがない場合は、お気に入りを追加します。
   a. [コンソール] ホームページの [+ ウィジェットの追加] ボタンを選択します。
   b. [ウィジェットの追加] メニューで、[⋮⋮] アイコンを使用して [お気に入り] ウィジェットをドラッグし、[コンソール] ホームページに配置します。
3. [お気に入り] ウィジェットでサービスおよびアプリケーションを表示します。

ウィジェットの詳細については、「the section called “ウィジェットの操作”」を参照してください。

でのお気に入りの削除 AWS マネジメントコンソール

[サービス] メニューを使用して、お気に入りからサービスとアプリケーションを削除できます。検索バーの検索結果ページを使用してサービスを削除することもできます。

Services menu

[サービス] メニューからお気に入りを削除するには

1. AWS マネジメントコンソール を開きます。
2. ナビゲーションバーで [サービス] を選択します。
3. [お気に入り] を選択します。
4. サービスまたはアプリケーションの横にある星を選択解除します。

Search box

> **Note**
>
> 現時点では、検索バーから検索結果ページを使用してのみサービスを削除できます。

検索ボックスからお気に入りを削除するには

1. AWS マネジメントコンソール を開きます。
2. 検索ボックスにサービス名を入力します。
3. 検索結果ページで、サービス名の横にある星印の選択を解除します。

でのパスワードの変更 AWS マネジメントコンソール

ユーザータイプとアクセス許可によっては、AWS マネジメントコンソール からパスワードを変更できます。次のトピックでは、ユーザータイプごとにパスワードを変更する方法について説明します。

トピック

- のルートユーザー AWS マネジメントコンソール
- の IAM ユーザー AWS マネジメントコンソール
- の IAM Identity Center ユーザー AWS マネジメントコンソール
- のフェデレーティッド ID AWS マネジメントコンソール

のルートユーザー AWS マネジメントコンソール

ルートユーザーは、 AWS マネジメントコンソールから直接パスワードを変更できます。ルートユーザーは、すべての AWS サービスとリソースへの完全なアクセス権を持つアカウント所有者です。AWS アカウントを作成し、ルートユーザーの E メールとパスワードを使用してサインインした場合、ユーザーはルートユーザーです。詳細については、「AWS IAM アイデンティティセンター ユーザーガイド」の「ルートユーザー」を参照してください。

ルートユーザーとしてパスワードを変更するには

1. AWS マネジメントコンソール にサインインします。
2. ナビゲーションバーで、アカウント名をクリックします。
3. [Security credentials] (セキュリティ認証情報) を選択します。

4. 表示されるオプションは、 AWS アカウント タイプによって異なります。コンソールに表示されている手順に従って、パスワードを変更します。
5. 現在のパスワードを 1 回、そして新しいパスワードを 2 回入力します。

   新しいパスワードは 8 文字以上にする必要があります。また、次の文字を含める必要があります。

   - 少なくとも 1 つの記号
   - 少なくとも 1 つの数値
   - 少なくとも 1 つの大文字
   - 少なくとも 1 つの小文字
6. [Change Password] (パスワードの変更) または [Save changes] (パスワードの保存) を選択します。

の IAM ユーザー AWS マネジメントコンソール

IAM ユーザーは、アクセス許可 AWS マネジメントコンソール に応じて、 からパスワードを変更できます。それ以外の場合は、 AWS アクセスポータルを使用する必要があります。IAM ユーザーは、特定のカスタムアクセス許可が付与された AWS アカウント内の ID です。 AWS アカウントを作成しておらず、管理者またはヘルプデスクの従業員が AWS 、アカウント ID またはアカウントエイリアス、IAM ユーザー名、パスワードを含むサインイン認証情報を提供した場合、ユーザーは IAM ユーザーです。詳細については、「AWS サインイン ユーザーガイド」の「IAM ユーザー」を参照してください。

以下のポリシーからのアクセス許可がある場合: AWS: IAM ユーザーがセキュリティ認証情報ページで自分のコンソールパスワードを変更できるようにする。コンソールからパスワードを変更できます。詳細については、「AWS Identity and Access Management ユーザーガイド」の「IAM ユーザーが自分のパスワードを変更する方法」を参照してください。

からパスワードを変更するために必要なアクセス許可がない場合は、「 AWS IAM アイデンティティセンター ユーザーガイド」のAWS IAM アイデンティティセンター 「ユーザーパスワードのリセット AWS マネジメントコンソール 」を参照してください。

の IAM Identity Center ユーザー AWS マネジメントコンソール

AWS IAM アイデンティティセンター ユーザーは、 AWS アクセスポータルからパスワードを変更する必要があります。詳細については、「 ユーザーガイド」の AWS IAM アイデンティティセンター「ユーザーパスワードのリセット」を参照してください。 AWS IAM アイデンティティセンター

IAM Identity Center ユーザーは、 AWS アカウントが の一部であり、一意の URL を使用して AWS アクセスポータルからサインイン AWS Organizations するユーザーです。これらのユーザーは、IAM Identity Center で直接作成することも、アクティブディレクトリまたは別の外部アイデンティティプロバイダーで作成することもできます。詳細については、「AWS サインイン ユーザーガイド」の「AWS IAM アイデンティティセンター ユーザー」を参照してください。

のフェデレーティッド ID AWS マネジメントコンソール

フェデレーティッド ID ユーザーは、 AWS アクセスポータルからパスワードを変更する必要があります。詳細については、「 ユーザーガイド」の AWS IAM アイデンティティセンター 「ユーザーパスワードのリセット」を参照してください。 AWS IAM アイデンティティセンター

フェデレーティッドアイデンティティユーザーは、外部 ID プロバイダー (IdP) を使用してサインインするユーザーです。以下のいずれかに該当する場合、あなたはフェデレーテッドアイデンティティです。

- Login with Amazon、Facebook、Google などのサードパーティーの認証情報を使用して、 AWS アカウントまたはリソースにアクセスします。
- 同じ認証情報を使用して企業システムや AWS サービスにサインインし、カスタム企業ポータルを使用してサインインします AWS。

詳細については、「AWS サインイン ユーザーガイド」の「フェデレーティッドアイデンティティ」を参照してください。

の言語の変更 AWS マネジメントコンソール

AWS Console Home エクスペリエンスには、 の AWS サービスのデフォルト言語を変更できる統合設定ページが含まれています AWS マネジメントコンソール。ナビゲーションバーの設定メニューから、デフォルトの言語をすばやく変更することもできます。

> **Note**
>
> この手順では、すべての AWS サービスコンソールの言語が変更されますが、 AWS ドキュメントの言語は変更されません。ドキュメントに使用される言語を変更するには、すべてのドキュメントページの右上にある言語メニューを使用します。

トピック

サポートされている言語

AWS マネジメントコンソール は現在、次の言語をサポートしています。

- 英語 (米国)
- 英語 (英国)
- バハサインドネシア語
- German
- Spanish
- フランス語
- Japanese
- Italian
- Portuguese
- Korean
- 簡体字中国語
- 繁体字中国語
- Turkish

のナビゲーションバーからデフォルト言語を変更する AWS マネジメントコンソール

次の手順では、ナビゲーションバーから直接デフォルトの言語を変更する方法について説明します。

ナビゲーションバーからデフォルトの言語を変更するには

1. AWS マネジメントコンソール にサインインします。
2. ナビゲーションバーで、 歯車アイコン (#) を選択します。
3. [言語] で、[ブラウザのデフォルト] を選択するか、ドロップダウンリストから希望する言語を選択します。

の統合設定によるデフォルト言語の変更 AWS マネジメントコンソール

次の手順では、統一された設定ページからデフォルト言語を変更する方法について詳しく説明します。

[統一された設定] でデフォルトの言語を変更するには

1. AWS マネジメントコンソール にサインインします。
2. ナビゲーションバーで、 歯車アイコン (#) を選択します。
3. [統一された設定] ページを開くには、[すべてのユーザー設定の表示] を選択します。
4. [統一された設定] で [ローカリゼーションとデフォルトのリージョン] の横にある [編集] を選択します。
5. コンソールで使用する言語を選択し、以下のオプションの 1 つを選択します。

   - ドロップダウンリストから [ブラウザのデフォルト] を選択し、[設定を保存] を選択します。

     すべての AWS サービスのコンソールテキストは、ブラウザ設定で設定した任意の言語で表示されます。

     > **Note**
     >
     > ブラウザのデフォルトは、 AWS マネジメントコンソールでサポートされている言語のみをサポートしています。

   - ドロップダウンリストから希望する言語を選択し、[設定を保存] を選択します。

     すべての AWS サービスのコンソールテキストが任意の言語で表示されます。

での AWS アカウント、組織、サービスクォータ、請求情報へのアクセス AWS マネジメントコンソール

必要なアクセス許可がある場合は、 コンソールから AWS アカウント、サービスクォータ、組織、請求情報に関する情報にアクセスできます。

> **Note**
>
> は、アカウント、組織、サービスクォータ、請求情報へのアクセス AWS マネジメントコンソール のみを提供します。これらのサービスには個別のコンソールがあります。詳細については次を参照してください:
>
> - AWS アカウント管理 リファレンスガイドの AWS アカウントを管理します。
> - AWS Organizations ユーザーガイドの「 AWS Organizationsとは」を参照してください。
> - 「Service Quotas ユーザーガイド」の「Service Quotas とは」
> - AWS 請求ユーザーガイドのAWS Billing and Cost Management ホームページの使用。

> **Tip**
>
> Amazon Q に質問することで、これらのトピックに関する詳細情報を取得することもできます。詳細については、「Amazon Q Developer とのチャット」を参照してください。

トピック

でのアカウント情報へのアクセス AWS マネジメントコンソール

必要なアクセス許可がある場合は、 コンソールから AWS アカウントに関する情報にアクセスできます。

アカウント情報にアクセスするには

1. AWS マネジメントコンソール にサインインします。
2. ナビゲーションバーで、アカウント名を選択します。
3. [アカウント] を選択します。
4. アカウント情報を表示します。

> **Note**
>
> AWS アカウントを閉鎖する場合は、「 AWS アカウント管理 リファレンスガイド」のAWS「アカウントを閉鎖する」を参照してください。

での組織情報へのアクセス AWS マネジメントコンソール

必要なアクセス許可がある場合は、 コンソールから AWS 組織に関する情報にアクセスできます。

組織情報にアクセスするには

1. AWS マネジメントコンソール にサインインします。
2. ナビゲーションバーで、アカウント名を選択します。
3. [組織]を選択します。
4. 組織情報を表示します。

のサービスクォータ情報へのアクセス AWS マネジメントコンソール

必要なアクセス権限を持っている場合、コンソールから Service Quotas に関する情報にアクセスできます。

Service Quotas 情報にアクセスするには

1. AWS マネジメントコンソール にサインインします。
2. ナビゲーションバーで、アカウント名を選択します。
3. [サービスクォータ] を選択します。
4. Service Quotas 情報を表示および管理します。

での請求情報へのアクセス AWS マネジメントコンソール

必要なアクセス許可がある場合は、 コンソールから AWS 料金に関する情報にアクセスできます。

請求情報にアクセスするには

1. AWS マネジメントコンソール にサインインします。

2. ナビゲーションバーで、アカウント名を選択します。
3. [請求情報とコスト管理] を選択します。
4. AWS Billing and Cost Management ダッシュボードを使用して、毎月の支出の概要と内訳を確認します。

複数のアカウントにサインインする

AWS マネジメントコンソール では、1 つのウェブブラウザで最大 5 つの異なる ID に同時にサインインできます。これらは、異なるアカウントまたは同じアカウントのルートロール、IAM ロール、またはフェデレーティッドロールの任意の組み合わせにすることができます。サインインする各 ID は、AWS マネジメントコンソール の独自のインスタンスを新しいタブで開きます。

マルチセッションサポートを有効にすると、コンソール URL にサブドメイン (例えば、`https://000000000000-aaaaaaaa.us-east-1.console.aws.amazon.com/console/home?region=us-east-1`) が含まれます。ブックマークとコンソールリンクを必ず更新してください。

> **Note**
>
> マルチセッションサポートにオプトインするには、AWS マネジメントコンソール のアカウントメニューで [マルチセッションを有効にする] を選択するか、https://console.aws.amazon.com/ で [マルチセッションを有効にする] を選択します。マルチセッションをいつでもオプトアウトするには、https://console.aws.amazon.com/ で [マルチセッションを無効にする] を選択するか、ブラウザの Cookie をクリアします。オプトインはブラウザ固有です。

複数の ID にサインインするには

1. にサインインします。。AWS マネジメントコンソール
2. ナビゲーションバーで、アカウント名をクリックします。
3. [セッションの追加] を選択し、[サインイン] を選択します。新しいタブが開き、サインインできます。

> **Note**
>
> ルートユーザーまたは IAM ユーザーとしてのサインインの詳細については、「AWS サインイン ユーザーガイド」の「AWS マネジメントコンソール へのサインイン」を参照してください。

4. 認証情報を入力します。
5. [サインイン] を選択します。AWS マネジメントコンソール は、選択した AWS ID としてこのタブにロードされます。
6. (オプション) 追加のロールにフェデレーションするには
   a. AWS IAM アイデンティティセンター アクセスポータルまたはシングルサインオン (SSO) ポータルで、追加のロールにサインインします。
   b. AWS マネジメントコンソール で、アカウント名を選択します。
   c. 選択できる追加のセッションを表示します。

AWS マネジメントコンソール の AWS 推奨アクション

AWS 推奨アクションは、タスクを完了し、ベストプラクティスを実装するためのコンテキストに応じた提案を提供することで、AWS マネジメントコンソール でより効率的に作業するのに役立ちます。関連する推奨が利用可能になると、動的ボタンが表示され、これらの提案に基づいて迅速にアクションを実行できます。

> **Note**
>
> AWS 推奨アクションはリソースの状態を分析して提案を提供しますが、ユーザーデータは処理しません。

トピック

- AWS 推奨アクションの機能
- 推奨アクションの使用
- を使用した AWS 推奨アクション API コールのログ記録 AWS CloudTrail

AWS 推奨アクションの機能

- アクションの推奨事項 — リソースの状態、ベストプラクティス、一般的な使用パターンに基づいて、関連する提案を取得します
- ワンクリックアクション — 成功メッセージまたはリソースビューから直接推奨アクションを実行します
- 統合右側パネル — 統合サイドパネルにアクセスして、ワークフローを中断することなく提案を実装します
- マルチサービスサポート — 複数の AWS サービスにまたがる推奨を取得します

推奨アクションの使用

推奨アクションを使用するには

1. AWS マネジメントコンソール にサインインします
2. # 推奨アクション ボタンを探します。

> **Note**
>
> 推奨アクションボタンは AWS マネジメントコンソール のどこにでも表示でき、推奨アクションが利用可能な場合にのみアクセスできます。

3. ボタンを選択すると、使用可能なアクションが表示されます。
4. 推奨を直接実行するか、サイドパネルから実行します。

を使用した AWS 推奨アクション API コールのログ記録 AWS CloudTrail

AWS 推奨アクションは、ユーザーAWS CloudTrail、ロール、または によって実行されたアクションを記録するサービスである と統合されています AWS のサービス。CloudTrail は、 AWS 推奨アクションのすべての API コールをイベントとしてキャプチャします。キャプチャされた AWS マネジメントコンソール 呼び出しには、 からの呼び出しと、 AWS 推奨アクション API オペレーションへのコード呼び出しが含まれます。CloudTrail で収集された情報を使用して、 AWS 推奨アクションに対するリクエスト、リクエスト元の IP アドレス、リクエスト日時などの詳細を確認できます。

CloudTrail は、アカウントを作成する AWS アカウント と でアクティブになり、CloudTrail イベント履歴に自動的にアクセスできます。CloudTrail の [イベント履歴] では、 AWS リージョンで過去

90 日間に記録された管理イベントの表示、検索、およびダウンロードが可能で、変更不可能な記録を確認できます。詳細については、「AWS CloudTrail ユーザーガイド」の「CloudTrail イベント履歴の使用」を参照してください。[イベント履歴] の閲覧には CloudTrail の料金はかかりません。

AWS アカウント 過去 90 日間のイベントの継続的な記録については、証跡または CloudTrail Lake イベントデータストアを作成します。

AWS CloudTrail での推奨アクション管理イベント

管理イベントは、 のリソースで実行される管理オペレーションに関する情報を提供します AWS アカウント。これらのイベントは、コントロールプレーンオペレーションとも呼ばれます。CloudTrail は、デフォルトで管理イベントをログ記録します。

AWS 推奨アクションは、すべての AWS 推奨アクションコントロールプレーンオペレーションを管理イベントとしてログに記録します。

AWS 推奨されるアクションイベントの例

各イベントは任意の送信元からの単一のリクエストを表し、リクエストされた API オペレーション、オペレーションの日時、リクエストパラメータなどに関する情報を含みます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、イベントは特定の順序で表示されません。

次の例は、 オペレーションを示す CloudTrail イベントを示しています。


```
{
  "awsRegion": "us-east-2",
  "eventCategory": "Management",
  "eventID": "3510a29e-8070-4cbc-b6a0-9e11f18e26ec",
  "eventName": "ListRecommendedActions",
  "eventSource": "action-recommendations.amazonaws.com",
  "eventTime": "2025-09-03T03:52:02Z",
  "eventType": "AwsApiCall",
  "eventVersion": "1.09",
  "managementEvent": true,
  "readOnly": true,
  "recipientAccountId": "123456789098",
  "requestID": "ec431c91-0315-413d-bdb6-d282fd4f6d83",
  "requestParameters": {
    "context": "*",
    "uxChannel": "EXAMPLE"
  },
```

```
  "responseElements": null,
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "EXAMPLE",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROARZDBH75ZCUYWFSTUS:EXAMPLE",
    "arn": "arn:aws:sts::123456789098:assumed-role/EXAMPLE",
    "accountId": "12345678909",
    "accessKeyId": "ASIARZDBEXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
          "type": "Role",
          "principalId": "AROARZDBHEXAMPLE",
          "arn": "arn:aws:iam::12345678909:role/EXAMPLE",
          "accountId": "12345678909",
          "userName": "EXAMPLE"
        },
        "attributes": {
          "creationDate": "2025-09-03T03:52:00Z",
          "mfaAuthenticated": "false"
        }
      },
    "invokedBy": "action-recommendations.amazonaws.com"
  }
}
```


CloudTrail レコードの内容については、「AWS CloudTrail ユーザーガイド」の「CloudTrail record contents」を参照してください。

AWS Console Home での の使用 AWS マネジメントコンソール

このトピックでは AWS Console Home、コンソールのホームページをカスタマイズする方法など、の使用方法について説明します。コンソールホームは、 AWS マネジメントコンソールのホームページです。コンソールに初めてログインすると、コンソールのホームページに移動します。ウィジェットとアプリケーションを使用して、コンソールホームページをカスタマイズできます。ウィジェットを使用すると、 AWS サービスとリソースに関する情報を追跡するカスタムコンポーネントを追加できます。アプリケーションを使用すると、 AWS リソースとメタデータをグループ化できます。myApplications を使用してアプリケーションを管理できます。Console Home を使用して、すべての AWS サービスのリストを表示したり、Amazon Q とチャットしたりすることもできます。

トピック

でのすべての AWS サービスの表示 AWS Console Home

すべての AWS サービスのリストを表示し、コンソールホームからコンソールにアクセスできます。

AWS サービスの完全なリストにアクセスするには

1. AWS マネジメントコンソール にサインインします。
2. ハンバーガーアイコン (☰) を選択して、コンソールホームメニューを展開します。
3. [すべてのサービス] を選択します。
4. コンソールに移動する AWS サービスを選択します。

でのウィジェットの使用 AWS Console Home

コンソールホームダッシュボードには、 AWS 環境に関する重要な情報を表示し、サービスへのショートカットを提供するウィジェットが含まれています。ウィジェットの追加と削除、再配置、またはサイズの変更により、エクスペリエンスをカスタマイズできます。

ウィジェットの管理

追加、削除、再配置、サイズ変更によってウィジェットを管理できます。デフォルトのウィジェットは削除して再度追加できます。コンソールホームをデフォルトのレイアウトにリセットし、新しいウィジェットをリクエストすることもできます。

ウィジェットを追加するには

1. コンソールホームダッシュボードの右上または右下にある [ウィジェットの追加] ボタンを選択します。
2. ウィジェットのタイトルバーの左上にある 6 つの縦のドット (⁝⁝) が示すドラッグインジケーターを選択し、コンソールホームダッシュボードまでドラッグします。

ウィジェットを削除するには

1. ウィジェットタイトルバーの右上にある 3 つの縦のドット (⁝) が示す省略記号を選択します。
2. [Remove widget] (ウィジェットの削除) を選択します。

ウィジェットを並べ替えるには

- ウィジェットのタイトルバーの左上にある 6 つの縦のドット (⁝⁝) が示すドラッグインジケーターを選択し、コンソールホームダッシュボードの新しい場所までドラッグします。

ウィジェットのサイズを変更するには

- ウィジェットの右下にあるサイズ変更アイコンを選択し、ウィジェットをページの新しい場所までドラッグします。

ウィジェットの整理と設定をやり直す場合は、コンソールホームダッシュボードをデフォルトのレイアウトにリセットできます。これにより、コンソールホームダッシュボードレイアウトへの変更が元に戻り、すべてのウィジェットがデフォルトの場所とサイズに復元されます。

ページをデフォルトレイアウトにリセットするには

1. ページの右上にある [デフォルトレイアウトにリセット] ボタンを選択します。
2. 確認するには、[リセット] を選択します。

> **Note**
>
> これにより、コンソールホームダッシュボードのレイアウトに対するすべての変更が元に戻ります。

コンソールホームダッシュボードで新しいウィジェットをリクエストするには

1. コンソールホームダッシュボードの左下にある [別のウィジェットをご希望の場合は、当社までお知らせください。] を選択します。

   コンソールホームダッシュボードへの追加を希望するウィジェットについて説明します。
2. [Submit] を選択してください。

> **Note**
>
> お客様の提案は定期的に確認されており、今後の AWS マネジメントコンソールのアップデートで新しいウィジェットが追加される可能性があります。

myApplications とは AWS Console Home

myApplications は、コンソールホームの拡張機能であり、 AWSでのアプリケーションのコスト、ヘルス、セキュリティ体制、パフォーマンスの管理とモニタリングに役立ちます。アプリケーションを使用すると、リソースとメタデータをグループ化できます。アカウント内のすべてのアプリケーション、すべてのアプリケーションの主要なメトリクス、コスト、セキュリティ、運用のメトリクスとインサイトの概要には、 の 1 つのビューからアクセスできます AWS マネジメントコンソール。myApplications には、次のものが含まれます。

- コンソールホームページのアプリケーションウィジェット
- アプリケーションリソースのコストとセキュリティ検出結果を表示するために使用できる myApplications
- コスト、パフォーマンス、セキュリティ検出結果などの主要なアプリケーションメトリクスを表示する myApplications ダッシュボード

トピック

- myApplications の機能

- 関連サービス
- myApplications へのアクセス
- 料金
- myApplications でサポートされているリージョン
- myApplications のアプリケーション
- myApplications のリソース
- の myApplications ダッシュボード AWS Console Home

myApplications の機能

- アプリケーションの作成 — 新しいアプリケーションを作成し、そのリソースを整理します。アプリケーションは myApplications に自動的に表示されるため、、APIs AWS マネジメントコンソール、CLI、および SDKs でアクションを実行できます。アプリケーションの作成時に Infrastructure as code (IaC) が生成され、myApplication ダッシュボードからアクセスできます。IaC は、 AWS CloudFormation や Terraform などの IaC ツールで使用できます。
- アプリケーションへのアクセス — どのアプリケーションでも、myApplications ウィジェットから選択してすばやくアクセスできます。
- リソースへのアクセス – アプリケーションを選択すると、[サービス] メニューからアプリケーションリソースをすばやく表示できます。リソースを選択すると、関連するサービスコンソールに直接移動します。リソーステーブル内の場所が保存されるため、[サービス] メニューからいつでもブラウジングを続行できます。
- アプリケーションのメトリクスの比較 — myApplications を使用すると、複数のアプリケーションにわたってアプリケーションリソースのコストや重要なセキュリティ検出結果の数など、アプリケーションの主要なメトリクスを比較できます。
- アプリケーションのモニタリングと管理 – アラーム、Canary、サービスレベルの目標、検出結果 Amazon CloudWatch、コスト傾向を使用して AWS Security Hub CSPM、アプリケーションのヘルスとパフォーマンスを評価します AWS Cost Explorer Service。コンピューティングメトリクスの概要と最適化を検索し、リソースのコンプライアンスと設定ステータスを管理することもできます AWS Systems Manager。

関連サービス

myApplications は、以下のサービスを利用します。

- AppRegistry
- AppManager
- Amazon CloudWatch
- Amazon EC2
- AWS Lambda
- AWS Resource Explorer
- AWS Security Hub CSPM
- Systems Manager
- AWS Service Catalog
- Tagging

myApplications へのアクセス

myApplications にアクセスするには、AWS マネジメントコンソールの左側のサイドバーで [myApplications] を選択します。

料金

の myApplications AWS は追加料金なしで提供されます。セットアップ料金や前払いの義務はありません。myApplication ダッシュボードに集約されている基盤となるリソースやサービスの使用料金は、該当するリソースの公表価格で引き続き適用されます。

myApplications でサポートされているリージョン

myApplications は、以下にあります AWS リージョン。

- 米国東部(オハイオ)
- 米国東部 (バージニア北部)
- 米国西部 (北カリフォルニア)
- 米国西部 (オレゴン)
- アジアパシフィック (ムンバイ)
- アジアパシフィック (大阪)
- アジアパシフィック (ソウル)
- アジアパシフィック (シンガポール)

- アジアパシフィック (シドニー)
- アジアパシフィック (東京)
- カナダ (中部)
- 欧州 (フランクフルト)
- 欧州 (アイルランド)
- 欧州 (ロンドン)
- 欧州 (パリ)
- 欧州 (ストックホルム)
- 南米 (サンパウロ)

オプトインリージョン

デフォルトでは、オプトインリージョンは有効ではありません。これらのリージョンを myApplications で使用するには、手動で各リージョンを有効にする必要があります。詳細については AWS リージョン、「 の管理 AWS リージョン」を参照してください。次のオプトインリージョンがサポートされています。

- アフリカ (ケープタウン)
- アジアパシフィック (香港)
- アジアパシフィック (ハイデラバード)
- アジアパシフィック (ジャカルタ)
- アジアパシフィック (メルボルン)
- 欧州 (ミラノ)
- 欧州 (スペイン)
- 欧州 (チューリッヒ)
- 中東 (バーレーン)
- 中東 (アラブ首長国連邦)
- イスラエル (テルアビブ)

myApplications のアプリケーション

アプリケーションを使用すると、リソースとメタデータをグループ化できます。アプリケーションを作成、オンボーディング、表示、編集、または削除することで管理できます。コードスニペットを作成して、新しいリソースを自動的にアプリケーションに追加することもできます。

> **Note**
>
> [お気に入り] にアプリケーションを追加して、アクセスしやすくすることもできます。詳細については、「???」を参照してください。

トピック

myApplications でのアプリケーションの作成

新しいアプリケーションを作成するか、2023 年 11 月 8 日より前に作成した the section called “アプリケーションのオオンボード” を使用して myApplications の使用を開始できます。新しいアプリケーションを作成するときは、リソースを検索して選択するか、既存のタグを使用してリソースを追加できます。

新しいアプリケーションを作成するには

1. AWS マネジメントコンソール にサインインします。
2. 左側のサイドバーを展開し、[myApplications] を選択します。
3. [アプリケーションを作成] を選択します。
4. アプリケーション名を入力します。
5. (オプション) アプリケーションの説明を入力します。
6. (オプション) タグを追加します。タグはリソースに適用されるキーと値のペアで、リソースに関するメタデータを保持します。

> **Note**
>
> AWS アプリケーションタグは、新しく作成されたアプリケーションに自動的に適用されます。詳細については、AWS Service Catalog AppRegistry 管理者ガイドの AWS「アプリケーションタグ」を参照してください。

7. (オプション) 属性グループを追加します。属性グループを使用してアプリケーションのメタデータを保存できます。
8. [次へ] を選択します。
9. (オプション) リソースを追加します。

   Search and select resources

   > **Note**
   >
   > リソースを検索して追加するには、 AWS Resource Explorerをオンにする必要があります。詳細については、「 の開始方法 AWS Resource Explorer」を参照してください。
   > 追加されたすべてのリソースには、 AWS アプリケーションタグが付けられます。

   検索を使用してリソースを追加するには

   1. [リソースの検索と選択] を選択します。
   2. [リソースを選択] を選択します。
   3. (オプション) ビューを選択します。
   4. リソースを検索します。キーワード、名前、またはタイプで検索するか、リソースタイプを選択することができます。

      > **Note**
      >
      > 探しているリソースが見つからない場合は、トラブルシューティングを行います AWS Resource Explorer。詳細については、[Resource Explorer ユーザーガイド」の「Resource Explorer での検索に関する問題のトラブルシューティング」を参照してください。

5. 追加するユーザーの横のチェックボックスをオンにします。
6. [Add] (追加) を選択します。
7. [次へ] を選択します。
8. 選択内容を確認します。

Automatically add resources using tags

アプリケーションを作成するときは、既存のタグキーと値のペアを指定することで、リソースを一括でオンボードできます。この方法では、 は指定されたキーと値のペアでタグ付けされたすべてのリソースに`awsApplication`タグ AWS を自動的に適用し、デフォルトでアプリケーションのリソースのタグ同期を作成します。タグ同期を有効にすると、指定されたタグキーと値のペアでタグ付けされたリソースが自動的にアプリケーションに追加されます。タグ同期のエラーを解決する方法の詳細については、「the section called “myApplications でのタグ同期エラーの解決”」を参照してください。

> **Note**
>
> タグを使用してアプリケーションにリソースを追加するには、AppRegistry アプリケーションを作成し、リソースをグループ化またはグループ解除し、リソースにタグを付けたり削除したりする権限が必要です。Resource Groups `ResourceGroupsTaggingAPITagUntagSupportedResources` AWS 管理ポリシーを追加するか、独自のカスタムポリシーを作成して維持できます。IAM のユーザーのポリシーステートメントに次のアクセス許可を追加する必要があります。
>
> - `servicecatalog:CreateApplication`
> - `resource-groups:GroupResources`
> - `resource-groups:UngroupResources`
> - `tag:TagResources`
> - `tag:UntagResources`

既存のタグを使用してリソースを追加するには

1. [タグを使用してリソースを自動的に追加] を選択します。
2. 既存のタグキーと値を選択します。

a. リソースにタグを付けるために使用される [ロール] を選択します。詳細については、「AWS Service Catalog AppRegistry 管理者ガイド」の「タグ同期にはアクセス許可が必要」を参照してください。

b. [タグキー] を選択します。

c. [タグ値] を選択します。

d. (オプション) [リソースのプレビュー] を選択して、タグキーと値のペアでタグ付けされているリソースをプレビューします。

e. 「タグ同期を作成するために、グループライフサイクルイベントが有効になることを認識しています」通知を確認して同意します。GLE では AWS 、 がキーと値のペアでタグ付けされたリソースの変更に気付くことができます。

3. [次へ] を選択します。

4. アプリケーションの詳細、選択したタグキーと値のペア、アプリケーションに追加されるリソースのプレビューを確認します。

> **Note**
>
> デフォルトでは、既存のタグキーと値のペアを使用してアプリケーションを作成すると、タグ同期が作成されます。また、セットアップ後、タグ同期はアプリケーションのリソースを継続的に管理し、指定されたキーと値のペアでタグ付けまたはタグ付け解除されたリソースを追加または削除します。タグ同期は、アプリケーションのリソース管理ページから管理できます。

10. CloudFormation スタックを関連付ける場合は、ページの下部にあるチェックボックスをオンにします。

> **Note**
>
> CloudFormation スタックをアプリケーションに追加すると、アプリケーションに追加されたすべてのリソースに AWS アプリケーションタグが付けられるため、スタックの更新が必要です。スタックの最終更新後に実行した手動設定は、この更新後に反映されない場合があります。これにより、ダウンタイムなどのアプリケーションの問題が発生する可能性があります。詳細については、「CloudFormation ユーザーガイド」の「スタックのリソースの更新動作」を参照してください。

11. [アプリケーションを作成] を選択します。

myApplications への既存の AppRegistry アプリケーションのオンボード

2023 年 11 月 8 日より前に作成した既存の AppRegistry アプリケーションをオンボードして、myApplications の使用を開始できます。

既存の AppRegistry アプリケーションをオンボードするには

1. AWS マネジメントコンソールにサインインします。
2. 左側のサイドバーで [myApplications] を選択します。
3. 検索バーを使用してアプリケーションを見つけます。
4. アプリケーションを選択します。
5. [**********をオンボード」を選択します。
6. CloudFormation スタックを関連付ける場合は、アラートボックスのチェックボックスをオンにします。
7. [アプリケーションをオンボード] を選択します。

myApplications でのアプリケーションの表示

アプリケーションは、myApplications または [サービス] メニューから表示できます。myApplications からアプリケーションを表示する場合は、すべて AWS リージョン または特定のアプリケーション AWS リージョン とその関連情報をカードまたはテーブルビューで表示できます。

> **Note**
>
> お気に入りメニューから、お気に入りに追加されたアプリケーションを表示することもできます。詳細については、「のお気に入り AWS マネジメントコンソール」を参照してください。

myApplications

myApplications のアプリケーションを表示するには

1. AWS マネジメントコンソール を開きます。
2. 左側のサイドバーで [myApplications] を選択します。
3. [リージョン] で、[現在のリージョン] または [サポートされているリージョン] を選択します。

4. 特定のアプリケーションを検索するには、その名前、キーワード、または説明を検索バーに入力します。
5. (オプション) デフォルトのビューはカードビューです。アプリケーションページをカスタマイズするには、次の手順に従います。
   a. 歯車アイコンを選択します。
   b. (オプション) ページサイズを選択します。
   c. (オプション) カードビューまたはテーブルビューを選択します。
   d. (オプション) ページサイズを選択します。
   e. (オプション) テーブルビューを使用する場合は、テーブルビューのプロパティを選択します。
   f. (オプション) 表示するアプリケーションのプロパティと表示順序を切り替えます。
   g. [確認] を選択します。

Services menu

[サービス] メニューからアプリケーションを表示するには

1. AWS マネジメントコンソール を開きます。
2. ナビゲーションバーで [サービス (⁝⁝⁝)] を選択します。
3. [すべてのアプリケーション] を選択します。
4. アプリケーションを選択します。
5. (オプション) [ビュー] を選択します。
6. (オプション) フィルターを選択します。プロパティまたはタグでリソースをフィルタリングできます。詳細については、「AWS Resource Explorer ユーザーガイド」の「Resource Explorer の検索クエリ構文リファレンス」を参照してください。
7. (オプション) リソースを選択して、関連するサービスコンソールで表示します。

> **Tip**
>
> [サービス (⁝⁝⁝)] を選択して、中断したところからリソースの閲覧を続けることができます。適用した検索フィルターも保持されます。

myApplications でのアプリケーションの編集

アプリケーションの編集に伴って AppRegistry が開き、その説明を更新できるようになります。AppRegistry を使用してアプリケーションのタグと属性グループを編集することもできます。

アプリケーションを編集するには

1. AWS マネジメントコンソールを開きます。
2. コンソールの左側のサイドバーで、[myApplications] を選択します。
3. 編集するアプリケーションを選択します。
4. myApplication ダッシュボードで、[アクション]、[アプリケーションの編集] の順に選択します。
5. [アプリケーションの編集] で、アプリケーションの説明、タグ、属性グループに必要な変更を加えます。

   > **Note**
   >
   > タグと属性グループの管理の詳細については、「AWS Service Catalog AppRegistry 管理者ガイド」の「タグの管理」と「属性グループの編集」を参照してください。

6. [更新] を選択します。

myApplications でのアプリケーションの削除

アプリケーションが不要になった場合は、削除できます。アプリケーションを削除する前に、 AWS サービスによって作成されていない関連するリソース共有と属性グループをすべて削除してください。

> **Note**
>
> アプリケーションを削除しても、リソースには影響しません。 AWS アプリケーションタグでタグ付けされたリソースはタグ付けされたままになります。

アプリケーションを削除するには

1. AWS マネジメントコンソールを開きます。
2. コンソールの左側のサイドバーで、[myApplications] を選択します。

3. 削除するアプリケーションを選択します。
4. myApplication ダッシュボードで、[アクション] を選択します。
5. [アプリケーションを削除] を選択します。
6. 削除を選択し、確定します。

myApplications でのコードスニペットの作成

myApplications は、すべてのアプリケーションのコードスニペットを作成します。コードスニペットを使用すると、Infrastructure as Code (IaC) ツールを使用して、新しく作成したリソースをアプリケーションに自動的に追加できます。追加されたすべてのリソースには、 AWS アプリケーションに関連付けるアプリケーションタグが付けられます。

アプリケーションのコードスニペットを作成するには

1. AWS マネジメントコンソールを開きます。
2. コンソールの左側のサイドバーで、[myApplications] を選択します。
3. アプリケーションを検索して選択します。
4. [アクション] を選択します。
5. [コードスニペットを取得] を選択します。
6. コードスニペットタイプを選択します。
7. [コピー] を選択して、コードをクリップボードにコピーします。
8. コードを IaC ツールに貼り付けます。

myApplications のリソース

では AWS、リソースは操作できるエンティティです。例としては、Amazon EC2 インスタンス、AWS CloudFormation スタック、Amazon S3 バケットなどがあります。myApplications でリソースを管理するには、アプリケーションにリソースを追加または削除します。

トピック

- myApplications でのリソースの追加
- myApplications でのリソースの削除
- myApplications でのリソースの表示

myApplications でのリソースの追加

アプリケーションにリソースを追加すると、リソースをグループ化して、セキュリティ、パフォーマンス、コンプライアンスを管理できます。リソースを検索して選択するか、既存のタグを使用してタグ同期を実行することで、既存のアプリケーションにリソースを追加できます。

Search and select resources

リソースを検索して選択するには

1. AWS マネジメントコンソールを開きます。
2. コンソールの左側のサイドバーで、[myApplications] を選択します。
3. アプリケーションを検索して選択します。
4. [リソースを管理] を選択します。
5. [リソースを追加] を選択します。
6. (オプション) ビューを選択します。
7. リソースを検索します。キーワード、名前、またはタイプで検索するか、リソースタイプを選択することができます。

> **Note**
>
> 探しているリソースが見つからない場合は、トラブルシューティングを行います AWS Resource Explorer。詳細については、[Resource Explorer ユーザーガイド」の「Resource Explorer での検索に関する問題のトラブルシューティング」を参照してください。

8. 追加するユーザーの横のチェックボックスをオンにします。
9. [Add] (追加) を選択します。

Automatically add resources using tags

アプリケーションを作成するときは、既存のタグキーと値のペアを指定することで、リソースを一括でオンボードできます。この方法では、 はすべてのリソースに `awsApplication` タグ AWS を自動的に適用し、デフォルトでアプリケーションのリソースのタグ同期を作成します。タグ同期を有効にすると、指定されたタグキーと値のペアでタグ付けされたリソースが自動的にアプリケーションに追加されます。

既存のタグを使用してリソースを追加するには

1. AWS マネジメントコンソールを開きます。
2. コンソールの左側のサイドバーで、[myApplications] を選択します。
3. [リソースを管理] を選択します。
4. [タグ同期の作成] を選択します。
5. 既存のタグキーと値を選択します。
   a. リソースにタグを付けるために使用される [ロール] を選択します。詳細については、「AWS Service Catalog AppRegistry 管理者ガイド」の「タグ同期タスクに必要なアクセス許可」を参照してください。
   b. [タグキー] を選択します。
   c. [タグ値] を選択します。
   d. 「タグ同期を作成するために、グループライフサイクルイベントが有効になることを認識しています」通知を確認して同意します。GLE では AWS 、 がキーと値のペアでタグ付けされたリソースの変更に気付くことができます。
6. [タグ同期の作成] を選択します。

myApplications でのタグ同期エラーの解決

このセクションでは、一般的なタグ同期エラーとその解決方法について説明します。エラーの解決を試行した後、失敗したタグ同期タスクを再試行できます。

- アクセス許可が不十分 — タグ同期を開始、更新、またはキャンセルするために必要な最低限のアクセス許可がありません。詳細については、「タグ同期にはアクセス許可が必要」を確認してください。タグ同期の実行に指定したロールに必要な最低限のアクセス許可があることを確認したら、失敗したタグ同期タスクを再試行します。
- 既に存在する — このアプリケーションには、このタグのキーと値のペアを持つタスクが既に存在します。アプリケーションは複数のタグ同期をサポートできますが、各タグ同期には異なるタグキーと値のペアが必要です。別のタグキーと値のペアを指定したら、失敗したタグ同期タスクを再試行します。
- 上限に達している — アプリケーション全体で、アカウントごとの上限である 100 個のタグ同期タスクに達しました。

myApplications でのリソースの削除

リソースを削除して、アプリケーションとの関連付けを解除できます。

リソースを削除するには

1. AWS マネジメントコンソールを開きます。
2. コンソールの左側のサイドバーで、[myApplications] を選択します。
3. アプリケーションを検索して選択します。
4. [リソースを管理] を選択します。
5. (オプション) ビューを選択します。
6. リソースを検索します。キーワード、名前、またはタイプで検索するか、リソースタイプを選択することができます。

> **Note**
>
> 探しているリソースが見つからない場合は、トラブルシューティングを行います AWS Resource Explorer。詳細については、[Resource Explorer ユーザーガイド」の「Resource Explorer での検索に関する問題のトラブルシューティング」を参照してください。

7. [を削除] を選択します。
8. [リソースを削除] を選択して、リソースを削除することを確認します。

myApplications でのリソースの表示

アプリケーションリソースは、myApplications および [サービス] メニューから表示できます。

myApplications

myApplications でリソースを表示するには

1. AWS マネジメントコンソール を開きます。
2. 左側のサイドバーを展開し、[myApplications] を選択します。
3. アプリケーションを選択します。
4. [リソース] ウィジェットで、リソースを表示します。

Services menu

[サービス] メニューからアプリケーションを表示するには

1. AWS マネジメントコンソール を開きます。
2. ナビゲーションバーで [サービス (⋮⋮⋮)] を選択します。
3. [すべてのアプリケーション] を選択します。
4. アプリケーションを選択します。
5. (オプション) [ビュー] を選択します。
6. (オプション) フィルターを選択します。プロパティまたはタグでリソースをフィルタリングできます。詳細については、「AWS Resource Explorer ユーザーガイド」の「Resource Explorer の検索クエリ構文リファレンス」を参照してください。
7. (オプション) リソースを選択して、関連するサービスコンソールで表示します。

> **Tip**
>
> [サービス (⋮⋮⋮)] を選択して、中断したところからリソースの閲覧を続けることができます。適用した検索フィルターも保持されます。

の myApplications ダッシュボード AWS Console Home

作成またはオンボードするアプリケーションごとに、独自の myApplications ダッシュボードがあります。myApplications ダッシュボードには、複数の AWS サービスからのインサイトを示すコスト、セキュリティ、運用ウィジェットが含まれています。各ウィジェットのお気に入り登録、並べ替え、削除、またはサイズ変更も可能です。詳細については、「でのウィジェットの使用 AWS Console Home」を参照してください。

トピック

- アプリケーションダッシュボード設定ウィジェット
- アプリケーション概要ウィジェット
- コンピューティングウィジェット
- コストと使用状況ウィジェット
- AWS セキュリティウィジェット
- AWS レジリエンシーウィジェット

- リソースウィジェット
- DevOps ウィジェット
- モニタリングと運用ウィジェット
- タグウィジェット

アプリケーションダッシュボード設定ウィジェット

このウィジェットには、アプリケーションリソースを管理する AWS のサービス ための の設定に役立つ、推奨される開始方法アクティビティのリストが含まれています。

アプリケーション概要ウィジェット

このウィジェットには、アプリケーションの名前、説明、AWS アプリケーションタグが表示されます。Infrastructure as Code (IAC) のアプリケーションタグにアクセスしてコピーし、リソースに手動でタグを付けることができます。

コンピューティングウィジェット

このウィジェットには、アプリケーションに追加するコンピューティングリソースの情報とメトリクスが表示されます。これには、アラームの合計数とコンピューティングリソースタイプの合計数が含まれます。このウィジェットには、Amazon EC2 インスタンスの CPU 使用率と Lambda 呼び出し Amazon CloudWatch に関する からのリソースパフォーマンスメトリクスの傾向グラフも表示されます。

コンピューティングウィジェットの設定

コンピューティングウィジェットにデータを入力するには、アプリケーションに少なくとも 1 つの Amazon EC2 インスタンスまたは Lambda 関数を設定します。詳細については、Amazon Elastic Compute Cloud ドキュメントと「AWS Lambda デベロッパーガイド」の「Lambda の開始方法」を参照してください。

コストと使用状況ウィジェット

このウィジェットには、アプリケーションリソースの AWS コストと使用状況のデータが表示されます。このデータを使用して、 AWS のサービスごとの毎月のコストを比較し、コストの内訳を表示できます。このウィジェットは、 AWS アプリケーションタグでタグ付けされたリソースのコストのみを要約します。ただし、税金、料金、およびリソースに直接関連付けられていないその他の共有コストは除きます。コストは、非ブレンドとして表示され、24 時間ごとに最低 1 回更新されます。詳細

については、「AWS Cost Management ユーザーガイド」の「AWS Resource Explorerを用いてコストを分析する」を参照してください。

コストと使用状況ウィジェットの設定

コストと使用状況ウィジェットを設定するには、アプリケーションとアカウント AWS Cost Explorer Service に対して を有効にします。このサービスは追加料金なしで提供され、セットアップ料金や前払いの義務もありません。詳細については、「AWS Cost Management ユーザーガイド」の「Cost Explorer を有効にする」を参照してください。

AWS セキュリティウィジェット

このウィジェットには、アプリケーションの AWS Security のセキュリティ検出結果が表示されます。 AWS Security は、 のアプリケーションのセキュリティ検出結果を包括的に表示します AWS。最近の優先度の高い検出結果に対する重大度別のアクセス、セキュリティ体制のモニタリング、最近の重要度/重大度の高い検出結果へのアクセス、次のステップに向けたインサイトの取得を行うことができます。詳細については、「AWS Security Hub CSPM」を参照してください。

AWS セキュリティウィジェットの設定

AWS セキュリティウィジェットを設定するには、アプリケーションとアカウント AWS Security Hub CSPM 用に を設定します。詳細については、「 AWS Security Hub CSPM ユーザーガイド」の「What is AWS Security Hub CSPM?」を参照してください。料金情報については、「AWS Security Hub CSPM ユーザーガイド」の「AWS Security Hub CSPM の無料トライアル、使用状況、料金」を参照してください。。

AWS Security Hub CSPM では、Config Recording AWS を設定する必要があります。このサービスは、 AWS アカウントに関連付けられたリソースの詳細ビューを提供します。詳細については、AWS Systems Manager ユーザーガイドの AWS Systems Managerを参照してください。

AWS レジリエンシーウィジェット

このウィジェットには、アプリケーションの AWS Resilience Hub からの障害耐性の詳細が表示されます。評価を開始した後、 AWS Resiliency Hub は、事前定義された障害耐性ポリシーに照らしてリソースを評価することで、アプリケーションの障害耐性体制を分析します。耐障害性スコア、ポリシー違反、ポリシードリフト、リソースドリフト、耐障害性スコアの履歴などのメトリクスにアクセスできます。アプリケーションは高度な追跡のために毎日評価されますが、この機能をいつでも無効にできます。詳細については、「AWS Resilience Hub」を参照してください。料金情報については、「AWS Resilience Hub の料金」を参照してください。

AWS レジリエンシーウィジェットの設定

AWS 障害耐性ウィジェットを設定するには、アプリケーションを追加します。詳細については、「AWS Resilience Hub ユーザーガイド」の「What is AWS Resilience Hub?」を参照してください。

リソースウィジェット

このウィジェットは、 AWS Resource Explorer を使用して、アプリケーションに追加したリソースをビュー内に表示します。また、このウィジェットを使用して名前、タグ、ID などのリソースメタデータを使用してリソースを検索またはフィルタリングできます。詳細については、「AWS Resource Explorer」を参照してください。

リソースウィジェットの設定

リソースウィジェットを設定するには、Resource Explorer をオンボードします。詳細については、「AWS Resource Explorer ユーザーガイド」の「Resource Explorer の使用開始」を参照してください。

DevOps ウィジェット

このウィジェットには運用上のインサイトが表示されるため、コンプライアンスを評価して、アプリケーションに対してアクションを実行できます。これらのインサイトには以下が含まれます。

- フリートの管理
- 状態の管理
- パッチ管理
- 設定と OpsItems の管理

DevOps ウィジェットの設定

DevOps ウィジェットを設定するには、アプリケーションとアカウントの enable AWS Systems Manager OpsCenter を有効にします。詳細については、「AWS Systems Manager ユーザーガイド」の「Systems Manager Explorer と OpsCenter の開始方法」を参照してください。OpsCenter を有効にする AWS Systems Manager Explorer と、 は AWS Config と を設定 Amazon CloudWatch して、そのイベントが一般的に使用されるルールとイベントに基づいて OpsItems を自動的に作成できるようにします。詳細については、「AWS Systems Manager ユーザーガイド」の「OpsCenter をセットアップする」を参照してください。

Systems Manager エージェントを実行するようにインスタンスを設定し、パッチスキャンを有効にするアクセス許可を適用できます。詳細については、「AWS Systems Manager ユーザーガイド」の「AWS Systems Manager Quick Setup」を参照してください。

AWS Systems Manager Patch Manager を設定することで、アプリケーションの Amazon EC2 インスタンスの自動パッチ適用を設定することもできます。詳細については、「AWS Systems Manager ユーザーガイド」の「Quick Setup パッチポリシーの使用」を参照してください。

料金情報については、「AWS Systems Manager の料金」を参照してください。

モニタリングと運用ウィジェット

このウィジェットには以下が表示されます。

- アプリケーションに関連するリソースのアラームとアラート
- アプリケーションのサービスレベル目標 (SLO) とメトリクス
- 使用可能な AWS Application Signals メトリクス

モニタリングと運用ウィジェットの設定

モニタリングとオペレーションウィジェットを設定するには、 AWS アカウントに CloudWatch アラームと Canary を作成します。詳細については、「Amazon CloudWatch ユーザーガイド」の「Amazon CloudWatch でのアラームの使用」と「canary を作成する」を参照してください。CloudWatch アラームと synthetic canary の料金については、「Amazon CloudWatch の料金」と「AWS クラウドの運用と移行に関するブログ」をそれぞれ参照してください。

CloudWatch Application Signals の詳細については、「Amazon CloudWatch ユーザーガイド」の「Amazon CloudWatch Application Signals を有効にする」を参照してください。

タグウィジェット

このウィジェットには、アプリケーションに関連するすべてのタグが表示されます。このウィジェットを使用して、アプリケーションのメタデータ (重要度、環境、コストセンター) を追跡および管理できます。詳細については、「 リソースのタグ付けのベストプラクティス」ホワイトペーパーの「タグとは」を参照してください。 AWS AWS

AWS Console Home での Amazon Q Developer とのチャット

Amazon Q Developer は、生成人工知能 (AI) を活用した会話型アシスタントであり、AWS アプリケーションの理解、構築、拡張、運用を支援します。AWS アーキテクチャ、AWS リソース、ベス

トプラクティス、ドキュメントなど、AWS に関するご質問は、Amazon Q にお問い合わせください。サポートケースを作成し、ライブエージェントからサポートを受けることもできます。詳細については、「Amazon Q Developer ユーザーガイド」の「Amazon Q とは」を参照してください。

Amazon Q の使用を開始する

AWS マネジメントコンソール、AWS ドキュメントウェブサイト、AWS ウェブサイト、AWS コンソールモバイルアプリケーションで、六角形の Amazon Q アイコンを選択することで Amazon Q とのチャットを開始できます。詳細については、「Amazon Q Developer ユーザーガイド」の「Amazon Q Developer の使用開始」を参照してください。

質問例

以下は、Amazon Q に尋ねることができる質問の例です。

- `How do I get billing support?`
- `How do I create an EC2 instance?`
- `How do I troubleshoot a "Failed to load" error?`
- `How do I close an AWS account?`
- `Can you connect me with a person?`

AWS マネジメントコンソール プライベートアクセス

AWS マネジメントコンソール プライベートアクセスは、 へのアクセスを制御するための高度なセキュリティ機能です AWS マネジメントコンソール。コンソールプライベートアクセスは、ユーザーがネットワーク内から予期しない AWS アカウント にサインインしないようにする場合に便利です。この機能を使用すると、トラフィックがネットワーク内から発信された AWS アカウント ときに、指定された既知のセット AWS マネジメントコンソール にのみ へのアクセスを制限できます。コンソールのプライベートアクセスは、 からのすべての呼び出し AWS マネジメントコンソール が AWS のサービス ネットワーク内および許可されたアカウントから発信されるようにする場合にも役立ちます。

トピック

- プライベートアクセスでサポートされる AWS リージョンサービスコンソールと機能
- AWS マネジメントコンソール プライベートアクセスのセキュリティコントロールの概要
- 必要な VPC エンドポイントと DNS 設定
- サービスコントロールポリシーと VPC エンドポイントポリシーの実装
- アイデンティティベースのポリシーとその他のポリシータイプの実装
- AWS マネジメントコンソール プライベートアクセスを試す
- リファレンスアーキテクチャ

プライベートアクセスでサポートされる AWS リージョンサービスコンソールと機能

AWS マネジメントコンソール プライベートアクセスは、リージョンと AWS サービスのサブセットのみをサポートします。サポートされていないサービスコンソールは、 AWS マネジメントコンソールで非アクティブになります。さらに、統合設定のデフォルトリージョンの選択など、 AWS マネジメントコンソール プライベートアクセスの使用時に特定の AWS マネジメントコンソール 機能が無効になる場合があります。

以下のリージョンとサービスコンソールがサポートされています。

サポート対象のリージョン

- 米国東部(オハイオ)
- 米国東部 (バージニア北部)

- 米国西部 (北カリフォルニア)
- 米国西部 (オレゴン)
- アジアパシフィック (ハイデラバード)
- アジアパシフィック (ムンバイ)
- アジアパシフィック (ソウル)
- アジアパシフィック (大阪)
- アジアパシフィック (シンガポール)
- アジアパシフィック (シドニー)
- アジアパシフィック (マレーシア)
- アジアパシフィック (タイ)
- アジアパシフィック (東京)
- カナダ (中部)
- 欧州 (フランクフルト)
- 欧州 (アイルランド)
- 欧州 (ロンドン)
- 欧州 (パリ)
- 欧州 (ストックホルム)
- 南米 (サンパウロ)
- アフリカ (ケープタウン)
- アジアパシフィック (香港)
- アジアパシフィック (ジャカルタ)
- アジアパシフィック (メルボルン)
- カナダ西部 (カルガリー)
- メキシコ (中部)
- 欧州 (ミラノ)
- 欧州 (スペイン)
- 欧州 (チューリッヒ)
- 中東 (バーレーン)
- 中東 (アラブ首長国連邦)

- イスラエル (テルアビブ)

サポートされているサービスコンソール

- Amazon API Gateway
- AWS App Mesh
- AWS Application Migration Service
- AWS Artifact
- Amazon Athena
- AWS Audit Manager
- AWS Auto Scaling
- AWS Batch
- AWS Billing Conductor
- AWS Billing and Cost Management
- AWS Budgets
- AWS Certificate Manager
- AWS Cloud Map
- AWS CloudFormation
- Amazon CloudFront
- AWS CloudTrail
- Amazon CloudWatch
- AWS CodeArtifact
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- Amazon CodeGuru
- AWS CodePipeline
- Amazon Comprehend
- Amazon Comprehend Medical
- AWS Compute Optimizer

- AWS Console Home
- AWS Control Tower
- Amazon DataZone
- AWS Database Migration Service
- AWS DataSync
- AWS DeepRacer
- AWS Direct Connect
- AWS Directory Service
- Amazon DocumentDB
- Amazon DynamoDB
- Amazon EC2
- Amazon EC2 Global View
- EC2 イメージビルダー
- Amazon EC2 Instance Connect
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- AWS Elastic Disaster Recovery
- Amazon Elastic File System
- アマゾン エラスティックKubernetesサービス
- エラスティックロードバランシング
- Amazon ElastiCache
- Amazon EMR
- Amazon EventBridge
- AWS Firewall Manager
- Amazon GameLift Servers
- AWS Glue
- AWS Global Accelerator
- AWS Glue DataBrew
- AWS Ground Station

- Amazon GuardDuty
- AWS IAM アイデンティティセンター
- AWS Identity and Access Management
- AWS Identity and Access Management Access Analyzer
- Amazon Inspector
- Amazon Kendra
- AWS Key Management Service
- Amazon Kinesis
- Amazon Managed Service for Apache Flink
- Amazon Data Firehose
- Amazon Kinesis Data Streams
- Amazon Kinesis Video Streams
- AWS Lambda
- Amazon Lex
- AWS License Manager
- Amazon Managed Grafana
- Amazon Macie
- Amazon Managed Streaming for Apache Kafka
- Amazon Managed Workflows for Apache Airflow (MWAA)
- AWS Migration Hub Strategy Recommendations
- Amazon MQ
- Network Access Analyzer
- AWS Network Firewall
- AWS Network Manager
- Amazon OpenSearch Service
- AWS Organizations
- AWS Private Certificate Authority
- Public Health Dashboard
- Amazon Rekognition

- Amazon Relational Database Service
- AWS Resource Access Manager
- AWS Resource Groups およびタグエディタ
- Amazon Route 53 Resolver
- Amazon Route 53 Resolver DNS ファイアウォール
- Amazon S3 on Outposts
- Amazon SageMaker
- Amazon SageMaker ランタイム
- Amazon SageMaker AI 合成データ
- AWS Secrets Manager
- AWS Service Catalog
- AWS Security Hub CSPM
- サービスクォータ
- AWS Signer
- Amazon Simple Email Service
- Amazon SNS
- Amazon Simple Queue Service
- Amazon Simple Storage Service (Amazon S3)
- AWS SQL Workbench
- AWS Step Functions
- AWS Storage Gateway
- サポート
- AWS Systems Manager
- Amazon Timestream
- AWS Transfer Family
- AWS Trusted Advisor
- 統一された設定
- Amazon VPC IP アドレスマネージャー
- Amazon Virtual Private Cloud

- Amazon WorkSpaces シンクライアント

AWS マネジメントコンソール プライベートアクセスのセキュリティコントロールの概要

ネットワーク AWS マネジメントコンソール からの のアカウント制限

AWS マネジメントコンソール プライベートアクセスは、ネットワーク AWS マネジメントコンソール からの へのアクセスを組織 AWS アカウント 内の既知の指定されたセットのみに制限する場合に役立ちます。そうすることにより、ユーザーがネットワーク内から予期しない AWS アカウント にログインするのを防ぐことができます。これらのコントロールは、 AWS マネジメントコンソール VPC エンドポイントポリシーを使用して実装できます。詳細については、「サービスコントロールポリシーと VPC エンドポイントポリシーの実装」を参照してください。

ネットワークからインターネットへの接続

静的コンテンツ (JavaScript AWS マネジメントコンソール、CSS、イメージ) など、 で使用されるアセットにアクセスするために、ネットワークからのインターネット接続が依然として必要です。これらはすべて で有効 AWS のサービス になっていませんAWS PrivateLink。で使用される最上位ドメインのリストについては AWS マネジメントコンソール、「」を参照してくださいトラブルシューティング。

> **Note**
>
> 現在、 AWS マネジメントコンソール プライベートアクセス は、`status.aws.amazon.com`、、 などのエンドポイントをサポートしていませんhealth.aws.amazon.comdocs.aws.amazon.com。これらのドメインはパブリックインターネットにルーティングする必要があります。

必要な VPC エンドポイントと DNS 設定

AWS マネジメントコンソール プライベートアクセスには、リージョンごとに次の 2 つの VPC エンドポイントが必要です。*#####*を、自身のリージョン情報に置き換えます。

1. の com.amazonaws.*region*.console AWS マネジメントコンソール
2. の com.amazonaws.*region*.signin AWS サインイン

> **Note**
>
> インフラストラクチャとネットワーク接続は、 AWS マネジメントコンソールで使用する他のリージョンに関係なく、常に米国東部 (バージニア北部) (us-east-1) リージョンにプロビジョニングします。 AWS Transit Gateway を使用して、米国東部 (バージニア北部) と他のすべてのリージョンとの接続を設定できます。詳細については、「Amazon VPC Transit Gateway ガイド」の「トランジットゲートウェイの開始方法」を参照してください。Amazon VPC ピアリング接続を使用することもできます。詳細については、「Amazon VPC ピアリング接続ガイド」の「VPC ピア機能とは」を参照してください。これらのオプションを比較するには、「Amazon Virtual Private Cloud 接続オプションホワイトペーパー」の「Amazon VPC 間の接続オプション」を参照してください。

トピック

DNS AWS マネジメントコンソール および の設定 AWS サインイン

ネットワークトラフィックをそれぞれの VPC エンドポイントにルーティングするには、 AWS マネジメントコンソールにユーザーがアクセスする元のネットワーク内の DNS レコードを設定します。これらの DNS レコードにより、ユーザーのブラウザトラフィックは、作成した VPC エンドポイントに誘導されます。

1 つのホストゾーンを作成できます。ただし、VPC エンドポイントがないため、`health.aws.amazon.com` や `docs.aws.amazon.com` などのエンドポイントにはアクセスできません。これらのドメインはパブリックインターネットにルーティングする必要があります。リージョンごとに 2 つのプライベートホストゾーンを作成することをお勧めします。1 つは `signin.aws.amazon.com` 用、別の 1 つは `console.aws.amazon.com` 用で、以下の CNAME レコードを使用します。

- サインイン
  - *`region`*.signin.aws.amazon.com *`#####`*が目的のリージョンであるサインインDNSゾーンの AWS サインイン VPC エンドポイントを指す
  - signin.aws.amazon.com 米国東部 (バージニア北部) (us-east-1) の AWS サインイン VPC エンドポイントを指す

- コンソール
  - *region*.console.aws.amazon.com region が目的のリージョンであるコンソールDNSゾーンの AWS マネジメントコンソール VPC エンドポイントを指す
  - *.*region*.console.aws.amazon.com は、*#####*が目的のリージョンであるコンソールDNSゾーンの AWS マネジメントコンソール VPC エンドポイントを指します。
  - *.*region*.console.aws.amazon.com コンソールDNSゾーンの AWS マネジメントコンソール VPC エンドポイントを指す
  - 米国東部 (バージニア北部) リージョン専用のリージョンレス CNAME レコード。常に米国東部 (バージニア北部) リージョンを設定する必要があります。
    - signin.aws.amazon.com 米国東部 (バージニア北部) (us-east-1) の AWS サインイン VPC エンドポイントを指す
    - *.console.aws.amazon.com 米国東部 (バージニア北部) (us-east-1) の AWS マネジメントコンソール VPC エンドポイントを指す

  CNAME レコードを作成する手順については、「Amazon Route 53 デベロッパーガイド」の「レコードを使用する」を参照してください。

  Amazon S3 を含む一部の AWS コンソールでは、DNS名前に異なるパターンが使用されます。以下に 2 つの例を示します。

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

  このトラフィックを AWS マネジメントコンソール VPC エンドポイントに送信できるようにするには、これらの名前を個別に追加する必要があります。完全にプライベートなエクスペリエンスを実現するために、すべてのエンドポイントにルーティングを設定することをお勧めします。ただし、これは AWS マネジメントコンソール プライベートアクセスを使用するためには必要ありません。

  次のjsonファイルには、リージョンごとに設定する AWS のサービスとコンソールエンドポイントの完全なリストが含まれています。DNS の名前には、`com.amazonaws.`*region*`.console` エンドポイントの下の `PrivateIpv4DnsNames` フィールドを使用します。

  - https://configuration.private-access.console.amazonaws.com/us-east-1.config.json
  - https://configuration.private-access.console.amazonaws.com/us-east-2.config.json
  - https://configuration.private-access.console.amazonaws.com/us-west-2.config.json
  - https://configuration.private-access.console.amazonaws.com/ap-northeast-1.config.json

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

> **Note**
>
> このリストは、 AWS マネジメントコンソール プライベートアクセスの範囲にエンドポイントが追加されるたびに毎月更新されます。プライベートホストゾーンを最新の状態に保つには、前述のファイルリストを定期的に取得してください。

Route 53 を使用して DNS を設定する場合は、https://console.aws.amazon.com/route53/v2/hostedzones# にアクセスして DNS のセットアップを確認してください。Route 53 のプライベートホストゾーンごとに、次のレコードセットが存在することを確認します。

- console.aws.amazon.com
- signin.aws.amazon.com
- *.*region*.console.aws.amazon.com
- *region*.console.aws.amazon.com
- *.*region*.console.aws.amazon.com
- signin.aws.amazon.com
- *region*.signin.aws.amazon.com
- 前述の JSON ファイルにある追加レコード

の AWS サービスの VPC エンドポイントとDNS設定 AWS マネジメントコンソール

ウェブサーバーによってプロキシされる直接ブラウザリクエストとリクエストの組み合わせ AWS のサービス による AWS マネジメントコンソール 呼び出し。このトラフィックを AWS マネジメントコンソール VPC エンドポイントに送信するには、VPC エンドポイントを追加し、依存 AWS するサービスDNSごとに を設定する必要があります。

次のjsonファイルには、 AWS のサービス サポートされている AWS PrivateLink が一覧表示されています。サービスと が統合されていない場合 AWS PrivateLink、サービスはこれらのファイルに含まれません。

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

対応するサービスの VPC エンドポイントの [`ServiceName`] フィールドを使用して VPC に追加します。

> **Note**
>
> このリストは毎月更新され、 AWS マネジメントコンソール プライベートアクセスのサポートがより多くのサービスコンソールに追加されます。常に最新の状態に保つには、前述のファイルリストを定期的に取得し、VPC エンドポイントを更新してください。

サービスコントロールポリシーと VPC エンドポイントポリシーの実装

プライベートアクセスのサービスコントロールポリシー (SCPs) と VPC エンドポイントポリシー AWS マネジメントコンソール を使用して、VPC 内および接続されたオンプレミスネットワーク AWS マネジメントコンソール から を使用できるアカウントのセットを制限できます。

トピック

- AWS Organizations サービスコントロールポリシーでの AWS マネジメントコンソール プライベートアクセスの使用
- 予想されるアカウントと組織にのみ AWS マネジメントコンソール 使用を許可する (信頼できる ID)

AWS Organizations サービスコントロールポリシーでの AWS マネジメントコンソール プライベートアクセスの使用

AWS 組織が特定のサービスを許可するサービスコントロールポリシー (SCP) を使用している場合は、許可されたアクション`signin:*`に を追加する必要があります。このアクセス許可は、プライベートアクセス VPC エンドポイント AWS マネジメントコンソール 経由で にサインインすると、アクセス許可なしで SCP がブロックする IAM 認可が実行されるために必要です。例えば、次のサービスコントロールポリシーでは、 AWS マネジメントコンソール プライベートアクセスエンドポイントを使用してアクセスされたときなど、組織内で Amazon EC2 および CloudWatch サービスを使用することを許可します。

```
{
  "Effect": "Allow",
  "Action": [
    "signin:*",
    "ec2:*",
```

```
    "cloudwatch:*",
    ... Other services allowed
  },
  "Resource": "*"
}
```

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。

予想されるアカウントと組織にのみ AWS マネジメントコンソール 使用を許可する (信頼できる ID)

AWS マネジメントコンソール と は、サインインアカウントの ID を具体的に制御する VPC エンドポイントポリシー AWS サインイン をサポートします。

他の VPC エンドポイントポリシーとは異なり、このポリシーは認証前に評価されます。その結果、認証されたセッションのサインインと使用のみを具体的に制御し、セッションが実行する AWS サービス固有のアクションは制御しません。例えば、セッションが Amazon EC2 コンソールなどの AWS サービスコンソールにアクセスする場合、これらの VPC エンドポイントポリシーは、そのページを表示するために実行される Amazon EC2 アクションに対して評価されません。代わりに、サインインした IAM プリンシパルに関連付けられた IAM ポリシーを使用して、 AWS サービスアクションへのアクセス許可を制御できます。

> **Note**
>
> AWS マネジメントコンソール および SignIn VPC エンドポイントの VPC エンドポイントポリシーは、ポリシー策定の限定されたサブセットのみをサポートします。各 `Principal` と `Resource` は `*` に設定する必要があります。また、`Action` は `*` または `signin:*` のいずれかにする必要があります。VPC エンドポイントへのアクセスを制御するには、`aws:PrincipalOrgId` および `aws:PrincipalAccount` 条件キーを使用します。

以下のポリシーは、コンソールエンドポイントと SignIn VPC エンドポイントの両方に推奨されています。

この VPC エンドポイントポリシーは、指定された AWS 組織の AWS アカウント へのサインインを許可し、他のアカウントへのサインインをブロックします。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgId": "o-xxxxxxxxxxx"
        }
      }
    }
  ]
}
```

この VPC エンドポイントポリシーは、特定の のリストへのサインインを制限 AWS アカウント し、他のアカウントへのサインインをブロックします。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalAccount": [ "111122223333", "222233334444" ]
        }
      }
    }
  ]
}
```

AWS マネジメントコンソール およびサインイン VPC エンドポイントで AWS アカウント または 組織を制限するポリシーは、サインイン時に評価され、既存のセッションについて定期的に再評価されます。

アイデンティティベースのポリシーとその他のポリシータイプの実装

でアクセスを管理するには、ポリシー AWS を作成し、IAM ID (ユーザー、ユーザーのグループ、またはロール) または AWS リソースにアタッチします。このページでは、 AWS マネジメントコンソール プライベートアクセスと一緒に使用する場合のポリシーの仕組みについて説明します。

サポートされている AWS グローバル条件コンテキストキー

AWS マネジメントコンソール プライベートアクセスは、 `aws:SourceVpce`および `aws:VpcSourceIp` AWS グローバル条件コンテキストキーをサポートしていません。 AWS マネジメントコンソール のプライベートアクセスを使用する場合は、代わりに `aws:SourceVpc` IAM 条件をポリシーで使用できます。

aws:SourceVpc での AWS マネジメントコンソール プライベートアクセスの仕組み

このセクションでは、 によって生成されたリクエストが AWS マネジメントコンソール 実行できるさまざまなネットワークパスについて説明します AWS のサービス。一般的に、 AWS サービスコンソールは、ブラウザの直接リクエストと、 AWS マネジメントコンソール ウェブサーバーによってプロキシされるリクエストを組み合わせて実装されます AWS のサービス。これらの実装は、予告なしに変更される可能性があります。セキュリティ要件に VPC エンドポイント AWS のサービス を使用した へのアクセスが含まれている場合は、VPC から直接使用するか AWS マネジメントコンソール 、プライベートアクセスを介して使用するかにかかわらず、VPC エンドポイントを VPC から使用する予定のすべてのサービスに設定することをお勧めします。さらに、プライベートアクセス機能では、特定の`aws:SourceVpce`値ではなく、ポリシーで `aws:SourceVpc` IAM AWS マネジメントコンソール 条件を使用する必要があります。このセクションでは、さまざまなネットワークパスの仕組みについて詳しく説明します。

ユーザーが にサインインすると AWS マネジメントコンソール、ブラウザの直接リクエストと、AWS マネジメントコンソール ウェブサーバーから AWS サーバーにプロキシされるリクエスト AWS のサービス を組み合わせて、 にリクエストを行います。たとえば、CloudWatch グラフデータ

リクエストはブラウザから直接行われます。Amazon S3 などの一部の AWS サービスコンソールリクエストは、ウェブサーバーによって Amazon S3 にプロキシされます。 Amazon S3

直接ブラウザリクエストの場合、 AWS マネジメントコンソール プライベートアクセスを使用しても何も変更されません。以前と同様、リクエストは VPC が monitoring.region.amazonaws.com に到達するように設定したネットワークパスを通じてサービスに到達します。VPC が com.amazonaws.region.monitoring の VPC エンドポイントで設定されている場合、リクエストはその CloudWatch VPC エンドポイントを経由して CloudWatch に到達します。CloudWatch の VPC エンドポイントがない場合、リクエストは VPC のインターネットゲートウェイ経由で、パブリックエンドポイントの CloudWatch に到達します。CloudWatch VPC エンドポイントを経由して CloudWatch に到達するリクエストでは、IAM 条件 `aws:SourceVpc` と `aws:SourceVpce` がそれぞれの値に設定されます。パブリックエンドポイント経由で CloudWatch に到達するリクエストには、`aws:SourceIp` がリクエストのソース IP アドレスに設定されます。これらの IAM 条件キーの詳細については、「IAM ユーザーガイド」の「 グローバル条件コンテキストキー」を参照してください。

Amazon S3 コンソールにアクセスしたときに Amazon S3 コンソールがバケットを一覧表示するリクエストなど、 AWS マネジメントコンソール ウェブサーバーによってプロキシされるリクエストの場合Amazon S3、ネットワークパスは異なります。これらのリクエストは VPC から開始されないため、そのサービス用に VPC に設定した VPC エンドポイントを使用しません。この場合、Amazon S3 の VPC エンドポイントがあっても、バケットを一覧表示する Amazon S3 へのセッションのリクエストは Amazon S3 VPC エンドポイントを使用しません。ただし、サポートされているサービスで AWS マネジメントコンソール プライベートアクセスを使用する場合、これらのリクエスト (Amazon S3 へのリクエストなど) にはリクエストコンテキストに `aws:SourceVpc`条件キーが含まれます。`aws:SourceVpc` 条件キーは、サインインとコンソールの AWS マネジメントコンソール プライベートアクセスエンドポイントがデプロイされる VPC ID に設定されます。そのため、アイデンティティベースのポリシーで `aws:SourceVpc` 制限を使用している場合、 AWS マネジメントコンソール プライベートアクセスサインインとコンソールエンドポイントをホストしているこの VPC の VPC ID を追加する必要があります。`aws:SourceVpce` 条件は、それぞれのサインインまたはコンソール VPC エンドポイント ID に設定されます。

> **Note**
>
> ユーザーが AWS マネジメントコンソール のプライベートアクセスでサポートされていないサービスコンソールへのアクセスを必要とする場合は、ユーザーのアイデンティティベースのポリシーで `aws:SourceIP` 条件キーを使用し、必要なパブリックネットワークアドレス (オンプレミスのネットワーク範囲など) のリストを含める必要があります。

さまざまなネットワークパスが CloudTrail にどのように反映されるか

によって生成されたリクエストで使用されるさまざまなネットワークパス AWS マネジメントコンソール は、CloudTrail イベント履歴に反映されます。

直接ブラウザリクエストの場合、 AWS マネジメントコンソール プライベートアクセスを使用しても何も変更されません。CloudTrail イベントには、サービス API 呼び出しに使用された VPC エンドポイント ID など、接続に関する詳細が含まれます。

AWS マネジメントコンソール ウェブサーバーによってプロキシされるリクエストの場合、CloudTrail イベントには VPC 関連の詳細は含まれません。ただし、`AwsConsoleSignIn`イベントタイプなど、ブラウザセッションを確立 AWS サインイン するために必要な への初期リクエストには、イベントの詳細に AWS サインイン VPC エンドポイント ID が含まれます。

AWS マネジメントコンソール プライベートアクセスを試す

このセクションでは、新しいアカウントで AWS マネジメントコンソール プライベートアクセスをセットアップしてテストする方法について説明します。

AWS マネジメントコンソール プライベートアクセスは高度なセキュリティ機能であり、VPC VPCs ネットワークと設定に関する事前の知識が必要です。このトピックでは、本格的なインフラストラクチャなしで AWS マネジメントコンソール プライベートアクセスを試行する方法について説明します。

トピック

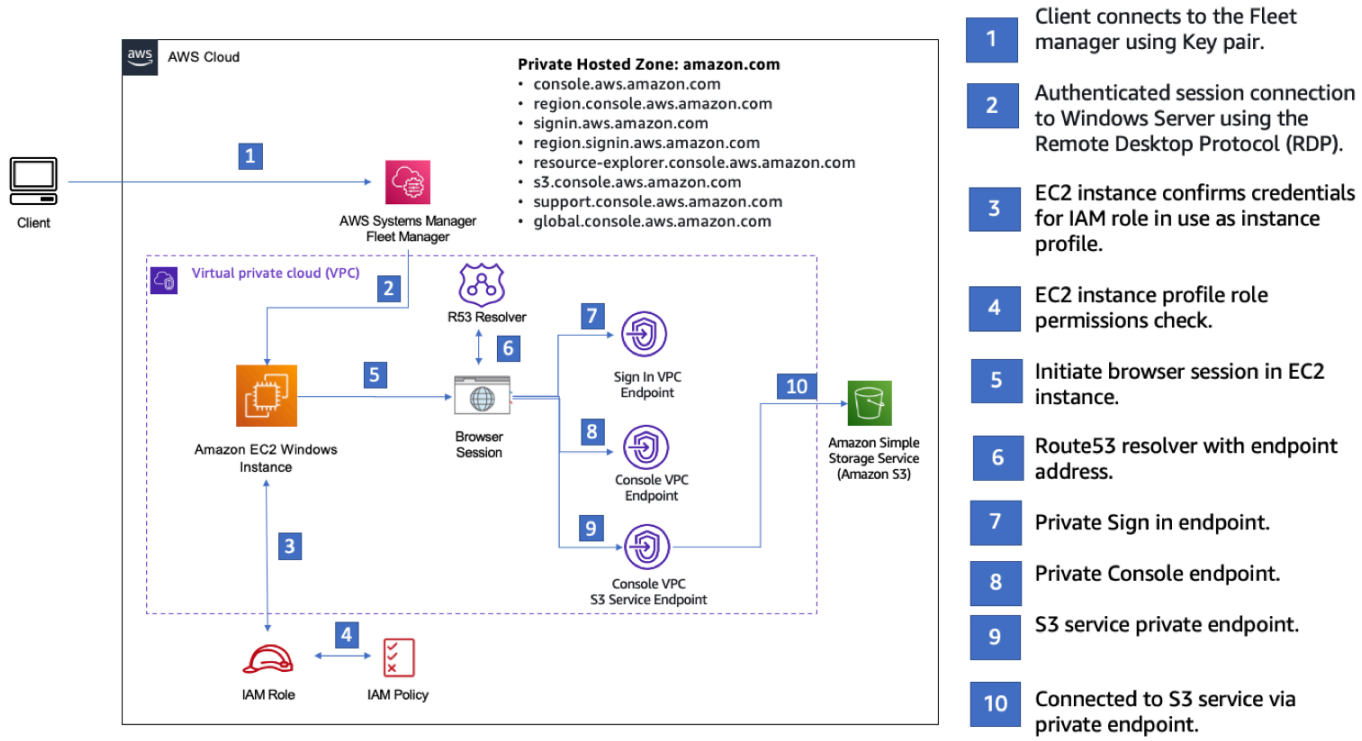
- Amazon EC2 でのテスト設定
- Amazon WorkSpaces でのテスト設定
- IAM ポリシーを使った VPC 設定のテスト

Amazon EC2 でのテスト設定

Amazon Elastic Compute Cloud (Amazon EC2) は、Amazon Web Service クラウドでスケーラブルなコンピューティングキャパシティーを提供します。Amazon EC2 を使用すると、必要な数 (またはそれ以下) の仮想サーバーの起動、セキュリティおよびネットワーキングの構成、ストレージの管理ができます。このセットアップでは、 AWS Systems Managerの一機能である Fleet Manager を使用して、リモートデスクトッププロトコル (RDP) を使って Amazon EC2 Windows インスタンスに接続できます。

このガイドでは、Amazon EC2 AWS マネジメントコンソール インスタンスから Amazon Simple Storage Service へのプライベートアクセス接続をセットアップして体験するためのテスト環境を示します。このチュートリアルでは CloudFormation 、 を使用して、この機能を視覚化するために Amazon EC2 が使用するネットワーク設定を作成および設定します。

次の図は、Amazon EC2 を使用して AWS マネジメントコンソール のプライベートアクセス設定にアクセスするためのワークフローを示しています。これは、ユーザーがプライベートエンドポイントを使用して Amazon S3 に接続する方法を示しています。



次の CloudFormation テンプレートをコピーし、「ネットワークをセットアップするには」のステップ 3 で使用するファイルに保存します。

> **Note**
>
> この CloudFormation テンプレートは、イスラエル (テルアビブ) リージョンで現在サポートされていない設定を使用します。

AWS マネジメントコンソール プライベートアクセス環境 Amazon EC2 CloudFormation template

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

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

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

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

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

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

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

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

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

  InstanceTypeParameter:
    Type: String
    Default: 't3.medium'


Resources:

#########################
# VPC AND SUBNETS
#########################

  AppVPC:
    Type: 'AWS::EC2::VPC'
    Properties:
      CidrBlock: !Ref VpcCIDR
      InstanceTenancy: default
      EnableDnsSupport: true
      EnableDnsHostnames: true

  PublicSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet1CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone:
        Fn::Select:
          - 0
          - Fn::GetAZs: ""

  PublicSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet2CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone:
        Fn::Select:
          - 1
          - Fn::GetAZs: ""
```

```
  PublicSubnetC:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet3CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone:
        Fn::Select:
          - 2
          - Fn::GetAZs: ""

  PrivateSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet1CIDR
      AvailabilityZone:
        Fn::Select:
          - 0
          - Fn::GetAZs: ""

  PrivateSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet2CIDR
      AvailabilityZone:
        Fn::Select:
          - 1
          - Fn::GetAZs: ""

  PrivateSubnetC:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet3CIDR
      AvailabilityZone:
        Fn::Select:
          - 2
          - Fn::GetAZs: ""

  InternetGateway:
    Type: AWS::EC2::InternetGateway
```

```
  InternetGatewayAttachment:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      InternetGatewayId: !Ref InternetGateway
      VpcId: !Ref AppVPC

  NatGatewayEIP:
    Type: AWS::EC2::EIP
    DependsOn: InternetGatewayAttachment

  NatGateway:
    Type: AWS::EC2::NatGateway
    Properties:
      AllocationId: !GetAtt NatGatewayEIP.AllocationId
      SubnetId: !Ref PublicSubnetA

#########################
# Route Tables
#########################

  PrivateRouteTable:
    Type: 'AWS::EC2::RouteTable'
    Properties:
      VpcId: !Ref AppVPC

  DefaultPrivateRoute:
    Type: AWS::EC2::Route
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      NatGatewayId: !Ref NatGateway

  PrivateSubnetRouteTableAssociation1:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetA

  PrivateSubnetRouteTableAssociation2:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetB
```

```
  PrivateSubnetRouteTableAssociation3:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetC

  PublicRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref AppVPC

  DefaultPublicRoute:
    Type: AWS::EC2::Route
    DependsOn: InternetGatewayAttachment
    Properties:
      RouteTableId: !Ref PublicRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      GatewayId: !Ref InternetGateway

  PublicSubnetARouteTableAssociation1:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetA

  PublicSubnetBRouteTableAssociation2:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetB

  PublicSubnetBRouteTableAssociation3:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetC


##########################
# SECURITY GROUPS
##########################

  VPCEndpointSecurityGroup:
```

```
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: Allow TLS for VPC Endpoint
      VpcId: !Ref AppVPC
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 443
          ToPort: 443
          CidrIp: !GetAtt AppVPC.CidrBlock

  EC2SecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: Default EC2 Instance SG
      VpcId: !Ref AppVPC

#########################
# VPC ENDPOINTS
#########################

  VPCEndpointGatewayS3:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.s3'
      VpcEndpointType: Gateway
      VpcId: !Ref AppVPC
      RouteTableIds:
        - !Ref PrivateRouteTable

  VPCEndpointInterfaceSSM:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ssm'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceEc2messages:
    Type: 'AWS::EC2::VPCEndpoint'
```

```
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ec2messages'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceSsmmessages:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ssmmessages'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceSignin:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.signin'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceConsole:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
```

```
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.console'
      VpcId: !Ref AppVPC

#########################
# ROUTE53 RESOURCES
#########################

  ConsoleHostedZone:
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Console VPC Endpoint Hosted Zone'
      Name: 'console.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  ConsoleRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  GlobalConsoleRecord:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'global.console.aws.amazon.com'
      AliasTarget:
```

```
       DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 ConsoleS3ProxyRecordGlobal:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
     Name: 's3.console.aws.amazon.com'
     AliasTarget:
       DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 ConsoleSupportProxyRecordGlobal:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
     Name: "support.console.aws.amazon.com"
     AliasTarget:
       DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 ExplorerProxyRecordGlobal:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
     Name: "resource-explorer.console.aws.amazon.com"
     AliasTarget:
       DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 WidgetProxyRecord:
   Type: AWS::Route53::RecordSet
```

```
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: "*.widget.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ["1", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],],]
        HostedZoneId: !Select ["0", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],],]
      Type: A

  ConsoleRecordRegional:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: !Sub "${AWS::Region}.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleRecordRegionalMultiSession:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: !Sub "*.${AWS::Region}.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  SigninHostedZone:
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Signin VPC Endpoint Hosted Zone'
      Name: 'signin.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"
```

```
  SigninRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: 'signin.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

  SigninRecordRegional:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: !Sub "${AWS::Region}.signin.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

##########################
# EC2 INSTANCE
##########################

  Ec2InstanceRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          -
            Effect: Allow
            Principal:
              Service:
                - ec2.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
      ManagedPolicyArns:
```

```
        - arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore

  Ec2InstanceProfile:
    Type: AWS::IAM::InstanceProfile
    Properties:
      Path: /
      Roles:
       - !Ref Ec2InstanceRole

  EC2WinInstance:
    Type: 'AWS::EC2::Instance'
    Properties:
      ImageId: !Ref LatestWindowsAmiId
      IamInstanceProfile: !Ref Ec2InstanceProfile
      KeyName: !Ref Ec2KeyPair
      InstanceType:
        Ref: InstanceTypeParameter
      SubnetId: !Ref PrivateSubnetA
      SecurityGroupIds:
        - Ref: EC2SecurityGroup
      BlockDeviceMappings:
        - DeviceName: /dev/sda1
          Ebs:
            VolumeSize: 50
      Tags:
      - Key: "Name"
        Value: "Console VPCE test instance"
```

ネットワークを設定するには

1. 組織の管理アカウントにサインインして、CloudFormation コンソールを開きます。
2. [スタックの作成] を選択してください。
3. [With new resources (standard)] (新しいリソースの使用 (標準)) を選択します。以前に作成した CloudFormation テンプレートファイルをアップロードし、次へを選択します。
4. **PrivateConsoleNetworkForS3** などスタックの名前を入力し、[次へ] を選択します。
5. VPC とサブネットの場合、希望する IP CIDR 範囲を入力するか、指定されたデフォルト値を使用してください。デフォルト値を使用する場合は、 内の既存の VPC リソースと重複していないことを確認します AWS アカウント。

6. EC2KeyPair パラメータには、アカウント内の既存の Amazon EC2 キーペアから 1 つ選択します。既存の Amazon EC2 キーペアがない場合は、次のステップに進む前に作成する必要があります。詳細については、「Amazon EC2 ユーザーガイド」の「Amazon EC2 を使用したキーペアの作成」を参照してください。
7. [スタックの作成] を選択してください。
8. スタックが作成されたら、[リソース] タブを選択して、作成されたリソースを表示します。

Amazon EC2 インスタンスに接続するには

1. 組織の管理アカウントにサインインして、[Amazon EC2 コンソール] を開きます。
2. ナビゲーションペインで、[インスタンス] を選択してください。
3. インスタンスページで、 CloudFormation テンプレートによって作成されたコンソール VPCE テストインスタンスを選択します。次に、[接続] を選択します。

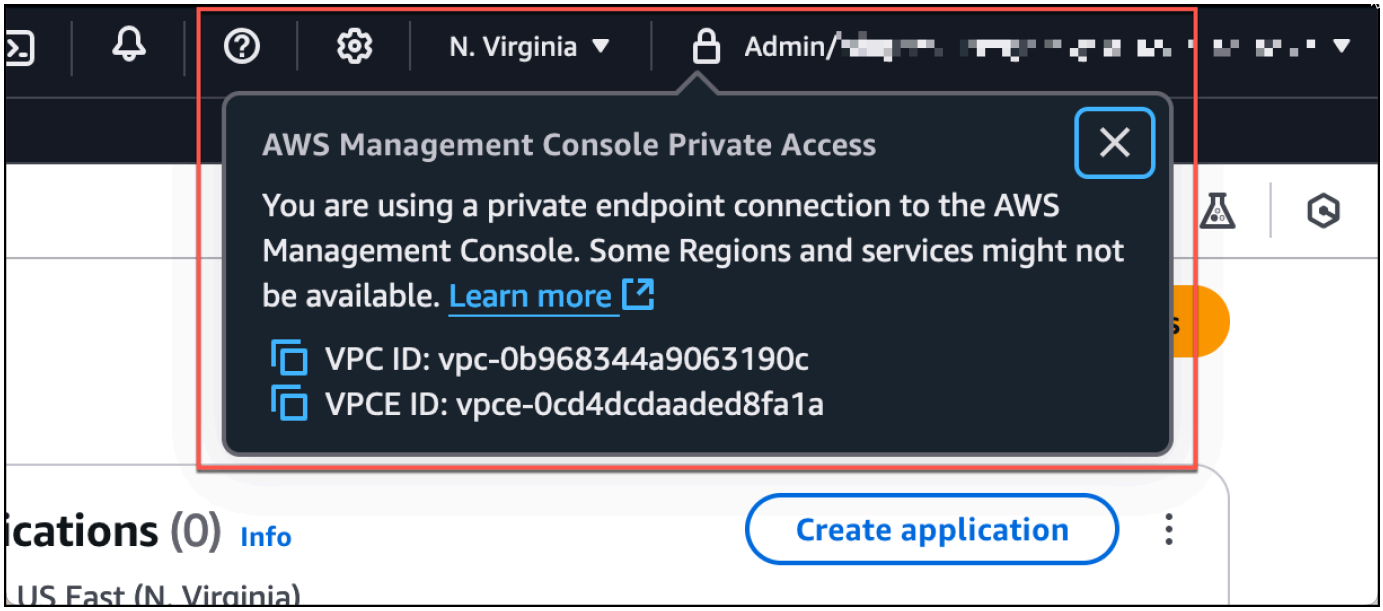
> **Note**
>
> この例では、 の一機能である Fleet Manager AWS Systems Manager Explorerを使用して Windows Server に接続します。接続を開始するまでに数分かかることがあります。

4. [インスタンスに接続] ページで、[RDP クライアント]、[Fleet Manager を使用して接続] の順に選択します。
5. [Fleet Manager リモートデスクトップ] を選択します。
6. Amazon EC2 インスタンスの管理パスワードを取得し、ウェブインターフェイスを使用して Windows Desktop にアクセスするには、 CloudFormation テンプレートの作成時に使用した Amazon EC2 キーペアに関連付けられたプライベートキーを使用します。
7. Amazon EC2 Windows インスタンスから、ブラウザ AWS マネジメントコンソール で を開きます。
8. AWS 認証情報を使用してサインインしたら、Amazon S3 コンソールを開き、プライベートアクセスを使用して AWS マネジメントコンソール 接続されていることを確認します。

AWS マネジメントコンソール プライベートアクセスの設定をテストするには

1. 組織の管理アカウントにサインインして、[Amazon S3 コンソール] を開きます。

2. ナビゲーションバーのロックプライベートアイコンを選択すると、使用中の VPC エンドポイントが表示されます。次のスクリーンショットは、ロックプライベートアイコンの場所と VPC 情報を示しています。



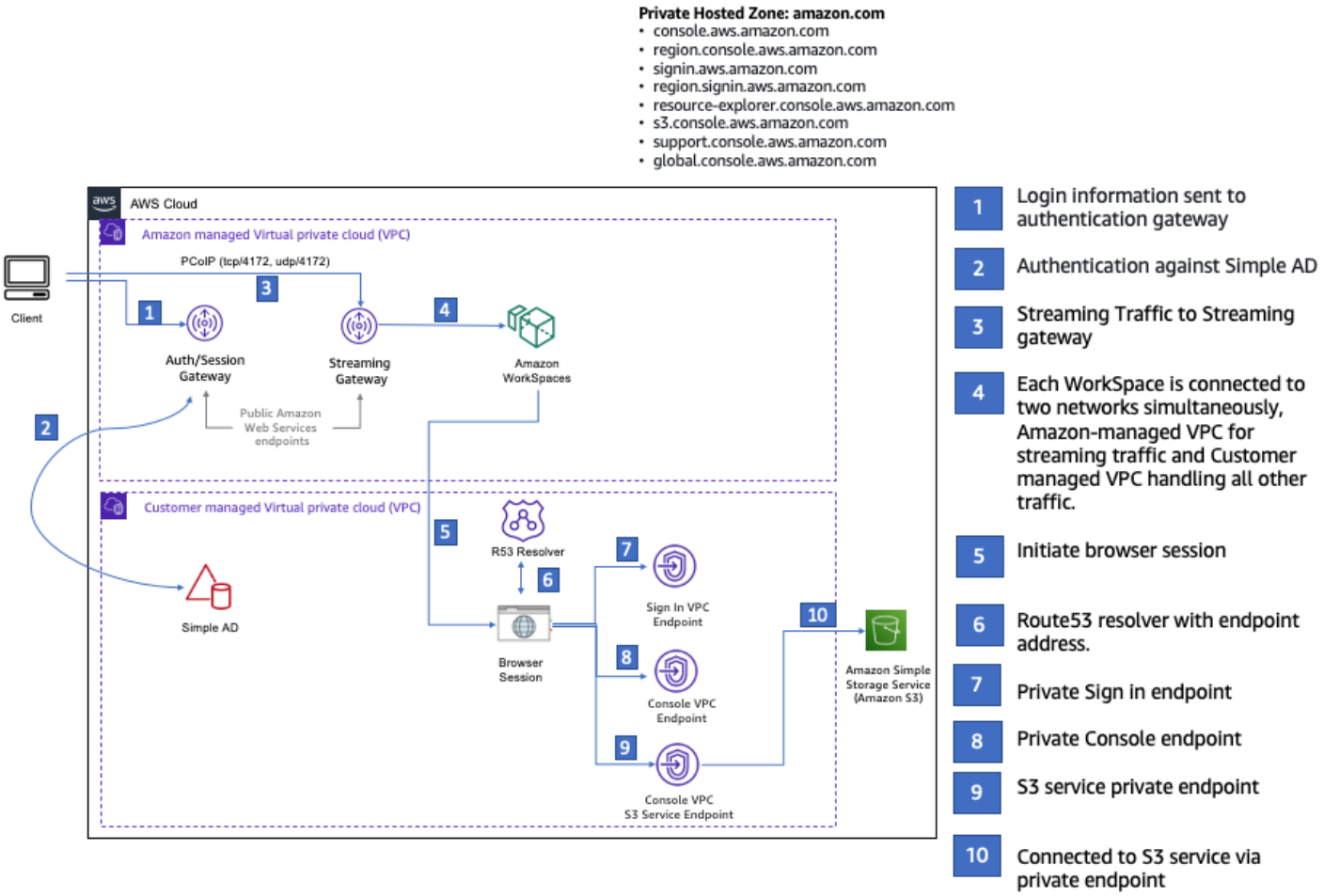
Amazon WorkSpaces でのテスト設定

Amazon WorkSpaces を使用すると、Microsoft Windows、Amazon Linux、または Ubuntu Linux をユーザー用のクラウドベースの仮想デスクトップ (WorkSpaces と呼ばれます) として プロビジョニングできます。必要に応じてユーザーをすばやく追加または削除できます。ユーザーは、複数のデバイスまたはウェブブラウザから仮想デスクトップにアクセスできます。WorkSpaces の詳細については、「Amazon WorkSpaces 管理ガイド」を参照してください。

このセクションの例では、ユーザー環境が WorkSpace で実行されているウェブブラウザを使用して AWS マネジメントコンソール プライベートアクセスにサインインするテスト環境について説明します。次に、ユーザーは Amazon Simple Storage Service コンソールにアクセスします。この WorkSpace は、VPC 接続ネットワーク上のラップトップを使用して、ブラウザ AWS マネジメントコンソール から にアクセスする企業ユーザーのエクスペリエンスをシミュレートすることを目的としています。

このチュートリアルでは AWS CloudFormation 、 を使用してネットワーク設定と WorkSpaces で使用する Simple Active Directory を作成および設定し、 を使用して WorkSpace をセットアップする手順を示します AWS マネジメントコンソール。

次の図は、WorkSpace を使用して AWS マネジメントコンソール プライベートアクセス設定をテストするためのワークフローを示しています。クライアントの WorkSpace、Amazon が管理する VPC、および顧客が管理する VPC の関係を示しています。



次の CloudFormation テンプレートをコピーし、ネットワークをセットアップする手順のステップ 3 で使用するファイルに保存します。

AWS マネジメントコンソール プライベートアクセス環境 CloudFormation テンプレート

```
Description: |
  AWS Management Console Private Access.
Parameters:

  VpcCIDR:
    Type: String
    Default: 172.16.0.0/16
    Description: CIDR range for VPC
```

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

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

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

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

  DSAdminPasswordResourceName:
    Type: String
    Default: ADAdminSecret
    Description: Password for directory services admin

# Amazon WorkSpaces is available in a subset of the Availability Zones for each
 supported Region.
# https://docs.aws.amazon.com/workspaces/latest/adminguide/azs-workspaces.html
Mappings:
  RegionMap:
    us-east-1:
      az1: use1-az2
      az2: use1-az4
      az3: use1-az6
    us-west-2:
      az1: usw2-az1
      az2: usw2-az2
      az3: usw2-az3
    ap-south-1:
      az1: aps1-az1
      az2: aps1-az2
      az3: aps1-az3
    ap-northeast-2:
```

```
      az1: apne2-az1
      az2: apne2-az3
    ap-southeast-1:
      az1: apse1-az1
      az2: apse1-az2
    ap-southeast-2:
      az1: apse2-az1
      az2: apse2-az3
    ap-northeast-1:
      az1: apne1-az1
      az2: apne1-az4
    ca-central-1:
      az1: cac1-az1
      az2: cac1-az2
    eu-central-1:
      az1: euc1-az2
      az2: euc1-az3
    eu-west-1:
      az1: euw1-az1
      az2: euw1-az2
    eu-west-2:
      az1: euw2-az2
      az2: euw2-az3
    sa-east-1:
      az1: sae1-az1
      az2: sae1-az3

Resources:

  iamLambdaExecutionRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service:
              - lambda.amazonaws.com
            Action:
              - 'sts:AssumeRole'
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole
      Policies:
```

```
        - PolicyName: describe-ec2-az
          PolicyDocument:
            Version: "2012-10-17"
            Statement:
              - Effect: Allow
                Action:
                  - 'ec2:DescribeAvailabilityZones'
                Resource: '*'
      MaxSessionDuration: 3600
      Path: /service-role/

  fnZoneIdtoZoneName:
    Type: AWS::Lambda::Function
    Properties:
      Runtime: python3.8
      Handler: index.lambda_handler
      Code:
        ZipFile: |
          import boto3
          import cfnresponse

          def zoneId_to_zoneName(event, context):
              responseData = {}
              ec2 = boto3.client('ec2')
              describe_az = ec2.describe_availability_zones()
              for az in describe_az['AvailabilityZones']:
                  if event['ResourceProperties']['ZoneId'] == az['ZoneId']:
                      responseData['ZoneName'] = az['ZoneName']
                      cfnresponse.send(event, context, cfnresponse.SUCCESS,
responseData, str(az['ZoneId']))

          def no_op(event, context):
              print(event)
              responseData = {}
              cfnresponse.send(event, context, cfnresponse.SUCCESS, responseData,
str(event['RequestId']))

          def lambda_handler(event, context):
              if event['RequestType'] == ('Create' or 'Update'):
                  zoneId_to_zoneName(event, context)
              else:
                  no_op(event,context)
      Role: !GetAtt iamLambdaExecutionRole.Arn
```

```
  getAZ1:
    Type: "Custom::zone-id-zone-name"
    Properties:
      ServiceToken: !GetAtt fnZoneIdtoZoneName.Arn
      ZoneId: !FindInMap [ RegionMap, !Ref 'AWS::Region', az1 ]
  getAZ2:
    Type: "Custom::zone-id-zone-name"
    Properties:
      ServiceToken: !GetAtt fnZoneIdtoZoneName.Arn
      ZoneId: !FindInMap [ RegionMap, !Ref 'AWS::Region', az2 ]

#########################
# VPC AND SUBNETS
#########################

  AppVPC:
    Type: 'AWS::EC2::VPC'
    Properties:
      CidrBlock: !Ref VpcCIDR
      InstanceTenancy: default
      EnableDnsSupport: true
      EnableDnsHostnames: true

  PublicSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet1CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone: !GetAtt getAZ1.ZoneName

  PublicSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet2CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone: !GetAtt getAZ2.ZoneName

  PrivateSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet1CIDR
```

```
      AvailabilityZone: !GetAtt getAZ1.ZoneName

  PrivateSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet2CIDR
      AvailabilityZone: !GetAtt getAZ2.ZoneName

  InternetGateway:
    Type: AWS::EC2::InternetGateway

  InternetGatewayAttachment:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      InternetGatewayId: !Ref InternetGateway
      VpcId: !Ref AppVPC

  NatGatewayEIP:
    Type: AWS::EC2::EIP
    DependsOn: InternetGatewayAttachment

  NatGateway:
    Type: AWS::EC2::NatGateway
    Properties:
      AllocationId: !GetAtt NatGatewayEIP.AllocationId
      SubnetId: !Ref PublicSubnetA

#########################
# Route Tables
#########################

  PrivateRouteTable:
    Type: 'AWS::EC2::RouteTable'
    Properties:
      VpcId: !Ref AppVPC

  DefaultPrivateRoute:
    Type: AWS::EC2::Route
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      NatGatewayId: !Ref NatGateway
```

```
  PrivateSubnetRouteTableAssociation1:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetA

  PrivateSubnetRouteTableAssociation2:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetB

  PublicRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref AppVPC

  DefaultPublicRoute:
    Type: AWS::EC2::Route
    DependsOn: InternetGatewayAttachment
    Properties:
      RouteTableId: !Ref PublicRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      GatewayId: !Ref InternetGateway

  PublicSubnetARouteTableAssociation1:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetA

  PublicSubnetBRouteTableAssociation2:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetB


##########################
# SECURITY GROUPS
##########################

  VPCEndpointSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
```

```
    Properties:
      GroupDescription: Allow TLS for VPC Endpoint
      VpcId: !Ref AppVPC
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 443
          ToPort: 443
          CidrIp: !GetAtt AppVPC.CidrBlock

########################
# VPC ENDPOINTS
########################

  VPCEndpointGatewayS3:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.s3'
      VpcEndpointType: Gateway
      VpcId: !Ref AppVPC
      RouteTableIds:
        - !Ref PrivateRouteTable

  VPCEndpointInterfaceSignin:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.signin'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceConsole:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
      SecurityGroupIds:
```

```
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.console'
      VpcId: !Ref AppVPC

#########################
# ROUTE53 RESOURCES
#########################

  ConsoleHostedZone:
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Console VPC Endpoint Hosted Zone'
      Name: 'console.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  ConsoleRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  GlobalConsoleRecord:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'global.console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleS3ProxyRecordGlobal:
```

```
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 's3.console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleSupportProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: "support.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ExplorerProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: "resource-explorer.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  WidgetProxyRecord:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref "ConsoleHostedZone"
      Name: "*.widget.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ["1", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],],]
```

```
        HostedZoneId: !Select ["0", !Split [":", !Select ["0", !GetAtt
VPCEndpointInterfaceConsole.DnsEntries],],]
      Type: A

  ConsoleRecordRegional:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: !Sub "${AWS::Region}.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleRecordRegionalMultiSession:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: !Sub "*.${AWS::Region}.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  SigninHostedZone:
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Signin VPC Endpoint Hosted Zone'
      Name: 'signin.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  SigninRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: 'signin.aws.amazon.com'
```

```
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

  SigninRecordRegional:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: !Sub "${AWS::Region}.signin.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

#########################
# WORKSPACE RESOURCES
#########################
  ADAdminSecret:
    Type: AWS::SecretsManager::Secret
    Properties:
      Name: !Ref DSAdminPasswordResourceName
      Description: "Password for directory services admin"
      GenerateSecretString:
        SecretStringTemplate: '{"username": "Admin"}'
        GenerateStringKey: password
        PasswordLength: 30
        ExcludeCharacters: '"@/\'

  WorkspaceSimpleDirectory:
    Type: AWS::DirectoryService::SimpleAD
    DependsOn: AppVPC
    Properties:
      Name: "corp.awsconsole.com"
      Password: '{{resolve:secretsmanager:ADAdminSecret:SecretString:password}}'
      Size: "Small"
      VpcSettings:
        SubnetIds:
          - Ref: PrivateSubnetA
          - Ref: PrivateSubnetB
```

```
        VpcId:
          Ref: AppVPC


Outputs:
  PrivateSubnetA:
    Description: Private Subnet A
    Value: !Ref PrivateSubnetA

  PrivateSubnetB:
    Description: Private Subnet B
    Value: !Ref PrivateSubnetB

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

  WorkspacesAdminPassword:
    Description : "The ARN of the Workspaces admin's password.  Navigate to the Secrets
 Manager in the AWS Console to view the value."
    Value: !Ref ADAdminSecret
```

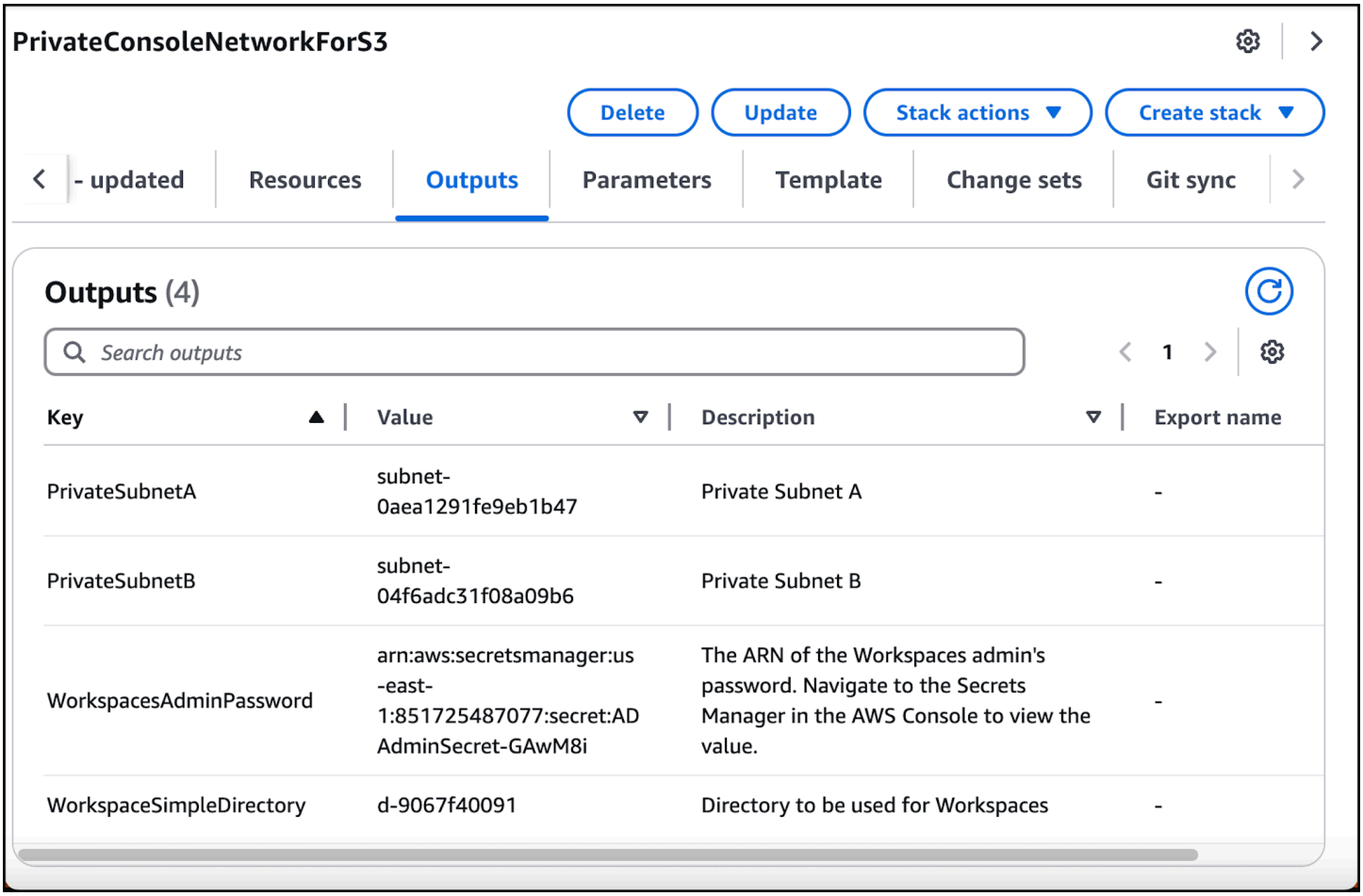
> **Note**
>
> このテスト設定は、米国東部 (バージニア北部) (us-east-1) リージョンで実行するように設計されています。

ネットワークを設定するには

1. 組織の管理アカウントにサインインして、CloudFormation コンソールを開きます。
2. [スタックの作成] を選択してください。
3. [With new resources (standard)] (新しいリソースの使用 (標準)) を選択します。以前に作成した CloudFormation テンプレートファイルをアップロードし、次へを選択します。
4. **PrivateConsoleNetworkForS3** などスタックの名前を入力し、[次へ] を選択します。
5. VPC とサブネットの場合、希望する IP CIDR 範囲を入力するか、指定されたデフォルト値を使用してください。デフォルト値を使用する場合は、 内の既存の VPC リソースと重複していないことを確認します AWS アカウント。
6. [スタックの作成] を選択してください。

7. スタックが作成されたら、[リソース] タブを選択して、作成されたリソースを表示します。
8. [出力] タブを選択すると、プライベートサブネットと Workspace Simple Directory の値が表示されます。これらの値は、次に示す WorkSpace の作成および設定手順のステップ 4 で使用するため、書き留めておいてください。

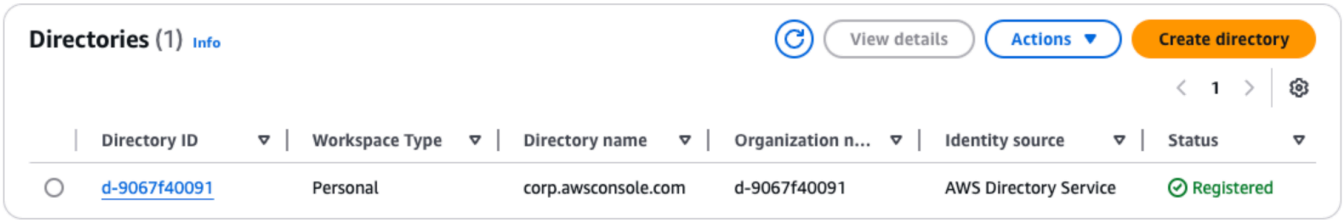
次のスクリーンショットは、プライベートサブネットと Workspace Simple Directory の値が表示された [出力] タブのビューを示しています。



ネットワークが作成できたので、以下の手順に従って WorkSpace を作成してアクセスします。

WorkSpace を作成するには

1. [WorkSpaces コンソール] を開きます。
2. ナビゲーションペインで [ディレクトリ] を選択します。
3. [ディレクトリ] ページで、ディレクトリのステータスが [アクティブ] であることを確認します。次のスクリーンショットは、アクティブディレクトリを含む [ディレクトリ] ページを示しています。



4. WorkSpaces のディレクトリを使用するには、そのディレクトリを登録する必要があります。ナビゲーションペインで [WorkSpaces] を選択し、[WorkSpaces の作成] を選択します。
5. [ディレクトリを選択] で、前の手順で CloudFormation が作成したディレクトリを選択します。[アクション] メニューで、[登録] を選択します。
6. サブネット選択については、前の手順のステップ 9 で説明した 2 つのプライベートサブネットを選択します。
7. [セルフサービス許可を有効化] を選択し、[登録] を選択します。
8. ディレクトリを登録したら、WorkSpace の作成を続行します。登録したディレクトリを選択し、[次へ] を選択します。
9. [ユーザーの作成] ページで、[追加ユーザーの作成] を選択します。名前とE メールアドレスを入力して、WorkSpace を使用できるようにします。WorkSpace のログイン情報がこの E メールアドレスに送信されるときに、E メールアドレスが有効であることを確認します。
10. [次へ] をクリックします。
11. [ユーザーの識別] ページで、手順 9 で作成したユーザーを選択し、[次へ] を選択します。
12. [バンドルの選択] ページで、[Amazon Linux 2 のスタンダード]、[次へ] の順に選択します。
13. 実行モードとユーザーカスタマイズにデフォルト設定を使用し、次に [ワークスペースを作成] を選択します。WorkSpace のステータスは `Pending` で始まり、約 20 分以内に `Available` ステータスに移行します。
14. WorkSpace が利用可能になると、手順 9 で指定した E メールアドレスに WorkSpace へのアクセス方法が記載されたメールが届きます。

WorkSpace にサインインした後、 AWS マネジメントコンソール プライベートアクセスを使用してアクセスしていることをテストできます。

WorkSpace にアクセスするには

1. 前の手順のステップ 14 で受信した E メールを開きます。

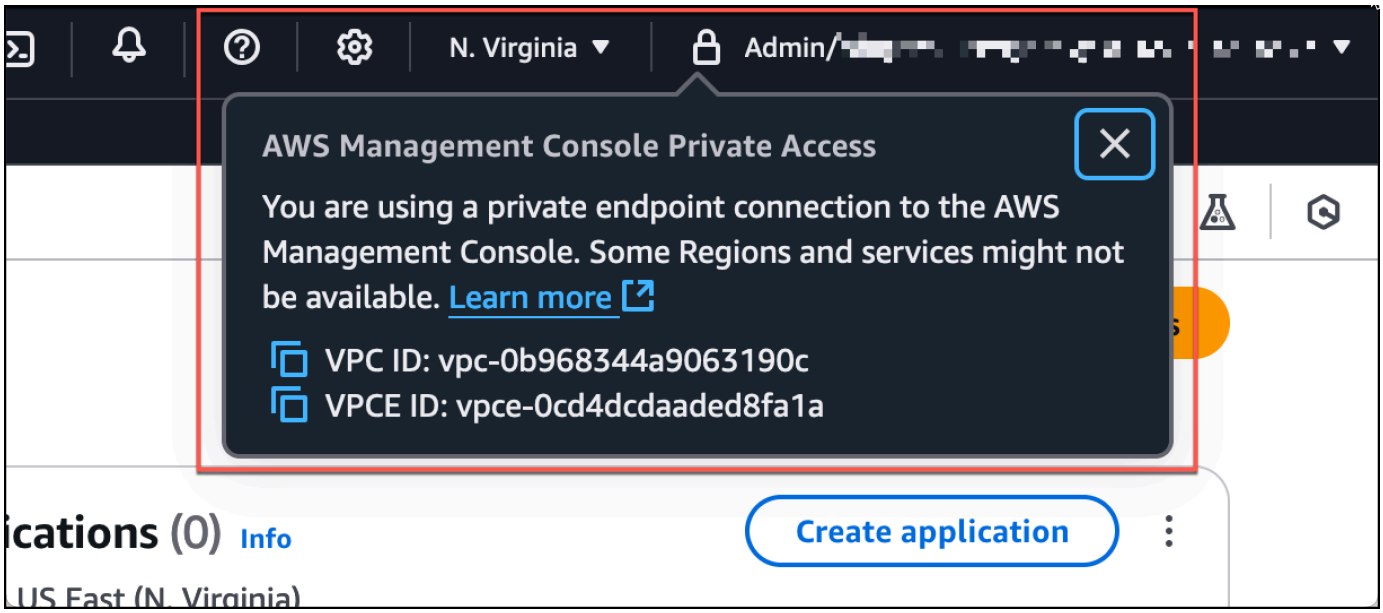
2. E メールに記載されている固有のリンクを選択してプロファイルを設定し、WorkSpaces クライアントをダウンロードします。
3. パスワードを設定します。
4. 任意のクライアントをダウンロードします。
5. クライアントをインストールして起動します。E メールに記載されている登録コードを入力して、[登録] を選択します。
6. ステップ 3 で作成した認証情報を使用して Amazon WorkSpaces にサインインします。

AWS マネジメントコンソール プライベートアクセスの設定をテストするには

1. WorkSpace からブラウザを開きます。次に、AWS マネジメントコンソールに移動し、認証情報を使用してサインインします。

> **Note**
>
> Firefox をブラウザとして使用している場合は、ブラウザの設定で [DNS over HTTPS を有効にする] オプションがオフになっていることを確認してください。

2. プライベートアクセスを使用して接続していることを確認できる Amazon S3 コンソールを開きます。 AWS マネジメントコンソール
3. ナビゲーションバーのロックプライベートアイコンを選択すると、使用中の VPC と VPC エンドポイントが表示されます。次のスクリーンショットは、ロックプライベートアイコンの場所と VPC 情報を示しています。



IAM ポリシーを使った VPC 設定のテスト

アクセスを制限する IAM ポリシーをデプロイすることにより、Amazon EC2 または WorkSpaces で設定した VPC に対してさらにテストを実施できます。

指定された VPC を使用していない限り、次のポリシーは Amazon S3 へのアクセスを拒否します。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "S3:*",
            "Resource": "*",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "aws:SourceVpc": "vpc-12345678"
                },
                "Bool": {
                    "aws:ViaAwsService": "false"
                }
            }
        }
    ]
}
```

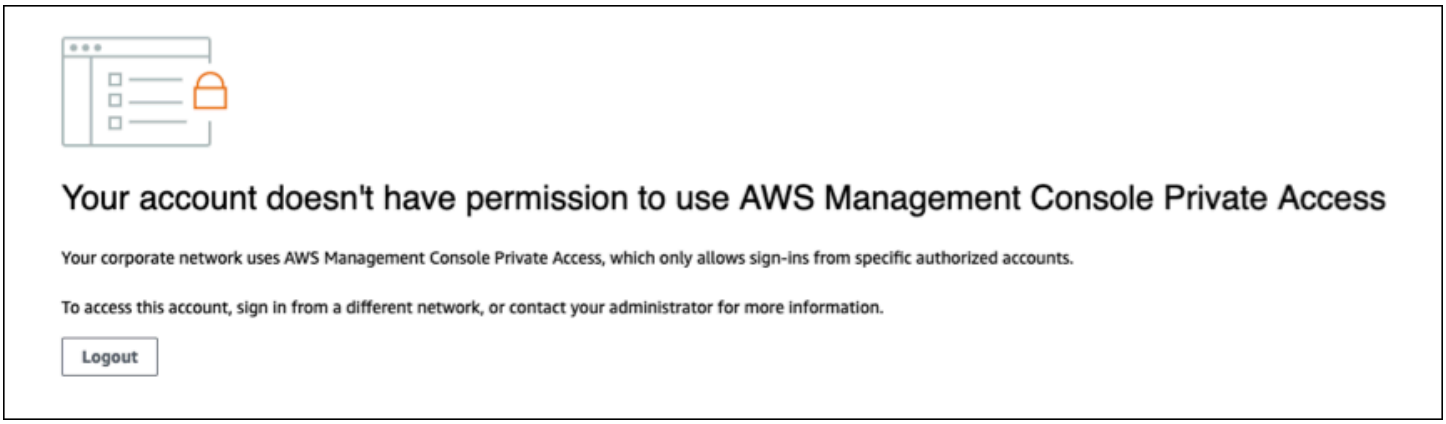
次のポリシーは、サインインエンドポイントのプライベートアクセスポリシーを使用して、 AWS マネジメントコンソール selected AWS アカウント IDs へのサインインを制限します。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
```

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalAccount": [
                        "AWSAccountID"
                    ]
                }
            }
        }
    ]
}
```

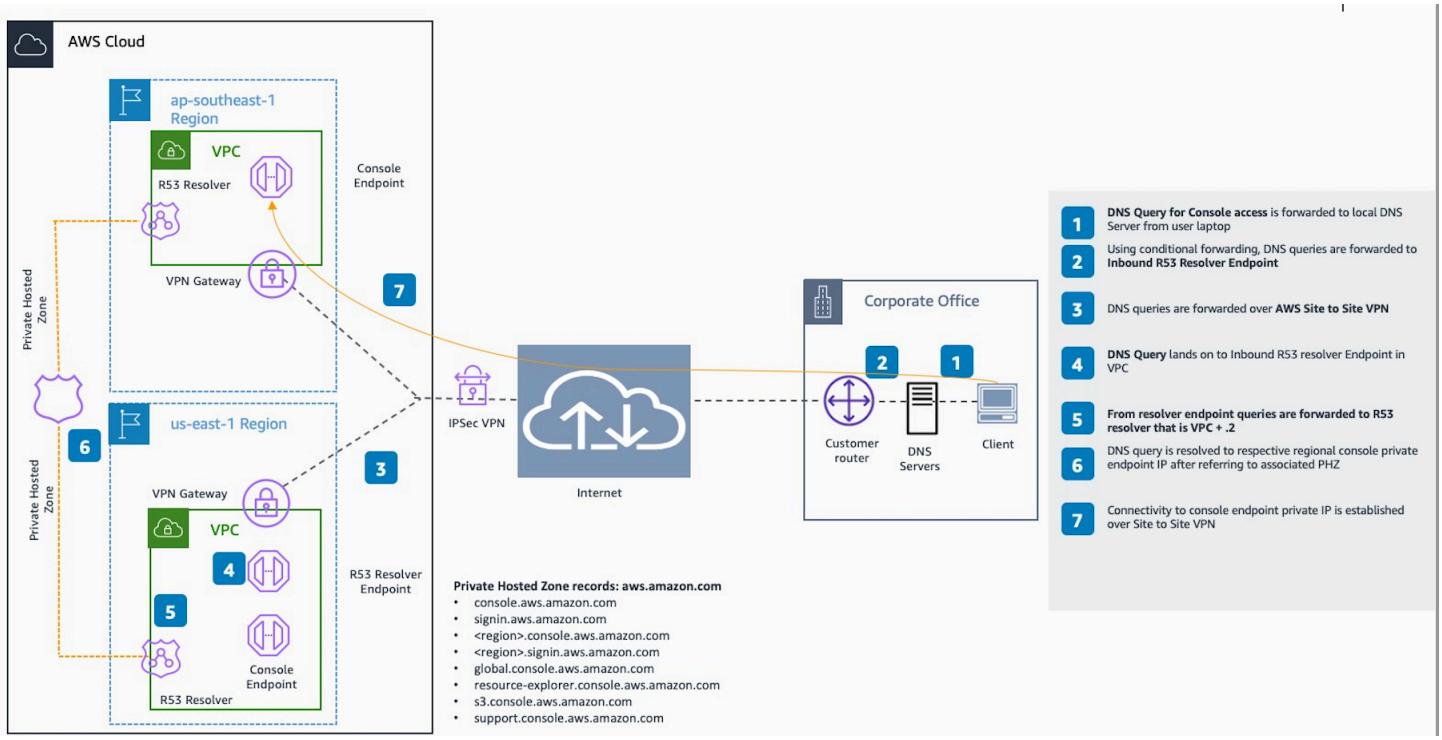
自分のアカウント以外の ID で接続すると、次のエラーページが表示されます。



リファレンスアーキテクチャ

オンプレミスネットワークから AWS マネジメントコンソール プライベートアクセスにプライベートに接続するには、 AWS Site-to-Site VPN から AWS Virtual Private Gateway (VGW) への接続オプションを利用できます。 AWS Site-to-Site VPN は、接続を作成し、接続を介してトラフィックを渡すようにルーティングを設定することで、VPC からリモートネットワークへのアクセスを有効にします。詳細については、AWS Site-to-Site VPN AWS ユーザーガイド」の「What isSite-to-Site VPN」を参照してください。 AWS 仮想プライベートゲートウェイ (VGW) は、VPC とオンプレミスネットワーク間のゲートウェイとして機能する高可用性のリージョンサービスです。

AWS Site-to-Site VPN AWS Virtual Private Gateway (VGW) への



このリファレンスアーキテクチャ設計の重要なコンポーネントは、 Amazon Route 53 Resolver、特にインバウンドリゾルバーです。プライベートアクセスエンドポイントが作成される VPC AWS マネジメントコンソール で設定すると、リゾルバーエンドポイント (ネットワークインターフェイス) が指定されたサブネットに作成されます。その後、その IP アドレスをオンプレミスの DNS サーバー上の条件付きフォワーダーで参照して、プライベートホストゾーンのレコードをクエリできます。オンプレミスクライアントが に接続すると AWS マネジメントコンソール、 AWS マネジメントコンソール プライベートアクセスエンドポイントのプライベート IPs。

AWS マネジメントコンソール プライベートアクセスエンドポイントへの接続を設定する前に、 にアクセスするすべてのリージョンと米国東部 (バージニア北部) リージョンで AWS マネジメントコンソール プライベートアクセスエンドポイントを設定し AWS マネジメントコンソール、プライベートホストゾーンを設定する前提条件のステップを完了します。

AWS ユーザーエクスペリエンスのカスタマイズ (UXC)

AWS ユーザーエクスペリエンスのカスタマイズにより、特定のニーズに合わせて AWS インターフェイスをカスタマイズし、効率を向上させることができます。UXC は現在、アカウント管理者向けにアカウントの色カスタマイズ機能を提供しています。この機能を使用すると、管理者は必要なグループ化に応じてアカウントの色を設定できます。たとえば、管理者はすべての本番稼働用アカウントに赤を、すべてのテストアカウントに黄色を、すべてのデベロッパーアカウントに緑を割り当てることができます。アカウントの色をカスタマイズする利点は次のとおりです。

- アカウントタイプを視覚的にすばやく識別する
- 間違ったアカウントへの変更のリスクを低減
- 類似アカウントをグループ化する (本番、テスト、開発)

ユーザーエクスペリエンスのカスタマイズへのアクセス

AWS マネジメントコンソールのアカウントページから UXC にアクセスできます。このページへのアクセスの詳細については、「???」を参照してください。

AWS ユーザーエクスペリエンスのカスタマイズの開始方法

管理者は、異なる AWS アカウントの色を設定できます。アカウントの色を使用すると、現在サインインしているアカウントを簡単に区別できます。組織はアカウントの色を使用して、異なるタイプのアカウントを区別できます。たとえば、開発アカウントには緑、テストアカウントには黄色、本番稼働用アカウントには赤を使用できます。

> **Note**
>
> AWS User Experience Customization AWS マネジメントコンソールや Amazon Q などの の基本的な機能には AWS CloudShell、適切な IAM アクセス許可が必要です。 AWS 管理ポリシーは、 内で使用されるユーザーとロールにこれらのアクセス許可を付与する便利な方法を提供します AWS マネジメントコンソール。次のマネージドポリシーは、以下の目的で利用できます。
>
> - `AWSManagementConsoleBasicUserAccess`
>   - 管理者以外のユーザーの場合

- 基本的なコンソール機能へのアクセスを提供します
- `AWSManagementConsoleAdministratorAccess`
  - 管理ユーザーの場合
  - 重要な AWS マネジメントコンソール 機能へのアクセスを提供します
  - 管理者が他の ID AWS マネジメントコンソール の を設定およびカスタマイズすることを許可する

詳細については、「???」を参照してください。

アカウントの色を設定するには

1. AWS マネジメントコンソール にサインインします。
2. ナビゲーションバーで、アカウント名を選択します。
3. [アカウント] を選択します。
4. [アカウント表示設定] で、色を選択します。
5. [更新] を選択します。

API リファレンス

AWS User Experience Customization API リファレンスには、 AWS 各 User Experience Customization API アクションの説明、API リクエストパラメータ、JSON レスポンスが記載されています。

トピック

- アクション
- 共通エラー

アクション

以下のアクションがサポートされています:

- ???
- ???

- ???

GetAccountColor

アカウントに関連付けられた色を取得します。

リクエストの構文

```
GET /v1/account-color HTTP/1.1
```

リクエストは URI パラメータを使用したり、リクエスト本文を含めたりしません。

レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json

{
    "color": "string"
}
```

レスポンス要素

color

アカウントに関連付けられた色。

タイプ: 文字列

有効な値: none | pink | purple | darkBlue | lightBlue | teal | green | yellow | orange | red

エラー

すべてのアクションに共通のエラーについては、「一般的なエラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

リクエストの処理中に予期しないエラーが発生しました。

HTTP ステータスコード: 500

ThrottlingException

リクエストのスロットリングにより、リクエストが拒否されました。

HTTP ステータスコード: 429

ValidationException

この例外は、通知イベントが検証に失敗したときにスローされます。

HTTP ステータスコード: 400

DeleteAccountColor

アカウントの色設定を削除します。

リクエストの構文

```
DELETE /v1/account-color HTTP/1.1
```

リクエストパラメーター

このオペレーションはリクエストパラメータを使用しません。

リクエスト本文

この操作にリクエストボディはありません。

レスポンス本文

このオペレーションはレスポンス本文を返しません。

エラー

すべてのアクションに共通のエラーについては、「一般的なエラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

リクエストの処理中に予期しないエラーが発生しました。

HTTP ステータスコード: 500

ThrottlingException

リクエストのスロットリングにより、リクエストが拒否されました。

HTTP ステータスコード: 429

ValidationException

この例外は、通知イベントが検証に失敗したときにスローされます。

HTTP ステータスコード: 400

PutAccountColor

アカウントに関連付けられた色を設定します。

リクエストの構文

```
PUT /v1/account-color HTTP/1.1
```

リクエスト本文

```
Content-type: application/json

{
   "color": "string"
}
```

レスポンスの構文

```
HTTP/1.1 200
```

```
Content-type: application/json

{
    "color": "string"
}
```

レスポンス要素

color

アカウントに関連付けられた色。

タイプ: 文字列

有効な値: none | pink | purple | darkBlue | lightBlue | teal | green | yellow | orange | red

エラー

すべてのアクションに共通のエラーについては、「一般的なエラー」を参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

InternalServerException

リクエストの処理中に予期しないエラーが発生しました。

HTTP ステータスコード: 500

ThrottlingException

リクエストのスロットリングにより、リクエストが拒否されました。

HTTP ステータスコード: 429

ValidationException

この例外は、通知イベントが検証に失敗したときにスローされます。

HTTP ステータスコード: 400

共通エラー

以下のエラーは、すべての AWS サービスの API アクションに共通しています。API アクションに固有のエラーについては、そのアクションのドキュメントを参照してください。

AccessDeniedException

このアクションを実行する十分なアクセス権限がありません。

HTTP ステータスコード: 403

詳細については、「アクセス拒否エラーのトラブルシューティング」を参照してください。

ExpiredTokenException

リクエストに含まれているセキュリティトークンが有効期限切れです。

HTTP ステータスコード: 403

IncompleteSignature

リクエスト署名が AWS 標準に準拠していません。

HTTP ステータスコード: 403

InternalFailure

不明なエラー、例外、または障害により、リクエストの処理が失敗しました。

HTTP ステータスコード: 500

MalformedHttpRequestException

HTTP レベルでリクエストに問題があります。例えば、コンテンツエンコードで指定された解凍アルゴリズムに従って本文を解凍することはできません。

HTTP ステータスコード: 400

NotAuthorized

このアクションを実行するためのアクセス許可がありません。

HTTP ステータスコード: 401

OptInRequired

AWS アクセスキー ID には、サービスのサブスクリプションが必要です。

HTTP ステータスコード: 403

RequestAbortedException

リクエストは、返信が返送される前に中止されました (クライアントが接続を閉じたなど)。

HTTP ステータスコード: 400

RequestEntityTooLargeException

HTTP レベルでリクエストに問題があります。リクエストエンティティが大きすぎます。

HTTP ステータスコード: 413

RequestExpired

リクエストの日付スタンプから 15 分を経過した後またはリクエストの有効期限 (署名付き URL の場合など) から 15 分を経過した後に、リクエストが到着しました。または、リクエストの日付スタンプが現在より 15 分以上先です。

HTTP ステータスコード: 400

RequestTimeoutException

HTTP レベルでリクエストに問題があります。リクエストの読み取りがタイムアウトしました。

HTTP ステータスコード: 408

ServiceUnavailable

サーバーの一時的な障害により、リクエストは失敗しました。

HTTP ステータスコード: 503

ThrottlingException

リクエストのスロットリングにより、リクエストが拒否されました。

HTTP ステータスコード: 400

UnrecognizedClientException

指定された X.509 証明書または AWS アクセスキー ID がレコードに存在しません。

HTTP ステータスコード: 403

UnknownOperationException

リクエストされたアクション、またはオペレーションは無効です。アクションが正しく入力されていることを確認してください。

HTTP ステータスコード: 404

ValidationError

入力が AWS サービスで指定された制約を満たしていません。

HTTP ステータスコード: 400

を使用した AWS User Experience Customization API コールのログ記録 AWS CloudTrail

AWS ユーザーエクスペリエンスのカスタマイズは、ユーザーAWS CloudTrail、ロール、またはによって実行されたアクションを記録するサービスである と統合されています AWS のサービス。CloudTrail は、UXC 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。キャプチャされるコールには、 UXC コンソールからのコールと、UXC API オペレーションへのコードコールが含まれます。CloudTrail によって収集された情報を使用して、UXC に対するリクエスト、リクエスト元の IP アドレス、リクエストの作成日時、およびその他の詳細を確認できます。

CloudTrail は、アカウントを作成する AWS アカウント と でアクティブになり、CloudTrail イベント履歴に自動的にアクセスできます。CloudTrail の [イベント履歴] では、 AWS リージョンで過去 90 日間に記録された管理イベントの表示、検索、およびダウンロードが可能で、変更不可能な記録を確認できます。詳細については、「AWS CloudTrail ユーザーガイド」の「CloudTrail イベント履歴の使用」を参照してください。[イベント履歴] の閲覧には CloudTrail の料金はかかりません。

AWS アカウント 過去 90 日間のイベントの継続的な記録については、証跡または CloudTrail Lake イベントデータストアを作成します。

CloudTrail での UXC 管理イベント

管理イベントは、 のリソースで実行される管理オペレーションに関する情報を提供します AWS アカウント。これらのイベントは、コントロールプレーンオペレーションとも呼ばれます。CloudTrail は、デフォルトで管理イベントをログ記録します。

AWS User Experience Customization は、すべての UXC コントロールプレーンオペレーションを管理イベントとしてログに記録します。UXC が CloudTrail に記録する AWS User Experience

Customization コントロールプレーンオペレーションのリストについては、AWS 「User Experience Customization API Reference」を参照してください。

UXC イベントの例

各イベントは任意の送信元からの単一のリクエストを表し、リクエストされた API オペレーション、オペレーションの日時、リクエストパラメータなどに関する情報を含みます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、イベントは特定の順序で表示されません。

次の例は、 オペレーションを示す CloudTrail イベントを示しています。


```
{
  "eventVersion" : "1.09",
  "userIdentity" : {
    "type" : "AssumedRole",
    "principalId" : "AIDACKCEVSQ6C2EXAMPLE:jdoe",
    "arn" : "arn:aws:sts::111122223333:assumed-role/user/jdoe",
    "accountId" : "111122223333",
    "accessKeyId" : "AKIAIOSFODNN7EXAMPLE",
    "sessionContext" : {
      "sessionIssuer" : {
        "type" : "Role",
        "principalId" : "AIDACKCEVSQ6C2EXAMPLE",
        "arn" : "arn:aws:iam::111122223333:role/user",
        "accountId" : "111122223333",
        "userName" : "jdoe"
      },
      "webIdFederationData" : { },
      "attributes" : {
        "creationDate" : "2022-12-09T23:48:51Z",
        "mfaAuthenticated" : "false"
      }
    }
  },
  "eventTime" : "2022-12-09T23:50:03Z",
  "eventSource" : "uxc.amazonaws.com",
  "eventName" : "GetAccountColor",
  "awsRegion" : "us-east-2",
  "sourceIPAddress" : "10.24.34.3",
  "userAgent" : "PostmanRuntime/7.43.4",
  "requestParameters" : null,
  "responseElements" : null,
```

```
  "requestID" : "543db7ab-b4b2-11e9-8925-d139e92a1fe8",
  "eventID" : "5b2805a5-3e06-4437-a7a2-b5fdb5cbb4e2",
  "readOnly" : true,
  "eventType" : "AwsApiCall",
  "managementEvent" : true,
  "recipientAccountId" : "111122223333",
  "eventCategory" : "Management"
}
```

CloudTrail レコードの内容については、「AWS CloudTrail ユーザーガイド」の「CloudTrail record contents」を参照してください。

AWS の 管理ポリシー AWS マネジメントコンソール

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できるように、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ように設計されています。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケースに固有のカスタマー管理ポリシーを定義して、アクセス許可を絞り込むことをお勧めします。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS マネージドポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) に影響します。 AWS は、新しい が起動されるか、新しい API オペレーション AWS のサービス が既存のサービスで使用できるようになったときに、 AWS マネージドポリシーを更新する可能性が高くなります。

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」を参照してください。

AWS マネージドポリシー: AWSManagementConsoleBasicUserAccess

ユーザー、グループおよびロールに `AWSManagementConsoleBasicUserAccess` をアタッチできます。

このポリシーは、 AWS マネジメントコンソールの非管理ユーザーに必要なアクセス許可を付与します。これには、リソース検出、通知、ブラウザベースのシェルアクセス、カスタマイズされたナビゲーションなどの機能が含まれます。

アクセス許可の詳細

この `AWSManagementConsoleBasicUserAccess` は、以下のアクセス許可セットにグループ化されます。

- cloudshell – 環境の作成、セッション管理、コマンド実行などの AWS CloudShell 機能へのフルアクセスをプリンシパルに許可します。
- ec2 – プリンシパルが統合ナビゲーションでアカウントに対して有効になっているリージョンを記述できるようにします。
- notifications – プリンシパルが からイベントを取得できるようにします AWS User Notifications。
- q – プリンシパルが Amazon Q Developer とチャットできるようにします。
- resource-explorer-2 – プリンシパルが統合検索を使用して AWS リソースを検索および検出できるようにします。
- uxc – プリンシパルに AWS ユーザーエクスペリエンスのカスタマイズ設定の読み取りを許可します。
- action-recommendations – プリンシパルがコンテキストアクションのレコメンデーションを受信できるようにします。
- account – プリンシパルが、アカウント名、アカウント ID、アカウント作成日時など、指定されたアカウントに関する情報を取得できるようにします。

このポリシーのアクセス許可を確認するには、「AWS マネージドポリシーリファレンス」の「AWSManagementConsoleBasicUserAccess」を参照してください。

AWS マネージドポリシー: AWSManagementConsoleAdministratorAccess

ユーザー、グループおよびロールに AWSManagementConsoleAdministratorAccess をアタッチできます。

このポリシーは、 AWS マネジメントコンソールを設定およびカスタマイズするためのフルアクセスを許可します。これにより、管理者はアカウントの色の設定、ユーザー通知の有効化、リソース検出の設定を行うことができます。また、AWSManagementConsoleBasicUserAccess マネージドポリシーからのアクセス許可も含まれ、 AWS マネジメントコンソールの非管理ユーザーにとって不可欠です。

アクセス許可の詳細

この AWSManagementConsoleAdministratorAccess は、以下のアクセス許可セットにグループ化されます。

- cloudshell – 環境の作成、セッション管理、コマンド実行などの AWS CloudShell 機能へのフルアクセスをプリンシパルに許可します。
- ec2 – プリンシパルが統合ナビゲーションでアカウントに対して有効になっているリージョンを記述できるようにします。
- notifications – プリンシパルが通知設定、イベント、および機能のオプトインステータスにアクセスして更新できるようにします。
- q – プリンシパルが AI アシストサポートのために Amazon Q Developer とチャットできるようにします。
- resource-explorer-2 – プリンシパルが統合検索を使用して AWS リソースを検索および検出できるようにします。
- uxc – AWS User Experience Customization 設定へのフルアクセスをプリンシパルに許可します。
- action-recommendations – プリンシパルがコンテキストアクションのレコメンデーションを受信できるようにします。
- account – プリンシパルが、アカウント名、アカウント ID、アカウント作成日時など、指定されたアカウントに関する情報を取得できるようにします。

このポリシーのアクセス許可を確認するには、「AWS マネージドポリシーリファレンス」の「AWSManagementConsoleAdministratorAccess」を参照してください。

AWS マネジメントコンソール AWS 管理ポリシーの更新

このサービスがこれらの変更の追跡を開始 AWS マネジメントコンソール してからの の AWS 管理ポリシーの更新に関する詳細を表示します。このページの変更に関する自動アラートについては、AWS マネジメントコンソール ドキュメント履歴ページの RSS フィードにサブスクライブしてください。

変更	説明	日付
AWSManagementConsoleBasicUserAccess – 更新されたポリシー	ポリシーを更新して、ユーザーが のナビゲーション中にアカウント情報を表示し、アクションのレコメンデーションを受信できるようにするアクセス許可を追加しました AWS マネジメントコンソール。	2025 年 12 月 9 日
AWSManagementConsoleAdministratorAccess – 更新されたポリシー	ポリシーを更新して、ユーザーが のナビゲーション中にアカウント情報を表示し、アクションのレコメンデーションを受信できるようにするアクセス許可を追加しました AWS マネジメントコンソール。	2025 年 12 月 9 日
AWSManagementConsoleBasicUserAccess – 新しいポリシー	基本的な AWS マネジメントコンソール ナビゲーション、アカウントの色表示、リソース検出に必要なアクセス許可を付与する新しい AWS マネージドポリシーを追加しました。	2025 年 8 月 14 日
AWSManagementConsoleAdministratorAccess – 新しいポリシー	を設定およびカスタマイズするためのフルアクセスを提供する新しい AWS マネージドポリシーを追加しました AWS マネジメントコンソール。	2025 年 8 月 14 日
AWS マネジメントコンソールが変更の追跡を開始しました	AWS マネジメントコンソールは、 AWS 管理ポリシーの変更の追跡を開始しました。	2025 年 8 月 14 日

コンソールでの Markdown の使用

Amazon CloudWatch など AWS マネジメントコンソール、 の一部のサービスは、特定のフィールドでの Markdown の使用をサポートしています。このトピックでは、コンソールでサポートされている Markdown のフォーマットのタイプについて説明します。

内容

段落、線の間隔、および水平線

段落は空白行で区切ります。HTML に変換されたときに段落間の空白行が確実にレンダリングされるようにするには、改行しないスペース ( ) を含む新しい行を追加し、それに続けて空白行を追加します。次の例のように、複数の空白行を 1 つずつ挿入するには、この行のペアを繰り返します。

```
 

 
```

段落を区切る水平の罫線を作成するには、3 つの連続したハイフン (---) を含む新しい行を追加します。

```
Previous paragraph.
---
Next paragraph.
```

等幅タイプのテキストブロックを作成するには、3 つのバックティック (`) を含む行を追加します。等幅タイプで表示するテキストを入力します。次に、3 つのバックティックを含む別の新しい行を追加します。次の例は、表示時に等幅に変換されるテキストを示しています。

```
```
This appears in a text box with a background shading.
The text is in monospace.
```
```

ヘッダー

見出しを作成するには、シャープ記号 (#) を使用します。1 つのシャープ記号とスペースは、トップレベルの見出しを示します。2 つのシャープ記号を使用すると第 2 レベルのヘッダーが作成され、3 つのシャープ記号を使用すると第 3 レベルのヘッダーが作成されます。次の例は、最上位レベル、第 2 レベル、第 3 レベルの見出しを示しています。

```
# Top-level heading
```

```
## Second-level heading
```

```
### Third-level heading
```

テキストのフォーマット

テキストを斜体でフォーマットするには、両端を 1 つのアンダースコア (_) またはアスタリスク (*) で囲みます。

```
*This text appears in italics.*
```

テキストを太字でフォーマットするには、両端を 2 つのアンダースコアまたは 2 つのアスタリスクで囲みます。

```
**This text appears in bold.**
```

テキストを取り消し線でフォーマットするには、両端を 2 つのチルダ (~) で囲みます。

```
~~This text appears in strikethrough.~~
```

Links

テキストのハイパーリンクを追加するには、角かっこ ([ ]) で囲まれたリンクテキストを入力します。その後に、かっこで囲んだ完全な URL (( )) を入力します。次に例を示します。

```
Choose [link_text](http://my.example.com).
```

Lists

行を箇条書きの一部としてフォーマットするには、1 つのアスタリスク (*) に続いてスペースで始まる別々の行に追加します。次に例を示します。

```
Here is a bulleted list:
* Ant
* Bug
* Caterpillar
```

行を番号付きリストの一部としてフォーマットするには、別々の行に、数値、ピリオド (.)、およびスペースで始まる行に追加します。次に例を示します。

```
Here is a numbered list:
1. Do the first step
2. Do the next step
3. Do the final step
```

表とボタン (CloudWatch ダッシュボード)

CloudWatch ダッシュボードテキストウィジェットは Markdown テーブルとボタンをサポートしています。

表を作成するには、縦棒 (|) を使用して列を区切り、新しい行を使用して行を区切ります。最初の行をヘッダー行にするには、ヘッダー行と、値の最初の行の間に行を挿入します。次に、表の各列に少なくとも 3 つのハイフン (-) を追加します。縦棒を使用して列を区切ります。次の例は、2 つの列、ヘッダー行、および 2 行のデータを含む表の Markdown を示しています。

```
Table | Header
----|-----
Amazon Web Services | AWS
```

```
1 | 2
```

前の例の Markdown テキストでは、以下の表が作成されます。

[テーブル]	ヘッダー
Amazon Web Services	AWS
1	2

CloudWatch ダッシュボードテキストウィジェットでは、ボタンとして使用されるハイパーリンクをフォーマットすることもできます。ボタンを作成するには、[button:*Button text*] を使用し、その後に、かっこで囲んだ完全な URL (( )) を入力します。次に例を示します。

```
[button:Go to AWS](http://my.example.com)
[button:primary:This button stands out even more](http://my.example.com)
```

トラブルシューティング

に関する一般的な問題の解決策については、このセクションを参照してください AWS マネジメントコンソール。

Amazon Q Developer を使用して、一部の AWS サービスの一般的なエラーを診断およびトラブルシューティングすることもできます。詳細については、「Amazon Q Developer ユーザーガイド」の「Amazon Q Developerを使用したコンソールの一般的なエラーの診断」を参照してください。

トピック

ページが正しく読み込まれない

- この問題がたまにしか発生しない場合は、インターネット接続を確認してください。別のネットワーク経由で、VPN あり/なしで、または別のウェブブラウザを使用しての接続を試みます。
- 影響を受けるすべてのユーザーが同じチームに属する場合、プライバシーブラウザの拡張機能またはセキュリティファイアウォールの問題である可能性があります。プライバシーブラウザ拡張機能とセキュリティファイアウォールは、 AWS マネジメントコンソールによって使用されているドメインへのアクセスをブロックする可能性があります。これらの拡張機能をオフにするか、ファイアウォールの設定の調整をお勧めします。接続の問題を確認するには、お使いのブラウザのデベロッパーツール (Chrome、Firefoxの) をクリックし、[コンソール] タブに表示されたエラーを確認します。は、次のリストを含むドメインのサフィックス AWS マネジメントコンソール を使用します。これはすべてを網羅したリストではありません。これらのドメインのサフィックスは、AWSのみが排他的に使用するわけではありません。
  - .a2z.com
  - .amazon.com
  - .amazonaws.com
  - .aws
  - .aws.com

- .aws.dev
- .awscloud.com
- .awsplayer.com
- .awsstatic.com
- .cloudfront.net
- .live-video.net

> **Warning**
>
> 2022 年 7 月 31 日以降、 は Internet Explorer 11 をサポートし AWS なくなりました。サポートされている他のブラウザ AWS マネジメントコンソール で を使用することをお勧めします。詳細については、AWS ニュースブログを参照してください。

への接続時にブラウザに「アクセス拒否」エラーが表示される AWS マネジメントコンソール

コンソールに対する最近の変更は、以下の条件がすべて満たされた場合、アクセスに影響する可能性があります。

- VPC エンドポイントを介して AWS サービスエンドポイントに到達するように設定されたネットワーク AWS マネジメントコンソール から にアクセスします。
- AWS サービスへのアクセスを制限するには、IAM ポリシーで `aws:SourceIp`または `aws:SourceVpc` グローバル条件キーを使用します。

`aws:SourceIp` または `aws:SourceVpc` グローバル条件キーを含む IAM ポリシーを確認することをお勧めします。必要に応じて `aws:SourceIp` と `aws:SourceVpc` の両方を適用します。

一部の AWS マネジメントコンソール 機能では、IPv4 接続と IPv6 接続の両方をサポートするデュアルスタックドメインを使用します。IAM ポリシー`aws:SourceIp`が IPv4 CIDR ブロックのみで を使用してアクセスを制限する場合、オペレーティングシステムが IPv6 接続を優先する場合 (またはその逆の場合) 、リクエストが失敗する可能性があります。これを回避するには、IPv4 CIDR ブロックと IPv6 CIDR ブロックの両方を`aws:SourceIp`条件に含めます。詳細については、 AWS Identity and Access Management ユーザーガイドの「aws:SourceIp」を参照してください。

AWS マネジメントコンソール プライベートアクセス機能にオンボードして、VPC エンドポイント AWS マネジメントコンソール を介して にアクセスし、ポリシーaws:SourceVpcの条件を使用することもできます。詳細については次を参照してください:

- AWS マネジメントコンソール プライベートアクセス
- the section called “aws:SourceVpc での AWS マネジメントコンソール プライベートアクセスの仕組み”
- the section called “サポートされている AWS グローバル条件コンテキストキー”

に接続するとブラウザにタイムアウトエラーが表示される AWS マネジメントコンソール

デフォルトにサービス停止がある場合 AWS リージョン、 に接続しようとすると、ブラウザに 504 Gateway タイムアウトエラーが表示されることがあります AWS マネジメントコンソール。別のリージョン AWS マネジメントコンソール から にログインするには、URL で代替リージョンエンドポイントを指定します。例えば、us-west-1 (北カリフォルニア) リージョンでサービス停止があった場合に、us-west-2 (オレゴン) リージョンにアクセスするには、次のテンプレートを使用します。

```
https://region.console.aws.amazon.com
```

詳細については、AWS 全般のリファレンス の「AWS マネジメントコンソール サービスエンドポイント」を参照してください。

を含むすべての のステータスを表示するには AWS のサービス、 AWS マネジメントコンソール「」を参照してくださいAWS Health Dashboard。

の言語を変更したい AWS マネジメントコンソール が、ページの下部に言語選択メニューが見つからない

言語選択メニューは新しい [Unified Settings] (統合設定) ページに移動しました。の言語を変更するには AWS マネジメントコンソール、統合設定ページに移動し、コンソールの言語を選択します。

詳細については、AWS マネジメントコンソールの言語の変更を参照してください。

ドキュメント履歴

以下の表は、AWS マネジメントコンソール 入門ガイドの 2021 年 3 月以降の重要な変更点をまとめたものです。

変更	説明	日付
ページが追加されました	推奨されるアクションを説明する新しいページが追加されました。詳細については、「???」を参照してください。	2025 年 10 月 15 日
新しい AWS マネージドポリシー	AWS マネジメントコンソールの使用、設定、カスタマイズのアクセス許可の範囲を設定する 2 つの新しいポリシーを追加しました。 • AWSManagementConsoleBasicUserAccess • AWSManagementConsoleAdministratorAccess	2025 年 8 月 14 日
User Experience Customization (UXC)	新しい サービスが利用可能になりました。	2025 年 8 月 14 日
ページの更新	[サービス] メニューから myApplications でアプリケーションを表示できるようになりました。詳細については、「???」を参照してください。	2025 年 7 月 29 日
ページが追加されました	マルチセッション機能を説明する新しいページが追加されました。詳細については、「???」を参照してください。	2024 年 12 月 6 日

変更	説明	日付
ページの更新	パスワードの変更ページが更新されました。詳細については、「???」を参照してください。	2024 年 6 月 18 日
新しいページの追加	サービスメニューと AWS イベント通知へのアクセス方法を説明する新しいページが追加されました。詳細については、「???」および「???」を参照してください。	2024 年 6 月 18 日
ページの更新	「AWS マネジメントコンソール とは」ページが更新されました。詳細については、「???」を参照してください。	2024 年 6 月 18 日
サポートを受ける	サポートを受ける方法を説明する新しいページが追加されました。詳細については、「???」を参照してください。	2024 年 6 月 18 日
統合ナビゲーションと AWS Console Home	コンソールの操作方法を説明する新しいページが追加されました。詳細については、「???」および「???」を参照してください。	2024 年 6 月 18 日
Amazon Q とのチャット	ユーザーが Amazon Q Developer に AWS の質問をする方法を詳しく説明した新しい設定ページです。詳細については、「Amazon Q Developer とのチャット」を参照してください。	2024 年 5 月 29 日

変更	説明	日付
myApplications	myApplications の概要を記載した新しいページです。詳細については、「AWS の myApplications とは」を参照してください。	2023 年 11 月 29 日
統合設定の指定	言語や地域など、現在のユーザーに適用される設定とデフォルト値を設定するための新しい設定ページ。詳細については、「統合設定の指定」を参照してください。	2022 年 4 月 6 日
AWS Console Homeの新しいUI	重要な使用状況情報と、AWS のサービスへのショートカットを表示するためのウィジェットが含まれた、AWS Console Homeの新しいUI。詳細については、「ウィジェットの操作」を参照してください。	2022 年 2 月 25 日
コンソールの言語の変更	AWS マネジメントコンソールの別の言語を選択します。詳細については、「AWS マネジメントコンソール の言語の変更」を参照してください。	2021 年 4 月 1 日
CloudShell の起動	AWS マネジメントコンソールから AWS CloudShell を開き、AWS CLI コマンドを実行します。詳細については、「AWS CloudShell の起動」を参照してください。	2021 年 3 月 22 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。