Amazon Connect

管理者ガイド

Amazon Connect: 管理者ガイド

Table of Contents

Amazon Connect とは

Amazon Connect は、クラウドベースのサポートセンターソリューションです。Amazon Connect を使えば、規模を問わず、カスタマーサポートセンターの設定と管理、および信頼性の高い顧客エンゲージメントの提供が容易になります。ほんの数ステップでサポートセンターを設定し、どこからでもエージェントをすぐに追加して、顧客対応をすぐに開始できます。

Amazon Connect には豊富なメトリクスとリアルタイムレポートが提供され、問い合わせのルーティングを最適化できます。顧客を適切なエージェントにつなげることで、顧客の問題を効率よく解決できます。Amazon Connect は既存システムとビジネスアプリケーションを統合し、顧客対応すべてに可視性と洞察を与えます。Amazon Connect は長期契約不要で、使用した分だけ料金が発生します。

Amazon Connect インスタンス

Amazon Connect サポートセンターを作成するには、Amazon Connect インスタンスを作成します。各インスタンスには、サポートセンターに関連するすべてのリソースと設定が含まれています。インスタンスの設定は、Amazon Connect コンソールから管理できます。サポートセンターの設定は、サポートセンター内から管理できます。インスタンスは複数作成できますが、各インスタンスは作成した AWS リージョン内でのみ機能します。設定、ユーザー、メトリクス、レポートは、Amazon Connect インスタンス間では共有されません。

ID 管理

Amazon Connect インスタンスを作成するときに、Amazon Connect ユーザーの管理方法を選択する必要があります。問い合わせコントロールパネル (CCP) を開く、電話を発信する、レポートを作成するなどの Amazon Connect の機能やリソースにアクセスする権限は Amazon Connect 内のユーザーアカウントに割り当てられます。ID 管理は、次の 3 つのオプションから選択できます。

- Amazon Connect にユーザーを格納します。
- AWS Directory Service を使った既存のディレクトリと連携します。
- SAML 2.0 ベースの認証を使用し、Amazon Connect インスタンスと連携し、シングルサインオンを有効にします。

Amazon Connect の ID 管理についての詳細は、ユーザーおよび ID 管理を計画する (p. 5) をご覧ください。

Amazon Connect 管理者

Amazon Connect 管理者は権限の設定、メトリクスの生成と管理、ユーザーの追加、サポートセンターのあらゆる面の設定を行います。Amazon Connect にセキュリティプロファイルを割り当てることにより、さまざまなタイプの権限を付与または拒否できます。

安全なストレージとデータの完全性

安全なストレージとデータの完全性は、記録された通話の管理で重要な部分です。顧客の通話はリアルタイムで録音され、その中には機密情報が含まれることもあります。

デフォルトでは、AWS は設定プロセスで暗号化機能を内蔵した Amazon S3 バケットを新たに作成します。既存の S3 バケットも使用できます。通話録音とエクスポートされるレポート用に別々のバケットが

あり、個別に設定されます。Amazon Connect では、フルアクセスと記録全体のコントロールができるため、保持ポリシーをカスタマイズすることができます。Amazon S3 の中に発行されたカスタマイズ可能なメトリクスレポートは、Amazon S3 API や AWS Lambda を使って処理できます。レポートは、労働力管理やビジネスインテリジェンスツールなどの外部システムと統合します。

Note

暗号化はデフォルト設定を変えないことを推奨します。

以下のセキュリティ対策がサポートされています。

- AWS Key Management Service—AWS KMS は、暗号鍵を完全に管理できる強力なマネージド型サービスです。デフォルトの AWS KMS キーが用意されています。
- ARN/ID—ARN/ID を AWS KMS のマスターキーの代わりに使用できます。これは高度なオプションで、予定している変更に自信がある場合のみお試しください。

サポートされるブラウザ

Amazon Connect を使った作業を始める前に、お使いのブラウザが対応していることを以下の表で確認してください。

ブラウザ	バージョン	バージョン確認方法
Google Chrome	最新 3 バージョン	Chrome を起動して、アドレスバーに 「chrome://version」 と入力します。バージョンは結果の表示上部の [Google Chrome] フィールドに表示されます。
Mozilla Firefox ESR	最新 3 バージョン	Firefox を開きます。メニューで[ヘルプ]アイコンを選択し、Firefox について を選択します。バージョン番号は、Firefox 名の下に表示されます。
Mozilla Firefox	最新 3 バージョン	Firefox を開きます。メニューで[ヘルプ]アイコンを選択し、Firefox について を選択します。バージョン番号は、Firefox 名の下に表示されます。

関連サービス

以下のサービスは Amazon Connect と併用します。

- AWS Directory Service — Microsoft アクティブディレクトリ (エンタープライズエディション) 用の AWS Directory Service を使えば、ディレクトリ対応ワークロードと AWS リソースが AWS クラウド内のマネージド型アクティブディレクトリ を使用できるようになります。Amazon Connect ユーザーと ID 管理はこのサービスをベースにしています。
- Amazon S3 — Amazon Connect では、Amazon Simple Storage Service (Amazon S3) を使用して、Amazon Connect からデータ (例: 通話記録、メトリクスレポート) を保存しています。
- AWS Lambda — Lambda では、サーバーのプロビジョニングや管理を行うことなく、コードを迅速に構築し、実行することができます。Amazon Connect では、問い合わせフローで関数を呼び出すことが

できます。内部システムと通信する Lambda 関数 (例: 注文のステータスの取得) を構築できます。これで、問い合わせフローでその関数から返った値を使用して、カスタマーエクスペリエンスをパーソナライズできます。

- Amazon Lex — Amazon Connect は、Amazon Lex と統合して、音声とテキストを使用した会話型インターフェイスを提供します。Amazon Lex には、音声をテキストに変換するための自動音声認識 (ASR) と、お客様の意図を認識する自然言語理解 (NLU) があります。詳細については、『Amazon Lex 開発者ガイド』を参照してください。
- Kinesis—Amazon Connect は、ストリーミングの問い合わせ追跡レコード (CTR) とエージェントイベントストリームのデータのプラットフォームとして Kinesis と統合します。データは、JSON 形式で Kinesis に発行され、サポートセンターでの連絡先とエージェントのアクティビティに関する詳細情報が含まれています。データストリームを使用して、CTR を Amazon Redshift (AWS データウェアハウスサービス) またはカスタムデータウェアハウスシステムに発行できます。これで、コンタクトセンターのデータに関する詳細な分析とレポート作成を有効にできます。Amazon QuickSight (クラウド対応のビジネス分析サービス) または独自の BI ツールを使用して、合成されたデータ上で強力な可視化を実現します。さらに、このデータは Elasticsearch にストリーミングさせて、便利なビジュアルインターフェイスを用いてデータにクエリを実行できます。詳細については、「Amazon Kinesis Data Streams 開発者ガイド」を参照してください。

  Note

  Amazon Connect はサーバー側で暗号化されているストリームへのデータ公開には対応していません。
- Amazon CloudWatch — Amazon Connect は CloudWatch と統合し、リアルタイムのオペレーションメトリクスをコンタクトセンター向けに提供します。メトリクスには、1 秒あたりの総コール数、拒否またはスロットリングされたコール数、同時コール数の割合 (%)、失敗/不在着信コール数 (エラー、間違い番号/住所 , ビジー/通話中)、および問い合わせフローエラーなどが含まれます。サポートセンターの健全性をトップレベルに保つため、これらのメトリクスのモニタリングを設定できます。詳細については、「Amazon Connect インスタンスの CloudWatch メトリクス (p. 28)」を参照してください。
- AWS Identity and Access Management — AWS マネジメントコンソール では、リソースへのアクセス許可があるかどうかをサービスが判断するために、ユーザー名とパスワードが要求されます。ルートユーザーの認証情報は、どのような方法でも許可を取り消したり、制限したりすることができないため、AWS へのアクセスにルートアカウントの認証情報を使用しないでください。代わりに、IAM ユーザーを作成し、管理アクセス権限のある IAM グループにそのユーザーを追加することをお勧めします。その結果、IAM ユーザーの認証情報を使用してコンソールにアクセスすることになります。詳細については、「IAM ユーザーガイド」を参照してください。

  AWS にサインアップしても、ご自分の IAM ユーザーをまだ作成していない場合は、IAM コンソールを使用して作成できます。詳細については、『IAM ユーザーガイド』の「個々の IAM ユーザーの作成」を参照してください。
- AWS Key Management Service—Amazon Connect は AWS KMS と統合され、顧客のデータを保護します。キーの管理は、AWS KMS コンソールから行うことができます。詳細については、『AWS Key Management Service Developer Guide』の「AWS Key Management Service とは」を参照してください。

Amazon Connect の使用開始

Amazon Connect インスタンスは、コンタクトセンターの出発点です。インスタンスを作成したら、その設定を編集することができます。設定には、テレフォニー、データストレージ、データストリーミング、アプリケーション統合、問い合わせフローなどが含まれます。その後、AWS マネジメントコンソール からインスタンスを起動し、コンタクトセンターの使用を開始することができます。

> Note
>
> Amazon Connect は、インドで Amazon Internet Services Pvt. Lt (AISPL) を介して Amazon Web Services を使用しているお客様にはご利用いただけません。。Amazon Connect でインスタンスを作成しようとすると、エラーメッセージが表示されます。

Amazon Connect インスタンスを作成した後、コンタクトセンターで使用する電話番号を要求します。電話番号を要求したら、コンタクトセンターへのテスト通話を実施し、正しく動作していることを確認します。コンタクトセンターへの通話は、Contact Control Panel (CCP) を使って処理されます。CCP は、Amazon Connect Contact Center Manager (CCM) に組み込まれています。エージェントによる CCP の使用の詳細については、『Amazon Connect ユーザーガイド』の「Contact Control Panel を使用する」を参照してください。

インスタンスの設定は、AWS マネジメントコンソール コンソールから編集できます。作成したインスタンスには、[アクセス URL] 列の URL を使ってアクセスします。アクセス URL は、エージェント、管理者、マネージャーが CCM と CCP にログインするために使用する URL です。詳細については、「Amazon Connect インスタンス (p. 1)」を参照してください。

> Note
>
> ID の管理に SAML ベースの認証を使用する場合、ユーザーは、インスタンスのアクセス URL ではなく、ID プロバイダーを介してインスタンスにログインしなければなりません。

開始する前に

Amazon Web Services (AWS) にサインアップすると、AWS アカウントは自動的に Amazon Connect など AWS のすべてのサービスにサインアップします。料金が発生するのは、実際に使用したサービスの分のみです。

すでに AWS アカウントをお持ちの場合は、次のタスクに進んでください。AWS アカウントをお持ちでない場合は、次に説明する手順にしたがってアカウントを作成してください。

AWS アカウントを作成するには

1. https://aws.amazon.com/ を開き、[AWS アカウントの作成] を選択します。

   > Note
   >
   > AWS アカウントのルートユーザー 認証情報を使用して、すでに AWS マネジメントコンソール にサインインしている場合は、[Sign in to a different account (別のアカウントにサインインする)] を選択します。IAM 認証情報を使用して、すでにコンソールにサインインしている場合は、[Sign-in using root account credentials (ルートアカウントの資格情報を使ってサインイン)] を選択します。[新しい AWS アカウントの作成] を選択します。

2. オンラインの手順に従います。

サインアップ手順の一環として、通話呼び出しを受け取り、電話のキーパッドを用いて確認コードを入力することが求められます。

ポートとプロトコルの要件

エージェントが Amazon Connect でコールを処理できるように Amazon Connect ソフトフォン問い合わせコントロールパネル (CCP) を使用する場合は、Amazon Connect で使用されるソフトフォンや AWS のその他のサービスと通信するために Amazon Connect で使用される必須プロトコルのポートを通過するトラフィックを許可する必要があります。ソフトフォンクライアントはウェブブラウザで実行され、パブリック IP アドレスと TCP/UDP ポートのセットを使用して Amazon Connect および AWS の他のサービスに接続されます。この通信を許可するには、「ソフトフォン CCP の IP アドレスの範囲」に記載されているポートおよびプロトコルへのネットワークのトラフィックを許可する必要があります。

ユーザーおよび ID 管理を計画する

Amazon Connect インスタンスを設定する前に、Amazon Connect ユーザーの管理方法を決定する必要があります。インスタンスの作成後に ID 管理のオプションを変更することはできません。選択したオプションまたはディレクトリを変更する場合は、インスタンスを削除して新しいインスタンスを作成します。インスタンスを削除すると、すべての設定とメトリクスデータが失われます。

Amazon Connect でサポートされている以下の ID 管理ソリューションの中から、いずれかを選択します。

- [Amazon Connect 内にユーザーを保存] — ユーザーアカウントを Amazon Connect の中で作成し、管理する場合は、このオプションを選択します。Amazon Connect でユーザーを管理する場合、各ユーザーのユーザー名とパスワードは、Amazon Connect 専用のものになります。ユーザーは、Amazon Connect へのログイン用に別のユーザー名とパスワードを覚えなければなりません。
- [既存のディレクトリへのリンク] — 既存のディレクトリを使用するには、このオプションを選択します。アカウントに関連付けられ、AWS Directory Service で設定され、インスタンスの作成先と同じリージョンでアクティブであるディレクトリを使用する必要があります。このオプションを選択する場合は、Amazon Connect インスタンスを作成する前にディレクトリを準備します。詳細については、Amazon Connect の ID 管理に既存のディレクトリを使用する (p. 6)を参照してください。
- [SAML 2.0 ベースの認証] — 既存のネットワーク ID プロバイダーを使用してユーザーを Amazon Connect と連携させる場合は、このオプションを選択します。ユーザーは、ID プロバイダーを通じて設定されたリンクを使用しないと Amazon Connect にログインできません。このオプションを選択する場合は、Amazon Connect インスタンスを作成する前に SAML 環境を設定します。詳細については、Amazon Connect での ID 管理用に SAML を設定する (p. 7) を参照してください。

Amazon Connect インスタンスの作成

インスタンスの作成または追加は、以下のように行います。

Amazon Connect インスタンスを作成するには

1. Amazon Connect コンソール (https://console.aws.amazon.com/connect/) を開きます。
2. 以下のいずれかを行います。
   - これまでに Amazon Connect インスタンスを作成したことがない場合は、[Get started (今すぐ始める)] を選択します。
   - インスタンスを作成したことがある場合は、[インスタンスを追加する] を選択します。
3. [ステップ 1: ID 管理] で、以下のいずれかを行います。

- Amazon Connect の中でユーザーを管理するには、[Amazon Connect 内にユーザーを保存] を選択します。
- 既存のディレクトリでユーザーが管理されていて、それを使用する場合は、[既存のディレクトリへのリンク] を選択します。既存のディレクトリの使用の詳細については、Amazon Connect の ID 管理に既存のディレクトリを使用する (p. 6) を参照してください。
- ID プロバイダーで SAML ベースの認証を使用し、ユーザーを Amazon Connect と連携させるには、[SAML 2.0 ベースの認証] を選択します。Amazon Connect で SAML を使用する方法については、Amazon Connect での ID 管理用に SAML を設定する (p. 7) を参照してください。

4. [アクセス URL] には、インスタンスのインスタンスエイリアスを入力し、[次のステップ] を選択します。

   入力した名前が AWS マネジメントコンソール にインスタンスエイリアスとして表示され、コンタクトセンターにアクセスするためのアクセス URL にドメインとして含まれます。エイリアスは、グローバルに一意である必要があります。つまり、1 つのエイリアスは、すべての Amazon Connect インスタンスとリージョンにまたがって 1 回しか使用できません。インスタンスの作成後にエイリアス URL を変更することはできません。
5. [ステップ 2: 管理者] で、以下のいずれかを行います。
   - ID 管理の方法として [Amazon Connect 内にユーザーを保存] を選択した場合は、管理者アカウントのユーザーの詳細を入力し、[次のステップ] を選択します。
   - ID 管理の方法として [既存のディレクトリへのリンク] を選択した場合は、インスタンスの管理者アカウントとして使用するアカウントのユーザー名を入力し、[次のステップ] を選択します。

     入力するユーザー名がディレクトリの中にない場合は、後で追加することができます。
   - 後で管理者アカウントを作成するには、[これをスキップ] を選択します。後で管理者を作成するには、Amazon Connect コンソールから管理者としてインスタンスにログインします。
6. [ステップ 3: テレフォニーオプション] では、コンタクトセンターで通話を受信するか、通話を発信するか、両方を行うかを指定します。ユーザーのアクセス権限は、Amazon Connect ウェブアプリケーション内で設定できます。設定後に電話番号のオプションが表示されます。
7. [ステップ 4: データストレージ] では、デフォルト設定をそのまま使用するか、[設定カスタマイズ] を選択します。詳細については、「データストレージ (p. 21)」を参照してください。
8. [ステップ 5: レビューと作成] では、設定内容を確認し、[インスタンスの作成] を選択します。

   Important

   ディレクトリ名とドメイン名の設定が変更できるのは、このタイミングだけです。その他の設定は、後から編集できます。
9. インスタンスの作成後、[今すぐ始める] を選択して電話番号を要求し、テストします。Amazon Connect によって自動的にインスタンスの設定が行われ、選択した電話番号が使用されるようになります。

   Note

   現在の電話番号を維持し、Amazon Connect で使用する方法については、現在の電話番号を移植する (p. 13) を参照してください。
10. (オプション) インスタンスの設定に進みます。詳細については、「Amazon Connect インスタンスを設定する (p. 20)」を参照してください。

Amazon Connect の ID 管理に既存のディレクトリを使用する

すでに AWS Directory Service ディレクトリを使ってユーザーを管理している場合は、同じディレクトリで Amazon Connect のユーザーアカウントを管理することができます。また、Amazon Connect 用

に、AWS Directory Service で新しいディレクトリを作成することもできます。AWS アカウントに関連付けられ、インスタンスの作成先と同じ AWS リージョンでアクティブであるディレクトリを選択する必要があります。AWS Directory Service ディレクトリは、1 度に 1 つの Amazon Connect インスタンスにのみ関連付けることができます。ディレクトリを別のインスタンスで使用するには、そのディレクトリが関連付けられているインスタンスを削除する必要があります。

Amazon Connect では、以下の AWS Directory Service ディレクトリがサポートされています。

- Microsoft Active Directory—AWS Directory Service では、Microsoft Active Directory をマネージド型サービスとして実行できます。
- Active Directory Connector — AD Connector は、ディレクトリリクエストをオンプレミスの Microsoft Active Directory にリダイレクトするために使用するディレクトリゲートウェイです。
- Simple Active Directory — Simple AD は、Samba 4 Active Directory Compatible Server を利用したスタンドアロンのマネージド型ディレクトリです。

選択した ID オプションをインスタンスの作成後に変更することはできません。選択したディレクトリを変更する場合は、インスタンスを削除して新しいインスタンスを作成します。インスタンスを削除すると、すべての設定とメトリクスデータが失われます。

Amazon Connect で既存のディレクトリや独自のディレクトリを使用する場合、追加料金はかかりません。AWS Directory Service の使用に関連する費用の詳細については、「AWS サービス料金の概要」をご覧ください。

AWS Directory Service を使用して作成した新しいディレクトリには、次のような制限が適用されます。

- ディレクトリ名には英数字のみを含めることができます。使用できる記号は「.」のみです。
- いったん Amazon Connect インスタンスに関連付けたディレクトリについて、関連付けを解除することはできません。
- 1 つの Amazon Connect インスタンスに追加できるディレクトリは 1 つだけです。
- 複数の Amazon Connect インスタンスでディレクトリを共有することはできません。

Amazon Connect での ID 管理用に SAML を設定する

Amazon Connect は、Security Assertion Markup Language (SAML) 2.0 を使った ID フェデレーションをサポートすることで、組織から Amazon Connect インスタンスへのウェブベースのシングルサインオン (SSO) を可能にします。これにより、ユーザーは SAML 2.0 互換の ID プロバイダー (IdP) によってホストされている組織のポータルにサインインすることができます。IdP には、Amazon Connect にログインするためのオプションがあります。このオプションでは、ユーザーは、Amazon Connect インスタンスにリダイレクトされます。Amazon Connect 用に認証情報を別途入力する必要はありません。

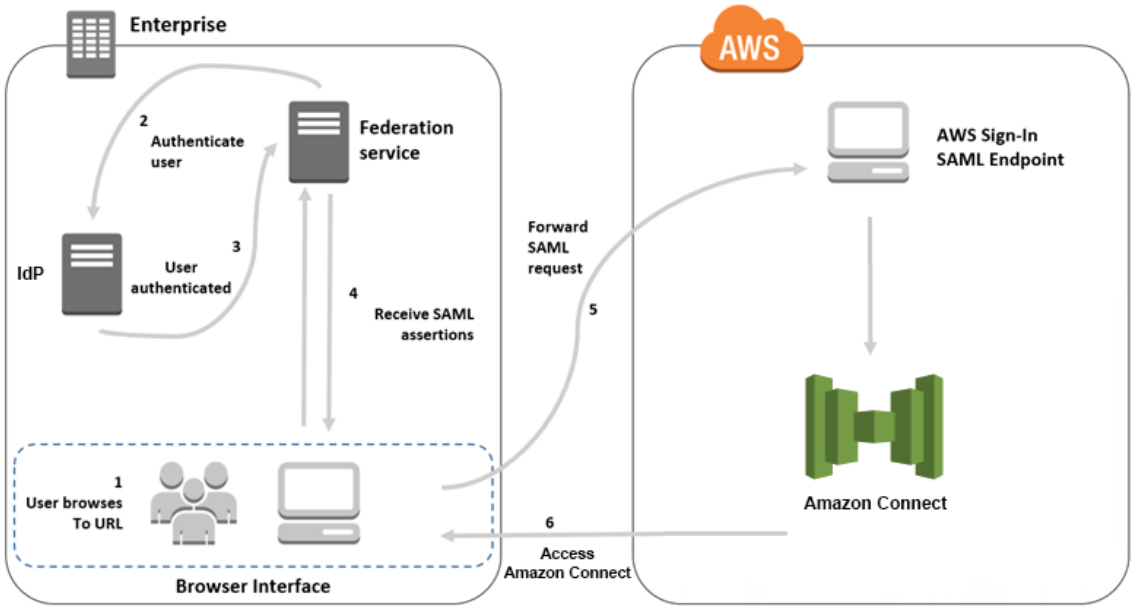
> Important
>
> SAML 認証を有効にするには、フェデレーションの AWS Identity and Access Management (IAM) ロールを作成します。このロールは、IdP と Amazon Web Services の間のフェデレーションに使用されます。AWS Identity and Access Management は、AWS リソースへのアクセスを安全にコントロールするのに役立つウェブサービスです。IAM により、誰を認証 (サインイン) し、誰にリソースの使用を承認する (アクセス権限を持たせる) かを制御します。この場合、IAM ロールは、ID プロバイダーと AWS の間のフェデレーションに使用されます。IAM ロールのアクセス権限が Amazon Connect へのアクセスを可能にします。
> 自分のルート AWS アカウントを SAML フェデレーションのアカウントとして使用することはできません。その代わりに、トピック内のステップや、AWS Identity and Access Management

ドキュメントにリンクされたトピックに従ってフェデレーション用の IAM ロールを作成します。IAM の詳細については、「IAM とは何ですか」を参照してください。

SAML を設定するためのステップは、以下のとおりです。

Amazon Connect での SAML の使用の概要

次の図は、ユーザーを認証して Amazon Connect と連携させる際の SAML リクエストのフローを示します。



SAML リクエストは、次のようなステップを通過します。

1. ユーザーがアクセスする内部ポータルに、Amazon Connect にログインするためのリンクが含まれています。リンクは、ID プロバイダーで定義されたものです。
2. フェデレーションサービスが組織の ID ストアからの認証をリクエストします。
3. ID ストアはユーザーを認証し、フェデレーションサービスに認証レスポンスを返します。
4. 認証が成功すると、フェデレーションサービスはユーザーのブラウザに SAML アサーションを送信します。
5. ユーザーのブラウザが、AWS サインイン SAML エンドポイント (https://signin.aws.amazon.com/saml) に SAML アサーションを送信します。AWS サインインでは、SAML リクエストの受信、リクエストの処理、ユーザーの認証、Amazon Connect への認証トークンの転送を行います。
6. Amazon Connect は、AWS からの認証トークンを使用してユーザーを認証し、ユーザーのブラウザで Amazon Connect を開きます。

Amazon Connect に対して SAML ベースの認証を有効にする

Amazon Connect インスタンスで SAML 認証を使用するには、以下のステップで有効化し、設定する必要があります。

1. Amazon Connect インスタンスを作成し、ID 管理のための SAML 2.0 ベースの認証を選択します。
2. ID プロバイダーと AWS の間で SAML フェデレーションを有効にします。
3. Amazon Connect ユーザーを Amazon Connect インスタンスに追加します。インスタンスを作成したときに作成した管理者アカウントを使用して、インスタンスにログインします。[ユーザー管理] ページに移動し、ユーザーを追加します。ユーザー名は、ネットワークディレクトリと ID プロバイダー内のユーザー名と完全に一致する必要があります。
4. SAML アサーション、認証レスポンス、リレーステートに向けて ID プロバイダーを設定します。ユーザーが ID プロバイダーにログインします。ログインしたら、Amazon Connect インスタンスにリダイレクトされます。IAM ロールを使用して、AWS と連携します。これで、Amazon Connect にアクセスできるようになります。

インスタンスの作成時に SAML 2.0 ベースの認証を選択する

Amazon Connect インスタンスを作成する際、ID 管理用に SAML 2.0 ベースの認証オプションを選択します。2 番目のステップでインスタンスの管理者を作成するとき、指定するユーザー名が既存のネットワークディレクトリ内のユーザー名と完全に一致しなければなりません。既存のディレクトリを通じてすでにパスワードが管理されているため、管理者ユーザーのパスワードを指定するオプションはありません。管理者は、Amazon Connect で作成され、[管理者] セキュリティプロファイルが割り当てられます。

ユーザーを追加するには、管理者アカウントを使用して IdP から Amazon Connect インスタンスにログインします。

ID プロバイダーと AWS の間で SAML フェデレーションを有効にする

Amazon Connect に対して SAML ベースの認証を有効化するには、IAM コンソールで ID プロバイダーを作成する必要があります。詳細は、「Enabling SAML 2.0 Federated Users to Access the AWS Management Console (SAML 2.0 でフェデレーションしたユーザーによる AWS マネジメントコンソールへのアクセスを可能にする)」を参照してください。

AWS の ID プロバイダーを作成するためのプロセスは、Amazon Connect と同じです。フロー図のステップ 7 で、クライアントは、AWS マネジメントコンソール ではなく Amazon Connect インスタンスに送信されます。

AWS との SAML フェデレーションを有効にするには、次のようなステップが必要です。

1. AWS で SAML プロバイダーを作成します。詳細については、「SAML ID プロバイダーの作成」を参照してください。
2. AWS マネジメントコンソール と SAML 2.0 フェデレーションを行うための IAM ロールを作成します。フェデレーション用にロールを 1 つのみ作成します。IAM ロールによって、ID プロバイダーを通じてログインするユーザーが AWS でどのアクセス権限を得るかが決まります。この例では、Amazon Connect にアクセスするためのアクセス権限が与えられます。Amazon Connect の機能へのアクセス権限を制御するには、Amazon Connect 内のセキュリティプロファイルを使用します。詳細については、「SAML 2.0 フェデレーション用のロールの作成 (コンソール)」を参照してください。

ステップ 5 では、[プログラムによるアクセスと AWS マネジメントコンソールによるアクセスを許可する] を選択します。手順のトピック (SAML 2.0 フェデレーション用のロールを作成する準備をするには) に示されている信頼ポリシーを作成します。次のアクセス許可を Amazon Connect インスタンスに割り当てるポリシーを作成します。アクセス許可は、「SAML ベースのフェデレーション用のロールを作成するには」の手順のステップ 9 で始まります。

SAML フェデレーションに向けて IAM ロールにアクセス権限を割り当てるポリシーを作成するには

1. On the [アクセス権限ポリシーをアタッチする] ページで [ポリシーの作成] を選択します。
2. [ポリシーの作成] ページで、[JSON] を選択します。
3. 以下のサンプルポリシーのいずれかをコピーして JSON ポリシーエディタに貼り付け、既存のテキストを置き換えます。いずれかのポリシーを使用して SAML フェデレーションを有効化することも、特定の要件に合わせてポリシーをカスタマイズすることもできます。

   このポリシーを使用すると、特定の Amazon Connect インスタンス内のすべてのユーザーに対してフェデレーションが有効化されます。SAML ベースの認証の場合、作成したインスタンスの `Resource` の値を ARN に置き換えます。

```
{
    "Version": "2012-10-17",
   "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": "connect:GetFederationToken",
            "Resource": [
                "arn:aws:connect:us-east-1:361814831152:instance/2fb42df9-78a2-2e74-
d572-c8af67ed289b/user/${aws:userid}"
            ]
        }
    ]
}
```

   このポリシーを使用すると、特定の Amazon Connect インスタンスへのフェデレーションが有効化されます。`connect:InstanceId` の値をインスタンスのインスタンス ID に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement2",
            "Effect": "Allow",
            "Action": "connect:GetFederationToken",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "connect:InstanceId": "2fb42df9-78a2-2e74-d572-c8af67ed289b"
                }
            }
        }
    ]
}
```

   このポリシーを使用すると、複数のインスタンスに対してフェデレーションを有効化することができます。リストされたインスタンス ID が括弧で囲まれていることに注意してください。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement2",
            "Effect": "Allow",
            "Action": "connect:GetFederationToken",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "connect:InstanceId": [
                    "2fb42df9-78a2-2e74-d572-c8af67ed289b",
                    "1234567-78a2-2e74-d572-c8af67ed289b"]
                }
            }
        }
    ]
}
```

4. ポリシーを作成したら、[Next: Review] を選択します。トピック「SAML 2.0 フェデレーション用のロールの作成 (コンソール)」にある手順「SAML ベースのフェデレーション用のロールを作成するには」のステップ 10 に戻ります。

3. ネットワークを AWS の SAML プロバイダーとして設定します。詳細は、「Enabling SAML 2.0 Federated Users to Access the AWS Management Console (SAML 2.0 でフェデレーションしたユーザーによる AWS マネジメントコンソールへのアクセスを可能にする)」を参照してください。
4. 認証レスポンス用の SAML アサーションを設定します。詳細については、「認証レスポンスの SAML アサーションを設定する」を参照してください。
5. ID プロバイダーのリレーステートを、Amazon Connect インスタンスをポイントするように設定します。リレーステートに使用する URL は、次のとおりです。

   `https://region-id.console.aws.amazon.com/connect/federate/instance-id`

   region-id を、Amazon Connect インスタンスを作成したリージョン名 (たとえば、米国東部を指す us-east-1) で置き換えます。*instance-id* をインスタンスのインスタンス ID で置き換えます。

   > Note
   >
   > インスタンスのインスタンス ID を検索するには、Amazon Connect コンソールでインスタンスエイリアスを選択します。[概要] ページに表示される [インスタンス ARN] の "/instance" に続く数字および文字一式がインスタンス ID です。たとえば、以下のインスタンス ARN では、178c75e4-b3de-4839-a6aa-e321ab3f3770 の部分がインスタンス ID です。
   > arn:aws:connect:us-east-1:450725743157:instance/178c75e4-b3de-4839-a6aa-e321ab3f3770

リレーステートの URL で送信先を使用する

ID プロバイダーのリレーステートを設定する際、URL で destination 引数を使用すると、ユーザーを Amazon Connect インスタンスの特定のページにナビゲートすることができます。たとえば、エージェントのログイン時に直接 CCP を開くリンクを使用します。ユーザーには、インスタンス内の該当ページへのアクセス権限を付与するセキュリティプロファイルが割り当てられていなければなりません。たとえば、エージェントを CCP に送信するには、次のような URL をリレーステートに使用します。URL 内の送信先の値には URL エンコードを使用する必要があります。

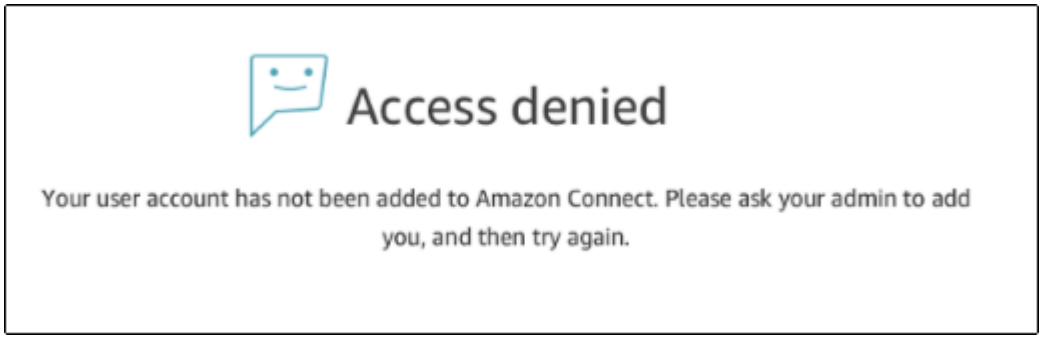
```
https://us-east-1.console.aws.amazon.com/connect/federate/instance-id?
destination=%2Fconnect%2Fccp
```

ユーザーを Amazon Connect インスタンスに追加する

インスタンスにユーザーを追加するときは、ユーザー名が既存のディレクトリ内のユーザー名と完全に一致することを確認してください。名前が一致しない場合、そのユーザー名を持つユーザーアカウントが

Amazon Connect に存在しないことになるため、ユーザーは、ID プロバイダーにログインすることはできても Amazon Connect にはログインできません。ユーザーは、[ユーザー管理] ページで手動で追加するか、CSV テンプレートを使って一括アップロードします。ユーザーを Amazon Connect に追加したら、セキュリティプロファイルや、他のユーザー設定を割り当てることができます。

ユーザーが ID プロバイダーにログインしたが、同じユーザー名を持つアカウントが Amazon Connect に存在しない場合は、次のように [アクセスが拒否されました] というメッセージが表示されます。



テンプレートを使ってユーザーを一括アップロードする

ユーザーをインポートするには、CSV ファイルに追加します。その後、CSV ファイルをインスタンスにインポートすると、そのファイルにすべてのユーザーが追加されます。CSV ファイルをアップロードしてユーザーを追加する場合は、SAML ユーザーのテンプレートを必ず使用してください。Amazon Connect の [ユーザー管理] を参照してください。SAML ベースの認証用には、別のテンプレートを使用します。テンプレートを以前ダウンロードしたことがある場合も、SAML ベースの認証を使ってインスタンスを設定した後、[ユーザー管理] ページで提供されているバージョンをダウンロードしてください。テンプレートに、E メールやパスワードの列を含めることはできません。

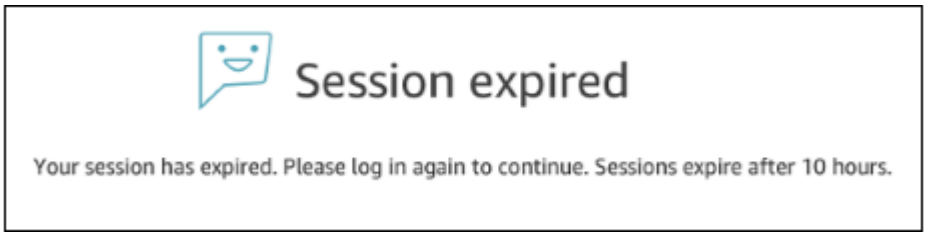
SAML ユーザーログインとセッションの長さ

Amazon Connect で SAML を使用する場合、ユーザーは、ID プロバイダー (IdP) から Amazon Connect にログインする必要があります。IdP は AWS と統合するように設定されています。認証後、セッションのトークンが作成されます。ユーザーは Amazon Connect インスタンスにリダイレクトされ、シングルサインオンによって Amazon Connect に自動ログインします。

ベストプラクティスとして、Amazon Connect の使用を終了したユーザーがログアウトできるよう、Amazon Connect ユーザーに対してプロセスを定義することが大切です。ユーザーは、Amazon Connect と ID プロバイダーの両方からログアウトする必要があります。そうしないと、そのセッションのトークンがセッションの長さ (デフォルトでは 10 時間) にわたって有効であるため、同じコンピュータに次にログインした人物がパスワードなしで Amazon Connect にログインできることになります。

セッションの有効期限について

Amazon Connect セッションの有効期限は、ユーザーのログインから 10 時間後に切れます。10 時間後、ユーザーは、通話中であっても自動的にログアウトされます。エージェントが 10 時間以上ログインしたままになっている場合は、期限が切れる前にセッショントークンを更新する必要があります。新しいセッションを作成するには、エージェントは Amazon Connect および IdP からログアウトし、再度ログインします。そうすれば、トークンで設定されているセッションタイマーがリセットされるため、エージェントが顧客との通話中にログアウトされてしまう事態を防ぐことができます。ログインしているユーザーのセッションの有効期限が切れると、次のようなメッセージが表示されます。ユーザーが Amazon Connect を再度使用するためには、ID プロバイダーにログインする必要があります。



現在の電話番号を移植する

米国国内で使用している現在の電話番号を Amazon Connect で使用するには、番号を Amazon Connect に移すためのサポートチケットを送信します。Amazon Connect チームによってリクエストが処理され、番号を移すプロセスがサポートされます。

電話番号の移植は、必要な情報を送信してから通常 2 ~ 4 週間かかります。必要な時間は、リクエストの複雑さと現在ご利用中の業者によって異なります。通常、フリーダイヤル番号の移植や、大量の番号を一度に移植するリクエストでは、地域の直通ダイヤル番号の移植よりも時間がかかります。

移送の完了を待つ間にサービスを試せるよう、Amazon Connect 用の電話番号を選択することをお勧めします。

現在の電話番号を Amazon Connect に移植するには

1. Amazon Connect コンソール (https://console.aws.amazon.com/connect/) を開きます。
2. 番号の移植先である Amazon Connect インスタンスを作成したときと同じアカウントを使ってログインします。
3. [サポート]、[サポートセンター] の順に選択します。
4. [サポートセンター] ページで、[Create Case (ケースの作成)] を選択します。
5. 以下のフィールドに値を入力します。
   - [Regarding (内容)] では、[Service Limit Increase (サービスの上限緩和を申請する)] を選択します。
   - [Limit Type (制限のタイプ)] で、[Connect (接続)] を選択します。
   - [Region (リージョン)] リストで、Amazon Connect インスタンスを作成したリージョンを選択します。
   - [Limit (制限)] で、[Phone Number Porting (電話番号の移植)] を選択します。
   - [New limit value (新しい制限値)] には、移植する電話番号の数を入力します。
   - [Use Case Description (申請理由の説明)] には、番号のタイプ (直通ダイヤルインなのか無料通話番号なのか)、現在のキャリア、現在の電話サービスを変更する権限を持つ人の連絡先情報など、リクエストに関する情報をできるだけ多く含めてください。不明な情報は、入力しなくてもかまいません。
6. フォームの残りを記入し、[送信] を選択します。

電話番号の移植について

当社では、現在の電話番号を Amazon Connect に移植する方にできるだけのサポートを提供しています。ただし、多くのステップは通信キャリアによって実施されます。

当社は、お客様がその番号を移植する権限をお持ちかどうかを検証するために必要な情報を収集します。その情報をお客様のこれまでのキャリアに渡し、新しいキャリアと協力して番号の移植を完了させます。どのキャリアも、独自のプロセスと要件に従って番号の移送を行っています。これまでのキャリアによって、お客様がその電話番号の所有者であり、移植する権限を持つことが検証されるまで、番号は移植され

ません。これまでのキャリアが番号の移植リクエストを承認して初めて、新しいキャリアによる番号のプロビジョニングが可能になります。それが完了したら、Amazon Connect チームが、移植された番号を使用するよう Amazon Connect インスタンスを設定します。

移植プロセスのステップは、次のとおりです。

1. 電話番号を移植するためのサポートチケットを送信します。
2. 番号の移植可能性を確認します。Amazon Connect チームが、リクエストされている番号を現在のキャリアから移植することが可能かどうか、確認します。その後、お客様に次のステップについてご連絡するか、リクエストされた番号が移植できない場合はその旨を通知します。
3. Letter of Authorization/Agency (LOA) に入力します。LOA フォームに入力する際、入力した情報が現在のキャリアに登録されている情報と一致している必要があります。情報が一致しないと、番号の移植が遅れる可能性があります。LOA フォームは、現在のキャリアに対し、電話番号を解放して移植を許可する権限を与えます。番号の移植が可能な場合は、番号のタイプにあった LOA フォームが提供されます。ローカル番号、直通ダイヤルイン (DID) 番号、無料通話番号のそれぞれに合わせてフォームが用意されています。複数の番号を異なるキャリアから移植する場合は、キャリアごとに個別のフォームに必要事項を入力します。

   LOA フォームには、次のような項目が含まれます。
   - 移植する番号
   - 現在のキャリアに関する情報 (通話料金の請求書など)
   - 電話サービスを変更する権限を持つ人の連絡先情報
4. 移植を開始するために、Amazon Connect チームがお客様に代わって LOA を Amazon Connect 用のキャリアに送信します。新しいキャリアが、現在のキャリアと協力して番号を自分のサービスに移します。このステップには、通常 3 ~ 5 営業日かかります。

   現在のキャリアは、リクエストを検証し、承認した時点で、番号を Amazon Connect に移植する日付を決定します。

   LOA の情報が間違っている、または不足しているなどの理由で現在のキャリアが移植のリクエストを拒否した場合、Amazon Connect チームがお客様に連絡し、キャリアに送信する新たな LOA を請求します。

現在のキャリアから日付が通知されたら、当社は、そのおよそ 1 日前に Amazon Connect インスタンスへの番号の追加を開始します。

CRM との統合

Amazon Connect は、Salesforce や Zendesk といった CRM と統合できます。統合により、任意の CRM でコンタクトセンターが起動できるようになり、既存のユーザーベースを維持し、Amazon Connect クラウドベースのインフラストラクチャを使用することができます。

Contact Control Panel (CCP) を CRM に統合するには、Amazon Connect Contact Streams を参照してください。完了したら、オリジンの URL をインスタンス設定に追加します。これによって、Amazon Connect と CRM の間の通信が可能になります。詳細については、「アプリケーション統合 (p. 23)」を参照してください。

Amazon Connect インスタンスの削除

Amazon Connect インスタンスが不要になった場合には、削除することができます。インスタンスを削除すると、そのインスタンスのために要求された電話番号が解放されます。インスタンスに関連付けられたすべての設定、データ、メトリクス、レポートが失われます。

Important

インスタンスの削除を元に戻すことはできず、削除されたインスタンスの設定やデータを復元することはできません。

Amazon Connect インスタンスを削除するには

1. Amazon Connect コンソール (https://console.aws.amazon.com/connect/) を開きます。
2. インスタンスのチェックボックスを選択し、[削除] を選択します。
3. プロンプトが表示されたら、インスタンスの名前を入力し、[削除] を選択します。

アジアパシフィック (東京) リージョン の Amazon Connect

アジアパシフィック (東京) リージョン に作成した Amazon Connect インスタンスの電話番号を取得するために必要な手順は、他の AWS リージョンの電話番号を請求する手順とは異なります。インスタンスの電話番号を請求するには、このセクションの情報を使用します。現在 Amazon Connect では、アジアパシフィック (東京) リージョン の電話番号の移植はサポートしていません。

アジアパシフィック (東京) リージョン で Amazon Connect を使用するためのポートとプロトコルの要件

エージェントで Amazon Connect のソフトフォンを使用している場合は、CCP が実行されているネットワークと、インスタンスを作成したリージョンの Amazon Connect の間の双方向のトラフィックを許可する必要があります。アジアパシフィック (東京) リージョン リージョンに作成したインスタンスに必要なアドレスには、次の内容が含まれます。

プロトコル	Port	Transport Layer	IP 範囲
HTTP	80	TCP	AWS EC2 と CLOUDFRONT の範囲は、https://ip-ranges.amazonaws.com/ip-ranges.json にあります。
HTTPS	443	TCP	AWS EC2 と CLOUDFRONT の範囲は、https://ip-ranges.amazonaws.com/ip-ranges.json にあります。
TURN/STUN	3478 および 49152-65535	UDP	AMAZON_CONNECT の範囲は、https://ip-ranges.amazonaws.com/ip-ranges.json にあります。
TURN 中継メディア	80 および 443	UDP および TCP	AMAZON_CONNECT の範囲は、https://ip-ranges.amazonaws.com/ip-ranges.json にあります。

アジアパシフィック (東京) リージョン で Amazon Connect を使用する

Amazon Connect では、アジアパシフィック (東京) リージョン に作成されたインスタンスでは、次の電話番号をサポートしています。

- 直通ダイヤル (DID) 番号 — DID 番号は市内局番とも呼ばれます。
  - 050 プレフィックス番号。
  - 03 プレフィックス番号 (東京)。現時点で Amazon Connect では、日本の他の都市の電話番号は提供されていません。

    03 プレフィックスがついた電話番号を取得するには、現住所が東京にあることを確認できるドキュメントを提出する必要があります。詳細については、次のセクションを参照してください。
- 通話料無料番号
  - 0120 プレフィックス番号。
  - 0800 プレフィックス番号。

  Note

  Amazon Connect のフリーダイヤル番号を取得すると、日本の他のフリーダイヤルと同様に、03 というプレフィックスを含む対応する DID 番号はありません。DID 番号を使用する場合は、Amazon Connect で取得できます。

アジアパシフィック (東京) リージョン の Amazon Connect インスタンスの電話番号を取得する方法

050 プレフィックスは、Amazon Connect 内で直接取得できます。東京の 03 プレフィックスの電話番号を取得する場合は、日本の規制要件に従って、インスタンス用に 03 プレフィックスの電話番号をリクエストするために Amazon Connect サービス上限緩和申請を提出する必要があります。承認プロセスの一環として、東京に現住所があることを確認するための住所に関するドキュメントの証明を提出する必要があります。住所の検証に必要なドキュメントについては、このトピックの後半で説明します。

リクエストの処理を待っている間に、インスタンス用に 050 プレフィックスの番号を取得できます。これで、Amazon Connect の設定方法および使用方法を理解しやすくなります。03 プレフィックス番号のサービス制限の引き上げが承認されたら、ステップ 6 に従ってプレフィックス番号「3」を検索して取得することができます。サービス制限の引き上げが承認されたら、その特定のアカウントの [電話番号の取得] ページで 03 のプレフィックス番号を追加取得できます。別のサポートケースを開く必要はありません。

アジアパシフィック (東京) リージョン で作成した電話番号をインスタンス向けに取得するには、以下のステップを行います。

1. Amazon Connect コンソール (https://console.aws.amazon.com/connect/) を開きます。

   AWS アカウントにサインインする必要がある場合があります。リージョンとして アジアパシフィック (東京) が選択されていることを確認します。
2. Amazon Connect コンソールページで、電話番号を請求するインスタンスの [アクセス URL] を選択します。
3. Amazon Connect の管理者セキュリティプロファイルが割り当てられているアカウントを使用して、インスタンスにログインします。

4. Amazon Connect ダッシュボードで、電話番号をまだ請求していない場合は、ステップ 5 に従います。電話番号を請求済みで、追加請求する場合は、ステップ 6 に進みます。
5. インスタンスの電話番号をまだ請求していない場合は、[開始] を選択して次のステップに従います。インスタンスの電話番号を請求済みで、追加請求する場合は、次のステップにスキップします。

   i. [電話番号の取得] ページで、電話番号を請求する国を選択します。

      アジアパシフィック (東京) リージョン のインスタンス向けに取得するには、050 プレフィックスの電話番号を使用することができます。東京の 03 プレフィックス番号を取得するには、「Amazon Connect サービス上限緩和申請」を送信する必要があります。

   ii. 取得する電話番号のタイプ ([直通ダイヤル] または [料金無料通話]) を選択します。

   iii. インスタンスで使用する電話番号を [電話番号] ドロップダウンメニューから選択します。

   iv. [次へ] を選択します。

      次のメッセージが表示された場合は、リクエスト承認して、指定されたリンクを使用して選択された電話番号を取得する必要があります。

      選択された国で電話番号を取得するには、その国の有効な事業所住所を入力する必要があります。有効な事業所住所を指定せずに取得した電話番号は取り消される場合があります。住所を入力するには、サポートケースを作成してください。今すぐサポートケースを作成するには、ここをクリックします。

   v. テストコールで、電話番号がインスタンスで正しく動作することを確認するには、このページのガイダンスに従うか、[ここではスキップ] を選択します。
6. インスタンスの電話番号を取得済みで追加番号を取得する場合は、[電話番号の表示] を選択し、次のステップに従います。

   i. [電話番号の管理] ページで [電話番号の取得] を選択します。

   ii. [電話番号の取得] ページで、取得する電話番号のタイプ ([料金無料通話] または [DID (直通ダイヤル)]) のタブを選択します。

   iii. 電話番号を取得するドロップダウンメニューから国を選択します。その国で使用できる数字が最大 5 つ表示されます。特定のプレフィックスから電話番号を検索するには、プレフィックスのすべてまたは一部をプレフィックスフィールドに入力します。そのプレフィックスが使用可能な番号がある場合は、そのページに表示されます。

   iv. インスタンス用に取得する電話番号を選択します。

   v. 後で分かりやすいように、電話番号の説明を入力します (オプション)。

   vi. その電話番号を問い合わせフローに関連付けるには、[問い合わせフロー/IVR] ドロップダウンメニューを選択します。電話番号をフローと関連付けたら、その電話番号のインスタンスに着信があると、選択した問い合わせフローが呼び出されます。

03 プレフィックス番号の住所証明に関する要件

Amazon Connect インスタンスに使用するために東京の 03 プレフィックス番号の取得リクエストを送信する場合は、次のように、日本の規制に従って、住所証明に関する次の書類を提出する必要があります。

- Amazon Connect インスタンスを作成するために使用される AWS アカウントが個人向けのものである場合は、電話番号が付与されている都市と一致する住所が文書に記載されている、政府発行の有効な身分証明書 (個人識別カード、パスポート、運転免許証など) を提出する必要があります。
- 企業用の AWS アカウントを使用してインスタンスを作成した場合、その組織の代表者は以下の両方を提出する必要があります。
  - 政府発行の有効な身分証明書 (例: 国民 ID カード、パスポート、運転免許証)。電話番号が付与されている都市と一致する住所が文書に記載されている必要があります。

- 以下のいずれかの文書。電話番号が付与されている都市と一致する住所が文書に記載されている必要があります。たとえば、公益法人、法務省からの企業登録証明書、国または地方の税務申告書、社会保障支払の領収書などの政府機関への支払い済み領収書などがあります。

これらの文書のコピーを番号のサポートリクエストとあわせて提出するか、AWS サポートからのリクエスト時に提出します。リクエストを送信したら、AWS サポートはそれを確認し、住所の確認が取れたか、詳細情報が必要になるとそのチケットをクローズします。リクエストの処理が完了した時点で、AWS サポートより結果が送信されます。AWS サポートがチケットを解決し、住所が確認されたら、上記のステップ 6 に従って、東京のプレフィックス番号 03 を取得することができます。

Amazon Connect インスタンスを設定する

AWS マネジメントコンソール を使用して、Amazon Connect インスタンスを設定できます。インスタンスの設定にアクセスするには、[インスタンスエイリアス] 列でインスタンスの名前を選択します。

設定

概要

概要 セクションには、Amazon Connect インスタンスに関する以下の情報が表示されます。

- インスタンス ARN— インスタンスの ARN です。インスタンスのインスタンス ID は、ARN に含まれており、instance/ 後の値です。たとえば、次のインスタンス ARN のインスタンス ID は df9e742b-310b-4eb2-a062-31bc99177ed4 です。

  ```
  arn:aws:connect:us-east-1:361814831152:instance/df9e742b-310b-4eb2-
  a062-31bc99177ed4
  ```
- ディレクトリ— インスタンスのインスタンスエイリアスです。
- ログイン URL— インスタンスのコンタクトセンターに直接ログインするのにブラウザで使用する URL です。

  エージェント (エージェントのセキュリティプロファイルのみが割り当てられているユーザー) が、この URL を使用して Amazon Connect にログインしようとすると、 "Error 403! (Forbidden) がそのページに表示されます。エージェントは、ページの右上にある電話アイコンを選択することによって、問い合わせコントロールパネル (CCP) をそのまま表示できます。

Login as administrator ボタンを使用して、完全な管理者アクセス許可を持つ AWS アカウントを使用してインスタンスにログインできます。これは、管理者アカウントのパスワードを忘れた場合、または Amazon Connect 設定を更新する必要がある場合に便利です。

テレフォニー

Amazon Connect インスタンスへの着信通話を受けるかどうか、そのインスタンスからの発信通話を許可するかどうかを選択します。セキュリティプロファイルを使用して、アウトバウンドコールを有効または無効にするようにアクセス許可を設定できます。

データストレージ

通話記録やレポートなどのデータは、Amazon S3 バケットに安全に保存されます。セットアップ中に、デフォルトの Amazon S3 バケットが作成され、AWS Key Management Service を使用して暗号化されます。このバケットおよびキーは、通話記録とレポートの両方で使用されます。または、通話記録とレポートで別々のバケットおよびキーを使用することもできます。

Amazon Connect の通話記録は wav ファイルとして保存され、8 kHz パルス符号変調 (PCM) 形式で再生されます。

データストレージの設定を更新する前に、Amazon S3 および AWS KMS について理解しておきます。

データストレージの設定を更新するには

1. Amazon Connect コンソール (https://console.aws.amazon.com/connect/) を開きます。
2. [インスタンスエイリアス] で、インスタンスの名前を選択します。
3. ナビゲーションペインで、[データストレージ] を選択します。
4. 以下の手順のステップでは、各データストレージの設定について説明します。

[通話記録] 設定の更新

1. [通話記録] で、[編集] を選択します。
2. 通話記録を有効にするには、[通話記録の有効化] をオンにします。
3. 以下のいずれかを行います。
   - [新しい S3 バケットの作成 (推奨)] を選択します。
     a. バケットの [名前] を入力します。
     b. 必要に応じて、バケットの [パスのプレフィックス] を入力します。プレフィックスを使用すると、S3 コンソールでバケットを簡単に識別することができます。
     c. 通話記録の暗号化を有効にするかどうかを選択します。有効にした場合は、インスタンスの通話記録の暗号化に使用する KMS マスターキーを選択します。
     d. [通話記録] で [保存] を選択します。
   - [既存の S3 バケットを選択します] を選択します。
     a. 通話記録に使用するバケットを [名前] ドロップダウンリストから選択します。
     b. 必要に応じて、使用する [パスのプレフィックス] を入力します。
     c. 通話記録の暗号化を有効にするかどうかを選択します。有効にした場合は、インスタンスの通話記録の暗号化に使用する [KMS マスターキー] を選択します。
     d. [通話記録] で [保存] を選択します。
4. [Save] を選択して変更を保存します。

[ライブメディアストリーミング] の設定

1. [ライブメディアストリーミング] で [編集] を選択します。
2. [ライブメディアストリーミングの有効化] を選択します。
3. インスタンス用に作成された Kinesis ビデオストリームに使用する [プレフィックス] を入力します。プレフィックスを使用すると、データが送信された後に必要なストリームを識別しやすくなります。
4. Kinesis に送信されたデータの暗号化に使用する KMS マスターキーを選択します。

5. [データ保持期間] の数値と単位を指定します。[データが保持されていません] を選択した場合、データは保持されず、すぐに使用する場合にのみ使用できます。
6. [ライブメディアストリーミング] で [保存] を選択します。
7. [保存] (ページの下部) を選択します。

[エクスポートされたレポート] の設定

1. [エクスポートされたレポート] で、[編集] を選択します。
2. エクスポートされたレポートを有効にするには、[エクスポートされたレポートの有効化] をオンにします。
3. 以下のいずれかを行います。
   - [新しい S3 バケットの作成 (推奨)] を選択します。
     a. バケットの [名前] を入力します。
     b. 必要に応じて、バケットの [パスのプレフィックス] を入力します。プレフィックスを使用すると、S3 コンソールでバケットを簡単に識別することができます。
     c. エクスポートされたレポートを有効にするかどうかを選択します。有効にした場合は、インスタンスの通話記録の暗号化に使用する KMS マスターキーを選択します。
     d. [通話記録] で [保存] を選択します。
   - [既存の S3 バケットを選択します] を選択します。
     a. エクスポートされたレポートに使用するバケットを [名前] ドロップダウンリストから選択します。
     b. 必要に応じて、使用する [パスのプレフィックス] を入力します。
     c. エクスポートされたレポートを有効にするかどうかを選択します。有効にした場合は、インスタンスの通話記録の暗号化に使用する [KMS マスターキー] を選択します。
     d. [エクスポートされたレポート] で、[保存] を選択します。
4. [保存] (ページの下部) を選択して変更を保存します。

データストリーミング

Amazon Connect から問い合わせ追跡レコード (CTR) およびエージェントイベントをエクスポートして、問い合わせの分析をリアルタイムで実行できます。データストリーミングでは、データは Amazon Kinesis に送信されます。

データストリーミングの有効化

1. Amazon Connect コンソール (https://console.aws.amazon.com/connect/) を開きます。
2. [インスタンスエイリアス] で、インスタンスの名前を選択します。
3. [データストリーミング] を選択します。
4. [データストリーミングの有効化] を選択します。
5. [Kinesis] または [Kinesis Data Firehose] を選択し、次のいずれかを実行します。
   - 既存の Amazon Kinesis ストリームまたは Kinesis Data Firehose を使用するには、ドロップダウンリストからそのリソースを選択します。
   - 新しいリソースを作成するには、[新しい Amazon Kinesis ストリームの作成] (または Kinesis Data Firehose) を選択します。

     これにより、Amazon Kinesis コンソールが表示され、Amazon Connect で使用するストリームまたは Firehose を作成できます。ストリームまたは firehose が作成されるまで待ってから、Amazon Connect コンソールに戻ります。

ページを再ロードして、作成したストリームまたは Firehose がリソースの選択で表示されたら、ストリームまたは Firehose を選択します。

Note

選択した Kinesis ストリームでサーバー側の暗号化を有効にした場合、Amazon Connect は、Kinesis kms:GenerateDataKey に対するアクセス許可を持たないため、そのストリームに発行することはできません。この問題を回避するには、通話記録またはスケジュールされたレポートの暗号化を有効にし、KMS を使用して暗号化に使用するカスタマーマスターキー (CMK) を作成してから、Kinesis に送られたデータを暗号化する適切なアクセス許可を Amazon Connect が持てるように、Kinesis データストリーム用に、通話記録またはスケジュールされたレポートの暗号化に使用するのと同じ CMK を選択します。カスタマーマスターキー (CMK) KMS の作成の詳細については、「キーの作成」を参照してください。

6. [Save] を選択します。

アプリケーション統合

特定のインスタンスに対して CCP を埋め込むすべてのドメインは、そのインスタンスへのクロスドメインアクセスに対して明示的にホワイトリストに登録される必要があります。たとえば Salesforce と統合するには、Salesforce Visualforce ドメインをホワイトリストに登録する必要があります。

ドメイン URL をホワイトリストに登録するには

1. Amazon Connect コンソール (https://console.aws.amazon.com/connect/) を開きます。
2. [インスタンスエイリアス] で、インスタンスの名前を選択します。
3. ナビゲーションペインで、[アプリケーション統合] を選択します。
4. [オリジンの追加] を選択します。
5. URL を入力して [追加] を選択します。

対応フロー

問い合わせフローにより、最初から最後までのコンタクトセンターでのカスタマーエクスペリエンスが定義されます。AWS マネジメントコンソール を使用して、次のように問い合わせフローを設定できます。

セキュリティキー

Amazon Connect は、公開鍵暗号方式を使用して、問い合わせフローにより収集された機密データを暗号化できます。X.509 証明書を問い合わせフロー内で提供して、保存された顧客入力システム属性を使用して収集されたデータを暗号化します。この機能を使用するには、署名キーを .pem 形式でアップロードする必要があります。署名キーを使用して、問い合わせフロー内で使用される証明書の署名を確認します。

Note

ローテーションを実行するには、最大 2 つの署名キーを同時にアクティブにしなければならない場合があります。

問い合わせフロー内で暗号化されたデータは、保存された顧客入力システム属性を通じて利用可能になります。AWS Encryption SDK はシステム内でこのデータの復号に使用することができます。詳細については、『AWS 暗号化 SDK 開発者ガイド』を参照してください。

セキュリティキーを追加するには

1. Amazon Connect コンソール (https://console.aws.amazon.com/connect/) を開きます。

2. [インスタンスエイリアス] 列からインスタンスの名前を選択します。
3. ナビゲーションペインで、[問い合わせフロー] を選択します。
4. [キーの追加] を選択します。
5. [パブリックキーの内容] にパブリックキーの内容を貼り付け、[追加] を選択します。

Amazon Lex ボットをインスタンスに追加する

Amazon Lex では、顧客にとって自然な会話のやり取り (ボット) を構築でき、Alexa で利用されているのと同じ音声認識および自然言語理解テクノロジーを利用できます。Amazon Lex ボットを作成した後で、インスタンスに追加して問い合わせフローに統合できます。Amazon Connect インスタンスと同じリージョンまたは異なるリージョンからボットを追加できます。

Amazon Lex ボットをインスタンスに追加する

1. Amazon Connect コンソール (https://console.aws.amazon.com/connect/) を開きます。
2. [インスタンスエイリアス] 列からインスタンスの名前を選択します。
3. ナビゲーションペインで、[問い合わせフロー] を選択します。
4. [Amazon Lex] の [リージョン] ドロップダウンリストで、Amazon Lex ボットを作成したリージョンを選択します。

   選択したリージョンに、AWS アカウントに関連付けられたボットがある場合は、[ボット] ドロップダウンリストにそのボットが表示されます。選択したリージョンにボットがない場合、またはそのリージョンから追加する追加のボットがないときは、ドロップダウンメニューは無効になります。そのリージョンで選択して利用できるボットがないことを示すメッセージが表示されます。
5. [ボット] ドロップダウンメニューからボットを選択し、[+ Lex ボットの追加] を選択します。

新しいボットを作成するには、[新しい Lex ボットの作成] を選択して Amazon Lex コンソールを開きます。Amazon Lex が使用可能なリージョンを選択する必要がある場合があります。

インスタンスからボットを削除するには、削除するボットの横にある [削除] を選択します。

AWS Lambda 関数をインスタンスに追加する

問い合わせフローで使用する際に Lambda 関数を参照しやすくするにはインスタンスに追加したら、問い合わせフローでその関数を簡単に使用することができます。

Lambda 関数をインスタンスに追加する

1. Amazon Connect コンソール (https://console.aws.amazon.com/connect/) を開きます。
2. [インスタンスエイリアス] 列からインスタンスの名前を選択します。
3. ナビゲーションペインで、[問い合わせフロー] を選択します。
4. [AWS Lambda] で、インスタンスに追加する関数を [関数] ドロップダウンから選択します。
5. [+ Lambda 関数の追加] を選択します。この関数は、インスタンスに追加され、[Lambda 関数] に一覧表示されます。問い合わせフローでその ARN を使用して関数を参照できるように、名前の横にあるアイコンを選択して、その関数の ARN をクリップボードにコピーします。

関数のリストには、AWS アカウントの関数がすべて含まれています。アカウントに関数が存在しない場合、リストは空になります。新しい関数を作成するには、[新しい Lambda 関数の作成] を選択して AWS Lambda コンソールを開きます。

インスタンスから関数を削除するには、関数名の横にある [削除] を選択します。

問い合わせフローログ

[問い合わせフローログを有効にする] チェックボックスをオンにして、問い合わせフローログの Amazon CloudWatch への送信を開始します。問い合わせフローログの詳細については、「問い合わせフローログ」を参照してください。

Amazon Connect のサービスにリンクされたロールの使用

Amazon Connect は、AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用します。サービスにリンクされたロールは、Amazon Connect に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは、Amazon Connect による事前定義済みのロールであり、ユーザーに代わってサービスから AWS の他のサービスを呼び出すために必要なすべてのアクセス許可が付与されています。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がなくなるため、Amazon Connect の設定が簡単になります。Amazon Connect はこのサービスにリンクされたロールのアクセス許可を定義し、特に定義されている場合を除き、Amazon Connect のみがそのロールを引き受けます。定義されるアクセス権限には、信頼ポリシーやアクセス権限ポリシーなどがあり、そのアクセス権限ポリシーをその他の IAM エンティティにアタッチすることはできません。

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

Amazon Connect のサービスにリンクされたロールのアクセス許可

Amazon Connect では、サービスにリンクされたロールとして AWSServiceRoleForAmazonConnect_ – Grants Amazon Connect permission to access AWS resources on your behalf を使用します。

AWSServiceRoleForAmazonConnect_ サービスにリンクされたロールは、ロールを引き受ける上で次のサービスを信頼します。

- `connect.amazonaws.com`

ロールのアクセス許可ポリシーは、Amazon Connect が次のアクションを指定されたリソースで完了することを許可します。Amazon Connect の追加機能を有効にすると、サービスにリンクされたロールに追加のアクセス許可が追加され、これらの機能に関連付けられたリソースにアクセスできます。

- アクション: すべての Amazon Connect リソースの Amazon Connect アクションすべて `connect:*`。アクション?
- アクション: Amazon S3 `s3:GetObject`、`s3:GetObjectAcl`、`s3:PutObject`、`s3:PutObjectAcl`、`s3:DeleteObject`、`s3:GetBucke` (通話記録で指定された S3 バケット用)。

  `s3:PutObject`、`s3:PutObjectAcl`、`s3:GetObjectAcl` は、エクスポートされたレポートで指定されたバケットにも付与されます。
- アクション: Amazon Kinesis Data Firehose `firehose:DescribeDeliveryStream`、`firehose:PutRecord`、`firehose:PutRecordBatch` (エージェントイベントストリームおよび CTR で定義された配信ストリーム用)
- アクション: Amazon Kinesis Data Streams `kinesis:PutRecord`、`kinesis:PutRecords`、`kinesis:DescribeStream` (エージェントイベントストリームおよび CTR で指定されたストリーム用)
- アクション: Amazon Lex `lex:PostContent` (インスタンスに追加されたボット用)

- アクション: Amazon CloudWatch Logs
  `logs:CreateLogStream`、`logs:DescribeLogStreams`、`logs:PutLogEvents` (問い合わせフローのログ記録で指定された CloudWatch Logs グループ用)

IAM エンティティ (ユーザー、グループ、ロールなど) がサービスにリンクされたロールを作成、編集、削除できるようにするには、アクセス権限を設定する必要があります。詳細については、IAM ユーザーガイド の「サービスにリンクされたロールのアクセス許可」を参照してください。

Amazon Connect のサービスにリンクされたロールの作成

サービスにリンクされたロールを手動で作成する必要はありません。AWS マネジメントコンソール で create a new instance in Amazon Connect すると、 Amazon Connect によって、サービスにリンクされたロールが作成されます。

このサービスにリンクされたロールを削除した後で再度作成する必要が生じた場合は、同じ方法でアカウントにロールを再作成できます。サービスにリンクされたロールは、create a new instance in Amazon Connect すると Amazon Connect で再度自動的に作成されます。

[Amazon Connect - Full access] ユースケースでサービスにリンクされたロールを作成するには、IAM コンソールを使用します。IAM CLI または IAM API で、サービスにリンクされたロールをサービス名 (`connect.amazonaws.com`) で作成します。詳細については、『IAM ユーザーガイド』の「サービスにリンクされたロールの作成」を参照してください。このサービスにリンクされたロールを削除する場合、この同じプロセスを使用して、もう一度ロールを作成できます。

Amazon Connect のサービスにリンクされたロールの編集

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

Amazon Connect のサービスにリンクされたロールの削除

AWSServiceRoleForAmazonConnect_ ロールを手動で作成する必要はありません。AWS マネジメントコンソール で delete your Amazon Connect instance すると、 Amazon Connect によって、リソースがクリーンアップされ、サービスにリンクされたロールは削除されます。

Amazon Connect のサービスにリンクされたロールでサポートされたリージョン

Amazon Connect は、サービスを利用できるすべてのリージョンで、サービスにリンクされたロールの使用をサポートします。詳細については、「AWS Regions and Endpoints」を参照してください。

Amazon Connect インスタンスの CloudWatch メトリクス

Amazon Connect は、CloudWatch メトリクスにインスタンスに関するデータを送信し、Amazon Connect 仮想サポートセンターの CloudWatch メトリクスを収集、表示、および分析を行ないます。主要な運用メトリクスを監視してアラームを設定するため、このデータを使用できます。サポートセンターに関するデータは、1 分毎に CloudWatch へ送信されます。

CloudWatch メトリクスダッシュボードを表示するとき、表示データの更新間隔を指定できます。ダッシュボードに表示される値は、定義した更新間隔値を反映しています。たとえば、[Refresh interval] を [1 minute] に設定した場合、表示される値は 1 分間に対するものです。更新間隔を 10 秒に選ぶことはできますが、Amazon Connect は 1 分間に複数回のデータ送信は行いません。CloudWatch に送信されたメトリクスは 2 週間利用可能で、その後は破棄されます。CloudWatch のメトリクスの詳細については、「Amazon CloudWatch ユーザーガイド」を参照してください。

CloudWatch に送信されたAmazon Connect メトリクス

`AWS/Connect` 名前空間には、次のメトリクスが含まれます。

CallsBreachingConcurrencyQuota

インスタンスの同時アクティブ通話の上限を超えた音声通話数です。これは、上限を超えた通話数で、上限を超えた同時通話数ではありません。

単位: 個

CallBackNonDialableNumber

顧客の電話番号が、このインスタンスに発信通話が許可されていない国であるため、キューに入れられた顧客へのコールバックができなかった回数です。インスタンスに許可されている国は、サービスの制限によって定義されます。

単位: 個

CallRecordingUploadError

インスタンスに設定された、Amazon S3 バケットにアップロードできなかった通話録音数です。これは、インスタンスの Data Storage > Call Recordings 設定で指定されたバケットです。

単位: 個

CallsPerInterval

インスタンスで 1 秒あたりの受信と発信両方の音声通話数です。

単位: 個

ConcurrentCalls

ダッシュボードにデータが表示された時点でのインスタンス内の同時アクティブ音声通話数です。このメトリクスとして表示される値はダッシュボード表示時点での同時アクティブ通話数で、設定された更新間隔の間隔全体の合計値ではありません。エージェントへ接続されたアクティブな通話だけではなく、アクティブな音声通話すべてを含みます。

単位: 個

ConcurrentCallsPercentage

インスタンス内で使用された、同時アクティブ音声通話のサービスの制限の割合 (%) です。この値は、`ConcurrentCalls/ConfiguredConcurrentCallsLimit * 100` で計算されます。

単位: パーセント

ContactFlowErrors

問い合わせフローに対するエラー分岐が実行された回数です。

単位: 個

ContactFlowFatalErrors

システムエラーが原因で問い合わせフローが実行に失敗した回数です。

単位: 個

LongestQueueWaitTime

問い合わせがキューで待機した最長時間 (秒数) です。これは、CloudWatch ダッシュボードで選択された更新間隔 (1 分または 5 分など) 中にキューでの待機した時間の長さです。

単位: 秒

MissedCalls

選択された更新間隔 (1 分または 5 分など) 中にエージェントが通話できなかった音声通話数です。不在着信とは、エージェントが 20 秒以内に応答しなかった通話です。

単位: 秒

MisconfiguredPhoneNumbers

電話番号が問い合わせフローと関連付けられていないために失敗した通話数です。

単位: 個

PublicSigningKeyUsage

問い合わせフローのセキュリティキー (公開署名キー) が問い合わせフローの顧客入力を暗号化するため使用された回数です。

単位: 個

QueueCapacityExceededError

キューがいっぱいなため、拒否された通話の数。

単位: 個

QueueSize

キュー内の問い合わせの数。この値は、ダッシュボードがアクセスされた時点でのキュー内のコンタクト値の数を反映し、報告間隔の期間に対するものではありません。

単位: 個

ThrottledCalls

1 秒あたりの呼び出しレートが、サポートされる上限を超えたためにために拒否された音声呼び出しの数。呼び出しのレートを増やすには、インスタンスあたりの同時アクティブ呼び出しのサービス制限の引き上げをリクエストします。

単位: カウント

ToInstancePacketLossRate

10 秒ごとに報告される、インスタンス内の通話に対するパケット損失率です。各データポイントは 0 と 1 の間で、インスタンスでのパケット損失率を表します。

単位: パーセント

Amazon Connect CloudWatch メトリクスのディメンション

CloudWatchでは、ディメンションとは、メトリクスを一意に識別する名前/値のペアです。ダッシュボードでは、メトリクスはディメンション別にグループ化されます。以下のディメンションは、Amazon Connect メトリクスの CloudWatch ダッシュボードで使用されます。ダッシュボードでメトリクスを表示すると、データを含むメトリクスのみが表示されます。メトリクスが存在する更新間隔中にアクティビティがない場合は、インスタンスからのデータは、ダッシュボードに表示されません。以下のディメンションは、CloudWatch の Amazon Connect メトリクスで使用されます。

問い合わせフローメトリクスディメンション

問い合わせフロー別にメトリクスデータをフィルタリングします。以下のメトリクスが含まれます。

- CallRecordingUploadError
- ContactFlowErrors
- ContactFlowFatalErrors
- MisconfiguredPhoneNumbers
- PublicSigningKeyUsage

インスタンスメトリクスディメンション

インスタンス別にメタデータをフィルタリングします。以下のメトリクスが含まれます。

- CallsBreachingConcurrencyQuota
- CallsPerInterval
- ConcurrentCalls
- ConcurrentCallsPercentage
- MissedCalls
- ThrottledCalls

インスタンス ID、参加者、ストリームタイプ、接続タイプ

接続別にメトリクスデータをフィルタリングします。以下のメトリクスが含まれます。

- ToInstancePacketLossRate

キューメトリクスディメンション

キュー別にメトリクスデータをフィルタリングします。以下のメトリクスが含まれます。

- CallBackNonDialableNumber
- LongestQueueWaitTime
- QueueCapacityExceededError
- QueueSize

Amazon Connect で AWS Lambda 関数を使用する

Amazon Connect は お客様のシステムと連携して、問い合わせフロー内のさまざまなパスを動的に使用することができます。これを実現するには、Lambda 関数を呼び出して、問い合わせフロー内に結果を取得し、お客様独自のサービスを呼び出すか、他の AWS データストアまたはサービスと連携します。

AWS Lambda の詳細については、AWS Lambda Developer Guide を参照してください。

問い合わせフローからの Lambda 関数の呼び出し

Amazon Connect から Lambda 関数を呼び出すのに必要な手順は以下のとおりです。

1. Lambda 関数を作成し、Amazon Connect でこの関数を呼び出せるようにするトリガーポリシーを定義します。
2. 問い合わせフローの [AWS Lambda 関数を呼び出す] ブロックで Lambda 関数の ARN を使用します。
3. Lambda 関数コードを設定して、問い合わせフローから送信された JSON イベントを解析し、実行するビジネスロジックを定義します。
4. 設定をテストして、Lambda 関数が正しい JSON レスポンスを返すことを確認します。
5. 問い合わせフローで使用する Lambda から返される属性値を使用します。

Lambda 関数を作成し、トリガーポリシーを設定する

Lambda 関数にリソースポリシーが設定されているときは、Amazon Connect は AWS アカウントで Lambda 関数を正常に呼び出すことができます。詳細については、『AWS Lambda Developer Guide』の「AWS Lambda でリソースベースのポリシーを使用する」を参照してください。

開始するには、Lambda 関数を作成し、関数名を書き留めます。Lambda 関数の作成の詳細については、「シンプルな Lambda 関数を作成する」を参照してください。

次の add-permission コマンドを使用し、以下の情報を使用してリソースポリシーを作成します。

```
aws lambda add-permission --function-name function:my-lambda-function --statement-id 1 \
     --principal connect.amazonaws.com --action lambda:InvokeFunction --source-
account 123456789012 \
     --source-arn arn:aws:connect:us-east-1:123456789012:instance/def1a4fc-ac9d-11e6-
b582-06a0be38cccf
```

このコマンドでは、以下の入力を使用します。

- Lambda 関数の名前 (**my-lambda-function** など)
- Amazon Connect インスタンスの ARN (**arn:aws:connect:us-east-1:123456789012:instance/def1a4fc-ac9d-11e6-b582-example** など)

  インスタンスの ARN を確認するには、Amazon Connect コンソールを開き、[インスタンスエイリアス] を選択して [概要] ページを開きます。

- Amazon Connect インスタンスの AWS アカウント ID (**123456789012** など)

問い合わせフローで Lambda 関数を呼び出す

問い合わせフローから Lambda 関数を呼び出すには、問い合わせフローに [AWS Lambda 関数を呼び出す] ブロックを追加し、問い合わせフローのプロパティで [関数の ARN] の値として作成した関数の ARN を追加します。関数の ARN は、AWS Lambda コンソールの https://console.aws.amazon.com/lambda/ で表示できます。

AWS Command Line Interface で次のコマンドを実行して関数の ARN を表示することもできます。

```
aws lambda get-function --function-name my-lambda-function
```

[AWS Lambda 関数を呼び出す] ブロックで、呼び出されたときに Lambda 関数に送られるキーと値のペアである [関数入力パラメータ] を追加できます。関数の [タイムアウト] の値を指定することもできます。

問い合わせフローから Lambda 関数を呼び出すたびに、進行中の問い合わせに関するデフォルトの一連の情報と、問い合わせフローに追加された [AWS Lambda 関数を呼び出す] ブロックの [関数入力パラメータ] で定義された追加の属性を渡します。

Lambda 関数への JSON リクエストの例を次に示します。

```
{
    "Details": {
        "ContactData": {
            "Attributes": {},
            "Channel": "VOICE",
            "ContactId": "4a573372-1f28-4e26-b97b-XXXXXXXXXXX",
            "CustomerEndpoint": {
                "Address": "+1234567890",
                "Type": "TELEPHONE_NUMBER"
            },
            "InitialContactId": "4a573372-1f28-4e26-b97b-XXXXXXXXXXX",
            "InitiationMethod": "INBOUND | OUTBOUND | TRANSFER | CALLBACK",
            "InstanceARN": "arn:aws:connect:aws-region:1234567890:instance/
c8c0e68d-2200-4265-82c0-XXXXXXXXXX",
            "PreviousContactId": "4a573372-1f28-4e26-b97b-XXXXXXXXXX",
            "Queue": "QueueName",
            "SystemEndpoint": {
                "Address": "+1234567890",
                "Type": "TELEPHONE_NUMBER"
            }
        },
        "Parameters": {
            "sentAttributeKey": "sentAttributeValue"
        }
    },
    "Name": "ContactFlowEvent"
}
```

このリクエストは次の 3 つのパートに分かれています。

- 問い合わせデータ— 問い合わせのたびに、Amazon Connect によって必ず渡されます。一部のパラメータは省略可能です。
- ユーザー属性— これらは、問い合わせフローの [問い合わせ属性の設定] ブロックの使用時など、以前に問い合わせに関連付けられていた属性です。このマップは、保存されている属性が何もない場合は空の場合もあります。
- パラメータ— これらは Lambda 関数を作成したときに定義されたこの呼び出しに固有のパラメータです。

Lambda 関数のレスポンスは、単純な Map *String String* である必要があります。このマップは最大で 32 k です。Lambda に到達できない場合、関数は例外をスローし、レスポンスが認識されないか、Lambda 関数が制限時間を超え、問い合わせフローは `Error` ラベルへジャンプします。次のコードは、Python Lambda 関数の例です。

Lambda 関数を設定する

Lambda 関数と Amazon Connect との間で属性を正しく渡すために、[AWS Lambda 関数を呼び出す] ブロックから送られた JSON リクエストを正しく解析し、適用する必要があるビジネスロジックを定義するように関数を設定します。JSON がどのように解析されるかは、関数に使用するランタイムによって異なります。たとえば、次の例は、sing Node.JS を使用して `sentAttributeKey` にアクセスする方法を説明しています。

```
var receivedAttribute = event['Details']['Parameters']['sentAttributeKey'];
```

関数のレスポンスを検証する

Lambda 関数から返された出力をテストして、Amazon Connect に返されたときに正常に使用されることを確認します。次の例は、Node.JS でのサンプルのレスポンスを示します。

```
exports.handler = function(event, context, callback) {

var resultMap = {
    Name:'CustomerName',
    Address:'1234 Main Road',
    CallerType:'Patient'
}

callback(null, resultMap);
}
```

またこの例は、Python を使用したサンプルのレスポンスを示します。

```
def lambda_handler(event, context):
resultMap = {"Name":"CustomerName","Address":"1234 Main Road","CallerType":"Patient"};
return resultMap;
```

関数から返される出力は、英数字、ダッシュ、アンダースコアのみが含まれる値を持つ、キーと値のペアのフラットオブジェクトである必要があります。ネストされた複雑なオブジェクトはサポートされません。返されるデータのサイズは、UTF-8 データの 32 KB 未満である必要があります。

次の例は、これらの Lambda 関数からの JSON 出力を示します。

```
{
    "Name": "CustomerName",
    "Address": "1234 Main Road",
    "CallerType": "Patient"
}
```

Lambda 関数のレスポンスを使用する

問い合わせフローで関数のレスポンスを使用するには 2 つの方法があります。Lambda から返される変数を直接参照するか、問い合わせ属性として関数から返される値を保存してから、保存された属性を参照することができます。Lambda からのレスポンスへの外部参照を使用する場合は、その参照は常に、最近呼び出された関数からのレスポンスを受け取ります。後続の関数が呼び出される前に関数からのレスポンス

を使用するには、レスポンスを問い合わせ属性として保存するか、次の関数にパラメータとして渡す必要があります。

直接 Lambda 属性にアクセスする

変数に直接アクセスする場合、それらは問い合わせフローブロックで使用できますが、問い合わせ追跡レコード (CTR) には含まれません。問い合わせフローブロックで直接これらの変数にアクセスするには、[AWS Lambda 関数を呼び出す] ブロックの後にブロックを追加してから、次の例に示すようにそれらの属性を参照します。

```
Name - $.External.Name
Address - $.External.Address
CallerType - $.External.CallerType
```

ソース属性に指定した名前が、Lambda から返されたキー名と一致することを確認します。

Lambda 変数を問い合わせ属性として保存する

変数を問い合わせ属性として保存すると、問い合わせフロー全体で使用でき、CTR に含まれるようになります。

問い合わせ属性として返された値を保存してから、それらを参照するには、問い合わせフローの [AWS Lambda 関数を呼び出す] ブロックの後で、[問い合わせ属性の設定] ブロックを使用します。[タイプ] で、[外部] を選択します。使用している例に従って、[宛先キー] を `returnedContactName` に設定し、[ソース属性] を `Name` に設定します。

アドレスを [ソース属性] として追加し、[宛先キー] として `returnedContactAddress` を使用します。次に、[ソース属性] として `callerType` を追加し、[宛先キー] に `returnedContactType` を使用します。

ソース属性に指定した名前が、Lambda から返されたキー名と一致することを確認します。

Amazon Connect と Salesforce との統合

Amazon Connect CTI アダプターのコア機能は、WebRTC によるブラウザベースの問い合わせコントロールパネル (CCP) を Salesforce 内に提供します。Amazon Connect の CTI 統合は、AWS 環境にデプロイされたマネージド型 Salesforce パッケージと AWS サーバーレスアプリケーションの 2 つのコンポーネントから構成されています。

これらのコンポーネントを使って、Amazon Connect サポートセンタープラットフォームと、トップクラスの顧客関係管理 (CRM) プラットフォームである Salesforce との間で緊密な統合を行なえます。プレビルドユーティリティのコレクションにより、この 2 つのプラットフォーム間を迅速に統合できます。AWS サーバーレスアプリケーションパッケージには、Amazon Connect が Salesforce と連携するために使用される一般的な Lambda 関数が含まれています。

アダプターについて

アダプターの重要な利点は以下のとおりです。

- Salesforce Omni と Amazon Connect 間でエージェント状態を同期
- コール属性の設定可能な表示を通じてエージェントに貴重な情報を提供
- 発信ダイヤリング自動化のために Amazon Connect Call Campaign Object を活用
- 通話タスクを自動的に作成し、適切な Salesforce オブジェクトに関連付け
- Amazon Connect 通話記録を Salesforce レコードに埋め込み
- エージェントの効率アップのために開いているタブを自動的にクリーンアップ
- Amazon Connect 問い合わせフロー内で、問い合わせやケースなど、さまざまな Salesforce オブジェクトの検索/作成/更新作業を簡単化。
- Salesforce Sales and Service Console に Classic と Lightning をサポート。

最初に Salesforce サンドボックスに本パッケージをインストールすることをお勧めします。パッケージがインストールされた後は、Salesforce 内で Salesforce サポートセンターのせっていが可能になります。

次に、Amazon Connect 内の Salesforce Visualforce ドメインをホワイトリストに登録するステップを行います。これで Amazon Connect インスタンスへクロスドメインでアクセスできるようになります。

このページはクイックセットアップガイドです。CTI アダプターの全機能の詳細な説明と設定については、「Amazon Connect CTI Adapter v3 for Salesforce インストレーションガイド」を参照してください。https://sfdc.co/Amazon-Connect からも始められます。なお、最新の CTI Adapter 機能のサポートは現在更新中です。

前提条件

次の前提条件を満たさないと、Amazon Connect CTI パッケージはインストールできません。

- Salesforce Classic、Salesforce Console、または Lightning Experience があること。
- Amazon Connect インスタンス (https://aws.amazon.com/connect/) を作成すること。

- Salesforce オムニチャネル が Salesforce org で有効になっていること。詳細については、オムニチャネルを有効にするをご覧ください。

ブラウザの互換性

Amazon Connect では、ソフトフォンの音声メディアストリーム用に WebRTC が、シグナリング用に Websockets が必要です。そのため、Google Chrome または Mozilla Firefox の最新バージョンを使用する必要があります。詳細については、「Amazon Connect よくある質問」ページを参照してください。

Salesforce と統合するには

1. Salesforce サンドボックスでマネージド型パッケージ Amazon Connect CTI アダプターをインストールします。
2. 次の適切なサポートセンター設定 (Amazon Connect CCP Adapter Classic、Console、または Lightning) のいずれかを編集します。

   - Amazon Connect CCP URL に、インスタンスの CCP URL を入力します (例 :https://instance.awsapps.com/connect/ccp)。
   - 電話番号フォーマットの国には、適切な 2 桁の ISO 国コードを指定します。
   - Salesforce ユーザーに [サポートセンターの設定] ページで、Amazon Connect CCP へのアクセス権を付与するには、[;Manage Call Center Users (サポートセンターユーザーの管理)] を選択します。この通話機能を利用するため有効にする Salesforce ユーザーを追加します。この機能を利用する場合は、必ず自分の Salesforce ユーザーアカウントを追加してください。
3. 「アプリケーションの統合 (p. 23)」の指示に従って、Salesforce Visualforce ドメインの URL をホワイトリストに加えます。URL を確認するには、設定で Visualforce ページを開きます。この URL は通常、次の形式です。

   https://amazonconnect.**your-instance-name**.visual.force.com
4. Amazon Connect インスタンスにログインします。
5. Salesforce を起動します。サイドパネル (Salesforce Classic の場合) または電話ツールバー (Salesforce Classic と Lightning Experience の場合) に、統合された CCP が表示されます。

よくある問題のトラブルシューティング

設定でエラーが発生した場合、以下のよくある問題を確認してください。

- Salesforce が iFrame をブロックしていないことを確認します。詳細については、「ヘッダーが有効でないときに Visualforce ページのクリックジャック保護を有効にする」を参照してください。
- Amazon Connect ユーザーには、エージェントのセキュリティプロファイルしか割り当てられていないことを確認します。
- Salesforce サポートセンターの電話番号フォーマット が次のパラメータを使って設定されていることを確認します。

  {"OPF":"0","NPF":"2 ######### ","Country":"2 #########
  #","NF":"International_plaintext","TNF":"(555) 123-4567"}
- Salesforce ユーザーがサポートセンターにアクセスできることを確認します。ユーザーのステータスを確認するには、サポートセンターユーザの管理を選択してください。
- ソフトフォンのレイアウト、スクリーンポップの下で、Single-matching record が詳細ページをポップに、Multiple-matching record がポップしてページを検索に設定されていることを確認してください。

- Salesforce Lightning Experience を使用していて、電話ツールバーアイコンが表示されない場合は、コンソール操作が有効か確認します。コンソール操作を有効にするには、Salesforce 設定コンソールで App Manager、Service Console (Lightning)、Edit を順に選択します。Edit ページで、App Options、App Navigation、Console Navigation を順に選択します。

Amazon Connect のトラブルシューティングとベストプラクティス

このガイドを使用して、Amazon Connect を使用するためのベストプラクティスを見極めます。また、正常に動作していない場合の情報をトラブルシューティングするためにも使用します。

このガイドのセクションは以下のとおりです。

Contact Control Panel を使用するベストプラクティス

このガイドには、CCP ソフトフォンに関する情報 (例: ベストプラクティスおよびトラブルシューティング) を含みます。ソフトフォン接続要件を満たせない、またはソフトフォンの問題が発生するワークステーションの場合、CCP にも外部デバイスにリダイレクトする機能が搭載されています。

このセクションのトピック:

エージェントのワークステーションの要件

コンタクトセンターのエージェントワークステーションは、大きく異なります。Amazon Connect CCP は、高レベルのジッタや高レイテンシーの環境に対応するよう構築されていますが、エージェントが使用するワークステーションのアーキテクチャ、コールを受ける場所や環境は、エクスペリエンスの質に影響を及ぼす可能性があります。

ワークステーションが電力不足の場合は、エージェントが発信者にサービスを提供するために必要なツールやリソースにアクセスしづらくなる可能性があります。また、負荷がかかっても、ユースケースに対して適切なマルチタスクを実行できるようにするには、ワークステーションのスコープ設定時のリソース要件に注意してください。エージェントと顧客のオーディオ体験で最良の結果を得るために、USB ヘッドセットの使用をお勧めします。または、エージェントの既存テレフォニーを使用して E.164 形式でコールを外部番号にリダイレクトすることもできます。

以下の値は、CCP のみを使用するワークステーションの最小システム要件です。リソースの競合を避けるために、オペレーティングシステムおよびワークステーション上で実行中のものについては、追加のメモリ、帯域幅、および CPU のスコープを設定する必要があります。

- ブラウザ — Google Chrome または Mozilla Firefox の最新の 3 つのバージョン
- ネットワーク — 接続されたワークステーションあたり 100 Kbps の帯域幅

- メモリ — 2 GB RAM
- プロセッサ (CPU) — 2 GHz

ワークステーションのモニタリング

ワークステーションレベルで CCP の機能に影響を及ぼす要因は多数あります。さまざまなレベルのログ情報へのアクセスは、修復に対する手順を決定する上で不可欠です。リソースの競合が発生しているワークステーションにロギングやモニタリングをさらに追加すると、使用可能なリソースは削減され、テスト結果が無効になる可能性があります。ワークステーションは、このガイドの エージェントのワークステーションの要件 (p. 39) セクションに示す最小要件を満たすことをお勧めしたことで、追加リソースはログ記録、モニタリング、マルウェアスキャン、オペレーティングシステム機能などの他の実行中のプロセスでそのまま使用することができます。

相関のために追加の履歴ログとデータソースを収集します。イベントの時刻と問題が報告された時刻との間に相関がある場合は、次の情報を使用して原因を特定できる場合があります。

- エージェントワークステーション、または同じネットワークセグメント上の同一ワークステーションから Amazon Connect リージョン内にあるエンドポイントへの往復時間 (RTT) およびパケット損失。セキュリティポリシーが原因でリージョンエンドポイントが使用できない場合は、パブリック WAN エンドポイント (www.Amazon.com など) で問題ありません。理想的には、インスタンスエイリアスアドレス (https://yourInstanceName.awsapps.com) とエンドポイントのシグナリングアドレスを使用します。
- 実行中のプロセス、および各プロセスのリソースの現在の使用状況を示すワークステーションの定期的なモニタリング。
- これらの領域におけるワークステーションのパフォーマンス/使用率:
  - プロセッサ (CPU)
  - ディスク/ドライブ
  - RAM/メモリ
  - ネットワークスループットおよびパフォーマンス
- 前述のすべての VDI デスクトップ環境をモニタリングします (エージェントワークステーションと VDI 環境間の RTT/パケットモニタリングを含む)。

ネットワークポートとプロトコル

CCP ソフトフォンには、AWS リソースへの 3 つの接続が必要です。CCP の完全な機能の実現に向けて、双方向通信を可能にするために Amazon Connect インスタンスを作成したリージョン向けに適切なプロトコルを使用して、これらのリソースへのアドレスとポートを開く必要があります。CCP では、Amazon Elastic Compute Cloud (Amazon EC2)、Amazon CloudFront、Amazon Connect の IP 範囲へのアクセスが必要です。詳細については、Amazon EC2 (EC2)、CloudFront (CLOUDFRONT)、または Amazon Connect (AMAZON_CONNECT) の https://ip-ranges.amazonaws.com/ip-ranges.json ファイルを参照してください。新しいリソースが追加されると、このファイル内のアドレス範囲が更新されます。つまり、エージェントが CCP を正常に使用できるように、含まれる範囲をモニタリングし、環境を更新する必要があります。このファイルに追加されてから 30 日後、新しい IP 範囲の使用が Amazon Connect で開始されます。

サービス	Port	プロトコル	コメント
Amazon Connect	3478	UDP イン/アウト	リージョン内のメディアエンドポイント、およびソフトフォンクライアントのコールの音声に使用されます。
Amazon Connect	443	TCP イン/アウト	

サービス	Port	プロトコル	コメント
Amazon EC2	443	TCP イン/アウト	CCP シグナリングエンドポイント
CloudFront	443	TCP イン/アウト	インスタンスに関連付けられたウェブコンテンツのホスティングに使用されます。エンドポイントは、エンドユーザークライアントの場所によって決まります。

また、Amazon EC2 エンドポイントの場合、AWS ipranges.json ファイルに記載されているすべての IP アドレス範囲ではなく、すべての Amazon EC2 エンドポイントが許可されるように、次の URL およびポートへのアクセスを許可することができます。

`rtc.connect-telecom.{region}.amazonaws.com:443`

`{region}` を Amazon Connect インスタンスを作成したリージョン (例: `us-east-1`) に置き換えます。特定のプロキシアプリケーションでは、このアドレスの使用時にウェブソケットの処理によって機能に影響を及ぼす可能性があります。実稼働環境にデプロイする前にテストを実行して検証する必要があります。

CloudFront では、すべての CloudFront エンドポイントのトラフィックが許可されるように、次の URL をポート 443 で使用することができます。AWS ipranges.json ファイルに記載されているすべての範囲を含めずに、この操作を行います: `https://`**`myInstanceName`**`.awsapps.com`**`myInstanceName`** をトラフィックを許可するインスタンスの名前に置き換えます。特定のプロキシアプリケーションでは、このアドレスの使用時にウェブソケットの処理によって機能に影響を及ぼす可能性があるため本稼働環境にデプロイする前にテストを実行して検証する必要があります。

ポートおよびプロトコルに関する考慮事項

Amazon Connect のネットワーク設定変更を実装するときは、次の点を考慮してください。

- Amazon Connect インスタンスを作成したリージョンのすべてのアドレスと範囲のトラフィックを許可する必要があります。
- CCP と Amazon Connect の間でプロキシまたはファイアウォールを使用している場合は、エージェントのシフト全体の期間をカバーするように SSL 証明書キャッシュのタイムアウトを延長します。これを行うことで、スケジュールされた作業時間内の証明書の更新に伴う接続の問題を回避できます。たとえば、エージェントが 8 時間作業予定の場合 (休憩を含む)、間隔は、8 時間に休憩や昼食の時間を加えた時間に延長します。
- ポートを開く際、Amazon EC2 と Amazon Connect では、インスタンスと同じリージョンにあるエンドポイントのみ必要です。ただし、CloudFront では、エージェントの所在地に最も近いリージョンのエンドポイントが必要です。複数のリージョンにエージェントが存在する場合は、エージェントが Amazon Connect CCP を使用している各リージョンのエンドポイントのトラフィックを許可する必要があります。たとえば、インスタンスが米国東部で、エージェントの現住所は別の国である場合は、エージェントの現住所があるリージョンの IP アドレス範囲を使用して、AWS CloudFormation のポートを開く必要があります。
- 範囲が AWS ipranges.json ファイルで更新されてから 30 日以内にトラフィックが許可される範囲を更新します。更新しない場合、トラフィックは新しい範囲にルーティングされるが、CCP を使用してエージェントに接続できない場合にソフトフォンで CCP を使用すると、断続的な接続の問題が発生する可能性があります。
- Amazon Connect ストリーム API でカスタム CCP を使用している場合は、Amazon Connect との通信にポートを開く必要がないメディアレス CCP を作成できますが、Amazon EC2 および CloudFront との通信するにはポートを開いておく必要があります。

リージョンの選択に関する考慮事項

Amazon Connect リージョンの選択は、データガバナンスの要件、ユースケース、各リージョンで利用可能なサービス、およびエージェント、発信者、外部転送エンドポイントの地理に関するレイテンシーによって決まります。

- エージェントの場所/ネットワーク — CCP 接続はパブリック WAN を経由するため、ワークステーションのレイテンシーが最小で、ホップが最小限に抑えられており、特にリソースと Amazon Connect インスタンスがホストされている AWS リージョンが重要です。たとえば、エッジルーターに到達するために数回のホップを行う必要のあるハブおよびスポークネットワークでは、レイテンシーが発生し、通信品質が低下する可能性があります。

  インスタンスとエージェントを設定するときは、インスタンスを作成するリージョンに地理的に最も近いリージョンにインスタンスを作成してください。会社のポリシーやその他の規制に準拠するために特定のリージョンにインスタンスを設定する必要がある場合は、エージェントコンピュータと Amazon Connect インスタンス間のネットワークホップが最小限になる設定を選択します。
- 発信者の場所 — 通話は Amazon Connect リージョンエンドポイントに固定されているため、PSTN のレイテンシーの影響を受けます。発信者と転送エンドポイントが、Amazon Connect インスタンスが最低限のレイテンシーでホストされている AWS リージョンに可能な限り近く配置されてることが理想的です。

  最適なパフォーマンスを実現し、お客様がコンタクトセンターにコールする際のレイテンシーを抑えるために、お客様がコールした場所から地理的に最も近い Amazon Connect インスタンスを作成します。複数の Amazon Connect インスタンスを作成し、お客様がコールした場所から最も近い番号で問い合わせ情報を指定できる場合があります。
- Amazon Connect からの外部転送 — では、通話中は Amazon Connect リージョンのエンドポイントに固定された状態になります。転送されたコールの受取人によって切断されるまで、使用料は引き続き分単位で発生します。エージェントが離れたり、転送が完了しても、コールは記録されません。転送されたコールの CTR データやそのコール記録は、コール終了後に生成されます。PSTN のレイテンシーが増えないように、可能な限り、コールは Amazon Connect に戻して転送しないでください (循環転送と呼ばれる)。

Amazon Connect をリモートに使用したエージェント

リモートエージェントで、組織のメインネットワークに接続されていない場所から Amazon Connect を使用しており、接続が不安定で、パケットが損失したり、レイテンシーが長い場合、ローカルネットワークに関する問題が発生する可能性があります。この問題は、VPN でリソースにアクセスする必要がある場合、複雑になります。エージェントが AWS リソースと Amazon Connect インスタンスがホストされている AWS リージョンの近くに配置されており、パブリック WAN に安定して接続されていることが理想的です。

オーディオの再ルーティング

既存のデバイスにオーディオをルーティングするときは、Amazon Connect リージョンでのデバイスの位置を考慮してください。これにより、レイテンシーが増える可能性を考慮することができます。音声を再ルーティングすると、エージェントを対象としたコールがある度に、設定されたデバイスに発信されます。エージェントがデバイスに応答すると、そのエージェントは発信者に接続されます。エージェントがデバイスに応答しない場合、エージェントまたは責任者が状態を使用可能に戻すまで、エージェントは不在着信状態に移行されます。

AWS Direct Connect の使用

AWS Direct Connect は、エッジルーターと AWS リソース間のレイテンシーやコール品質の問題を解決するのに役立ちます。また、パブリック WAN を経由するのではなく、AWS トラフィックを専用ファイバに

リダイレクトするようにエッジルーターを設定することもできます。これにより、ISP に依存してリクエストを AWS リソースに動的にルーティングするのではなく、永続的で一貫性のある接続が可能になります。エッジルーターへのプライベート LAN/WAN トラバーサルに関する問題は解決されない点に注意してください。

VDI 環境での Amazon Connect の使用

仮想デスクトップインフラストラクチャ (VDI) 環境では、ソリューションが複雑になるため、POC の作業とパフォーマンステストを別々にして最適化する必要があります。他の WebRTC ベースのブラウザアプリケーションと同様に、Amazon Connect Contact Control Panel (CCP) は、シッククライアント、シンクライアント、ゼロクライアントの VDI 環境で動作し、VDI サポートチームによって適切に設定/サポート/最適化が行われます。以下は、VDI ベースの顧客に役立つ考慮事項とベストプラクティスをまとめたものです。

- エージェントの場所 — エージェントが CCP を使用する場所と VDI ホストの場所との間のラウンドトリップ時間をできるだけ短くし、ホップ数を可能な限り少なくすることが理想的です。
- VDI ソリューションのホストの場所 — VDI ホストの場所が、エージェントと同じネットワークセグメントにあり、内部リソースとエッジルーターの両方のホップ数が可能な限り少ないことが理想的です。また、WebRTC と Amazon EC2 範囲の両方のエンドポイントにできるだけ小さいラウンドトリップ時間を設定することもできます。
- ネットワーク — トラフィックがエンドポイント間を通過するホップによって、障害やレイテンシーが発生する可能性は高くなります。VDI 環境では、基本的なルートが最適化されていない場合や、パイプが十分に高速または広い場合でも、コール品質の問題が発生しやすくなります。AWS Direct Connect ではエッジルーターから AWS のコール品質は向上しますが、内部ルーティングの問題が解消されることはありません。コールオーディオの問題を回避するには、プライベート LAN/WAN をアップグレードまたは最適化するか、外部デバイスにリダイレクトする必要があります。ほとんどのシナリオでは、これが必要な場合、問題が発生しているアプリケーションは CCP だけではありません。
- 専用リソース — アクティビティから利用可能なエージェントリソースへの影響を回避するには、ネットワークレベルおよびデスクトップレベルで行うことが推奨されています (例: バックアップ、大規模なファイル転送)。リソース競合を防止するひとつの方法として、異なるリソースを使用する可能性のある他のビジネスユニットとリソースを共有するのではなく、環境を同じように使用する Amazon Connect ユーザーにデスクトップアクセスを制限します。
- リモート接続を搭載したソフトフォンの使用 — VDI 環境ではオーディオ品質に影響を及ぼす可能性があります。エージェントがリモートエンドポイントに接続してその環境で動作する場合は、オーディオを外部 E.164 エンドポイントにルーティングするか、ローカルデバイスでメディアに接続してからリモート接続でシグナリングすることをお勧めします。カスタム CCP を Amazon Connect Streams API で構築するには、コールシグナリング用のメディアを持たない CCP を作成します。このように、メディアは標準の CCP を使用してローカルデスクトップ上で処理され、シグナリングおよびコール制御はメディアなしで CCP とのリモート接続で処理されます。streams API の詳細については、GitHub リポジトリ (https://github.com/aws/amazon-connect-streams) を参照してください。

CCP 接続

エージェントがログインすると、CCP は AWS ipranges.json ファイルに一覧表示されている Amazon EC2 シグナリングエンドポイント、メディアの場合は Amazon Connect、イメージなどのウェブアーティファクトの場合は CloudFront への接続を試みます。エージェントがログアウトするか、ブラウザが閉じられると、エンドポイントはエージェントの次回ログイン時に再選択されます。Amazon EC2 または Amazon Connect への接続に失敗すると、エラーが CCP に表示されます。CloudFront への接続に失敗すると、ボタンやアイコンなどのウェブ要素だけでなく、ページも読み込めなくなります。

発信通話:

- 通話が発信されると、イベントシグナルは Amazon EC2 エンドポイントに送信され、Amazon Connect と通信してコールを発信します。ダイヤルが正常に終了したら、エージェントは接続され、エージェン

トの Amazon Connect エンドポイントへのコールが固定されます。また、コールが切断されるまで、外部転送やカンファレンスでアンカーが使用されます。固定することで、PSTN のレイテンシーを短縮できます。

受信通話:

- 通話を受信すると、そのコールは Amazon Connect エンドポイントに固定されます。また、コールが切断されるまで、外部転送やカンファレンスでこのアンカーが使用されます。
- エージェントが利用可能になると、新しい Amazon EC2 接続経由でブラウザにプッシュされ、エージェントに提供されます。
- エージェントがコールを受け入れ、外部デバイスが応答されたか、CCP で通話を受信できると判断されると、エージェントへのコールメディアに対して Amazon Connect への接続が確立されます。

転送されたコール:

- コールが転送されると、指定された転送先に通話を発信するシグナルを送信する転送イベントが Amazon EC2 に送信され、Amazon Connect と通信して通話を発信します。
- コールが接続されると、エージェントはブリッジされ、コールはエージェントの既存の Amazon Connect エンドポイントに固定されます。また、コールが切断されるまで、外部転送やカンファレンスでこのアンカーが使用されます。
- コールがブリッジされた後にエージェントがハングアップすると、そのコールに対するエージェントの接続は終了しますが、遠方が切断されるまで、Amazon Connect アンカーポイントの Amazon Connect コールはハングします。コールが切断されると、CTR とその録音が生成され、コールに使用できるようになります。

不在着信:

- コールがエージェントで待機している場合は、エージェントが使用可能になりコールがそのエージェントに正常にルーティングされるまで、お客様キューフローのロジックが使用されます。
- エージェントがコールを受け付けない場合、エージェントは不在着信状態になり、エージェントまたはコールセンターマネージャーがステータスを再び使用可能に変更するまでコールを受けることはできません。エージェントの受信を待っている間、発信元には呼び出し音は鳴らず、お客様キューフローのロジックで定義されたエージェントに接続されるまで発信し続けます。

パニックログアウト:

- CCP が実行されているブラウザウィンドウが閉じている場合、コールは接続されたままですが、ブラウザを開いてログインし直した場合、メディア接続を再度確立することはできません。コールを転送または終了することはできますが、エージェントと発信元の間に音声パスは確立されません。

CCP に関する問題のトラブルシューティング

CCP の問題をトラブルシューティングするには、ネットワークオペレーション、システム管理者、および VDI ソリューションチームから、根本的な原因とドライブ解決策を特定するための適切なレベルの情報を収集するサポートが必要です。関与する適切なリソースを判断しやすいように、同様の現象が発生しているユーザーに問題を共有することが重要です。次のガイダンスは、Amazon Connect のお客様がオペレーションサポートチームと CCP の問題を解決するのに役立ちます。

このセクションのトピック:

- Streams API を使用して役立つ情報を収集します。 (p. 46)
- データの分析 (p. 47)

一般的な CCP の問題

Amazon Connect CCP を使用する際に発生する一般的な問題を以下に示します。

- CCP で初期化/接続できない — 最も一般的な原因は、ポート/IP ホワイトリストのエントリがないため、ブラウザのマイクアクセスを許可していないか、外部デバイスに応答していないことです。このガイドの ネットワークポートとプロトコル (p. 40) セクションで説明しているすべての IP がホワイトリストに登録されていることと、プロンプトが表示された際、ブラウザへのマイクアクセスを許可していることを確認してください。
- 定期的な接続エラー — 最も一般的な原因として、ネットワークの競合が生じているか、ipranges.json の更新があり、新しいエントリがホワイトリストに登録されていない可能性があります。詳細については、このガイドの「ネットワークポートとプロトコル (p. 40)」セクションを参照してください。
- 不在着信、状態変更の遅延、CCP 不応答 — ほとんどの場合、これは断続的で、エージェントのワークステーションかネットワーク、またはその両方のリソース競合と直接相関しています。この問題は、プライベート WAN/LAN、パブリック WAN レベル、またはローカルワークステーションリソースの競合で、AWS リソースへの接続が弱い、不安定、または制限によって状況が悪くなる可能性があります。

CCP 使用時のコール品質に関する一般的な問題を以下に示します。通話品質は、潜在的な原因が広範囲に含まれているため、最適な方法で対応するために、直面している問題のタイプを最初に識別することをお勧めします。

- レイテンシー/クロストーク — 音声接続では、一方が発声し、もう一方に伝わるまでの遅延として作成されます。多くの会話を必要とするユースケースでは、レイテンシーが長くなると、相互に発声している状況が生じることがあります。このシナリオでは、PSTN レイテンシー、エージェントレイテンシー、またはその両方を削減するための要因を特定し、対策を講じるために、PSTN とエージェントのレイテンシーを算出する必要があります。詳細については、このドキュメントの「PSTN とエージェント接続のレイテンシー」セクションを参照してください。
- 片通話 — エージェント側で発信者の音声が聞こえないか、発信者側でエージェントの音声が聞こえない状態です。通常、エージェントのワークステーションのハードウェア、ネットワーク、リソースレベル、またはこれらの 3 つのすべてにおける問題を示しています。また、ブラウザのマイクのアクセス許可やヘッドセットの問題に関連している可能性もあります。詳細については、このガイドの「ワークステーションのモニタリング (p. 40)」セクションを参照してください。
- ボリュームの増減 — コールの開始時または断続的に発生する可能性があり、トラブルシューティングを行うためにもこの 2 つを区別することが重要です。通常、これは、サードパーティーの転送に関する問題からこれを継承する Amazon Connect との間の通話転送に関連します。
- 音声の途切れ、切り取られ、エコー、残響、またはその他のシグナルノイズ — ロボット音やその他のひずみとして発生し、エージェント、発信者、または両者が内容を理解するのが困難になる場合があります。通常、エージェントのワークステーションのハードウェア、ネットワーク、リソースレベル、またはこれらの 3 つのすべてにおける問題を示しています。詳細については、このガイドの「ワークステーションのモニタリング (p. 40)」セクションを参照してください。
- 振動 — 高いジッタとレイテンシーに対抗するためにオーディオの速度を調整するメディアコーデックの影響をオーディオに及ぼす場合があります。通常、エージェントのワークステーションのハードウェア、ネットワーク、リソースレベル、またはこれらの 3 つのすべてにおける問題を示しています。詳細については、このガイドの「ワークステーションのモニタリング (p. 40)」セクションを参照してください。
- 切断 — コール中に発生する可能性があります。通話が切断された場合にパターンを識別する際に注意することが重要です。たとえば、特定の外部番号へのコール転送の切断された場合は、通常、サードパーティーの転送の問題から継承した Amazon Connect との間コールの転送に関連しています。また、循環転送に関連している可能性もあります。つまり、Amazon Connect からコールを転送し、同じコールでコールを戻している可能性があります。

便利なトラブルシューティングのツールと情報

Amazon Connect に関する問題のトラブルシューティングには、次のツールと情報が役立ちます。

- インスタンス ARN — Amazon Connect AWS サポートでインスタンスのアクティビティを確認できるように、お問い合わせの際はインスタンス ARN を記載してください。インスタンスの ARN は、[概要] ページ (Amazon Connect コンソールからインスタンスのエイリアスを選択) で確認できます。
- 通話の録音 — 報告された動作を表し、特定するだけでなく、エージェント側からの音声の問題を排除します。Amazon Connect の録音は、操作のインスタンス側で行われてから、その音声がエージェントの接続を横断します。これにより、オーディオの問題がエージェント側で解消したか、エージェントが受信したオーディオに存在するかどうかを判断できます。問い合わせに関連付けられた通話記録は、問い合わせの検索レポートで確認できます。
- CTR の問い合わせ ID — AWS サポートにお問い合わせされる際は記載してください。
- エージェントのデスクトップパフォーマンス/プロセスログ — ローカルリソース/ネットワークの競合を排除するのに役立ちます。
- Contact Control Panel のログ — エージェントのアクションとタイミングを追跡します。CCP のログをダウンロードするには、CCP の設定の歯車を選択し、[Download logs (ログのダウンロード)] を選択します。ログは、ブラウザのデフォルトのダウンロードディレクトリに保存されます。
- ネットワーク使用率のログ記録/モニタリング — 主に、エージェントと同じネットワークセグメント上のレイテンシーおよび削除されたパケットを確認します。
- プライベート WAN/LAN ネットワーク図 — AWS へのエッジルーターへの接続パスを概説しながら、ネットワークトラバーサルについて説明します。
- ファイアウォールホワイトリストアクセス — IP/ポート範囲が ネットワークポートとプロトコル (p. 40) に示されているとおりにホワイトリストに登録されていることを確認します。
- オーディオのキャプチャおよび分析ツール — エージェントのワークステーションからのレイテンシーを算出します。
- AWS リージョンのレイテンシーテストツール — Amazon Connect Call Control Panel 接続ツールなど。

Streams API を使用して役立つ情報を収集します。

大規模な問題を追跡してトラブルシューティングするために、全体的な通話品質に関するデータを収集することをお勧めします。通話品質が良くない場合、エージェントは、次の図に示すように、配置キーチャートを使用して、現在の時刻と対応する配置コードを書き留めることができます。または、Streams API を使用して独自のレポートを組み込み、カスタム CCP に機能を発行して、対応するコール情報とともにこれらの配置をデータベース (例: Amazon DynamoDB) に書き込むことができます。Amazon Connect Streams API の詳細については、GitHub リポジトリ (https://github.com/aws/amazon-connect-streams) を参照してください。

エージェントの問題レポートの配置の例

次の配置キーの例は、現象やシナリオ、および重要度ごとに一覧表示されています。

症状

- S — ソフトフォンエラー
- M — 不在着信
- L — レイテンシーによって生じる品質の低下
- P — 開始時は問題ないが、時間の経過とともに悪化している
- D — 通話の切断
- W — 片通話 (例: エージェント側でお客様の音声は聞こえるが、お客様側でエージェントの音声が聞こえていない状態)

- V — ボリュームが小さすぎる、または大きすぎる
- C — 断続的に途切れる

シナリオ

- O — 発信通話
- I — 受信通話
- T — 三者間通話

重要度

- 1 — 影響 (小)、CCP を効率的に使用できる
- 2 — 影響 (中)、通信は困難だが通話可能
- 3 — 影響 (大)。CCP コールを使用することはできません

例:

- 5:45PM agentName LT2 (三者間通話でレイテンシー、影響: 中)。
- 6:05PM agentName DO3 (三者間通話で切断、影響: 大)。
- 6:34 PM agentName MI3 (不在着信、影響: 大)。

データの分析

次のガイドラインは、環境内の問題の特定に必要なデータの分析に役立ちます。

- CTR/問い合わせ検索レポートを使用して、通話品質の問題が発生した問い合わせの問い合わせ ID を特定します。CTR には、関連する通話記録へのリンクや、現象の確認、AWS サポート担当者に提供するための追加の詳細がそれぞれ含まれています。
- CTR のエージェント名とタイムスタンプを使用して、発生している問題の種類や、エージェント、現象、シナリオ、および時間の経過に伴う重要度による影響を認識します。これにより、同じ時間に問題が発生しているか、特定のイベントが関連しているか、特定のエージェントまたはエージェントのアクションに特化しているかどうかを確認できます。また、サポートを必要とする場合は、関連する通話記録と関連する問い合わせ ID を簡単に識別してアクセスすることができます。
- ローカルネットワークログ、CPU/ディスク/メモリ使用率、プロセスモニターログなどのデータソースを、クライアントワークステーションのオペレーティングシステムから相関させます。これにより、時間の経過とともにエージェントがイベントを相関させ、ローカルリソースの競合を原因または寄稿者として排除することができます。
- 報告された現象およびシナリオによるデータ (時間または分) を分析して、問題のヒートマップをタイプ別および重要度別にエージェントごとに作成します。これは、バックアップや大規模なファイル転送などのスケジュールされたアクティビティに関連するクラスタ化された影響があるため、環境のトラブルシューティングに特に役立ちます。
- ローカルリソース競合の証拠がない場合や注目すべき相関を導出できない場合は、収集した問い合わせ ID を使用してサポートケースを開くことができます。問題が断続的に発生する場合は、エージェントのワークステーション、ネットワーク接続、またはその両方に関する問題に関連している可能性があります。

検証テスト

音声品質の問題には、関連する多数の原因があります。管理されたテストを実行して、問題を報告している環境やワークステーションと同じ環境やワークステーションをモニタリングし、同じユースケースを再

現できることが重要です。音声品質の問題を調査するために、データの測定と収集に関する一般的なテストの推奨事項を検討してください。

PSTN とエージェント接続のレイテンシー

クロストークの問題を解決するには、さまざまな修復作業が必要なため、エージェントおよび未処理の PSTN レイテンシーの対応を区別して測定する必要があります。

- [overall_latency] は、発信者とエージェントとの間で発生する合計レイテンシーを指します。このレイテンシーは、[overall_latency] = [agent_latency] + [pstn_latency] と計算できます。
- [pstn_latency] は、Amazon Connect エンドポイントと発信者の間のレイテンシーを指します。このレイテンシーは、[pstn_latency] = [overall_latency] - [agent_connection_latency] と計算できます。このレイテンシーを改善するには、Amazon Connect リージョンの別の場所を使用するか、地理的に離れたエンドポイントの場所への外部転送と循環転送を回避します。
- [agent_latency] は、Amazon Connect エンドポイントとエージェントの間のレイテンシーを指します。このレイテンシーは、[agent_latency] = [overall_latency] - [recording_latency] と計算できます。オンプレミスのエージェントでこのレイテンシーを改善するには、AWS Direct Connect を使用することで、VPN 接続を使用しない、プライベート WAN/LAN パフォーマンス/耐久性を強化する、エージェントに近い場所の Amazon Connect リージョンを使用するといった対策を行います。ユースケースによっては、別のリージョンを選択しても [pstn_latency] が増えることもあります。
- [redirect_latency] は、オーディオを外部デバイスにリダイレクトするためのレイテンシーです。このレイテンシーを算出するには、[overall_latency] をリダイレクトした場合としない場合とで 1 回ずつ測定し、その間の差分を計測します。
- [forward_latency] は、Amazon Connect との間で転送呼び出しを行う際のレイテンシーです。このレイテンシーを算出するには、[overall_latency] を転送した場合としない場合とで 1 回ずつ測定し、その間の差分を計測します。

レイテンシーの測定

- ユースケースを再生成します。テスト結果に変更が生じるため、偏差を測定して考慮する必要があります。
- 本稼働の管理と環境を可能な限り一致させます。フロー、電話番号、エンドポイントの場所は同じものを使用します。
- 発信者、エージェント、および外部転送先の地理的な位置を書き留めます (該当する場合)。複数の国にサービスを提供する場合は、国別にテストし、エージェントが本稼働環境で使用するようにテスト範囲を設定する必要があります。
- テストでは、モバイルと固定回線の使用に注意してください。モバイルネットワークでは、レイテンシーを増やすことができるため、適用可能な場合は、お客様やエージェント、転送エンドポイントを測定して考慮する必要があります。
- ビジネスユースケースを再現します。エージェントが会議および転送を使用する場合は、必ずこれらのシナリオをテストしてください。循環転送は推奨されませんが、それらも同様にテストしてください。
- 同じネットワークセグメント上にあるワークステーション環境を含め、エージェントが使用する機器を使用してエージェント環境を再現します。

レイテンシーのテスト要件

レイテンシーを効率的にテストするには、次のものが必要です。

- [agent_latency] をキャプチャするために通話記録が有効になっていること。通話記録がない場合は、[overall_latency] のみ計算できます。
- お客様の電話のソース。テストの場合は、お客様からの実際の通話で通話品質を確認します。

- エージェントの電話機 (オーディオを外部デバイスにリダイレクトする場合)。このデバイスの入出力を記録できる必要があります。
- サードパーティーの転送エンドポイント (該当する場合)。テストは、実際の通話またはサードパーティーからの転送で実行される場合に最適です。
- 録音または解析のソフトウェアが搭載されたエージェントのワークステーション。
- 再現可能なユースケース。再現できない問題については、トラブルシューティングが難しくなる場合があります。
- NTP、またはタイムスタンプを同期させて特定の問い合わせや、それらの発生時刻 (特に複数のタイムゾーンでアクティビティが発生した場合) を特定するメソッド。

ソフトフォンを使用した受信通話のテスト

このプロセスでは、レイテンシーのテストシナリオを約 15 秒で完了できます。結果の分析とタイムスタンプのマーキングには、1 回の記録につき約 1–2 分かかります。

1. 静かな場所に移動します。
2. 外部のスピーカーからオーディオを再生し、それらが再生されていることを確認できるようにエージェントワークステーションを設定します。
3. CCP にログインするには、エージェントワークステーションを使用します。
4. エージェントワークステーションのオーディオキャプチャツールを使用して録音を開始します。
5. お客様の電話ソースから、スピーカーフォンを使用して Amazon Connect インスタンスの着信番号に発信します。実際には、お客様の呼び出しをシミュレートするための外部の電話ソースを使用する場合があります。
6. エージェントワークステーションのソフトフォンを使用して着信コールに応答します。
7. お客様の電話がミュートされていないことを確認します。
8. お客様側で、オブジェクトや手を使用して、机やテーブルの上を大きく叩いてから、すぐにお客様の電話をミュートします。
9. 3 秒以上待ちます。少なくとも 3 回、ステップ 7 ~ 8 を繰り返します。
10. エージェントワークステーションの録音を停止します。
11. オーディオ分析ツールで録音を開きます。机の上で叩いた最初のタッピング音と、もう一方のエージェント回線のタップ音の両方が表示されます。3 つの差分と [overall_latency] の平均値を取得します。
12. オプションで、[agent_latency] を計算するには、オーディオ解析ツールで関連する Amazon Connect の通話記録を開きます。最初のタップ音と相手側のエージェントに到達したときの両方を音声が表示されます。3 つの差分と [recording_latency] の平均値を取得します ([agent_latency] = [overall_latency] - [recording_latency])。必要に応じて操作を繰り返します。

ユースケースに合わせて、必要に応じてテストプランを変更します。ステップが変わっても、オーディオの録音と分析のプロセスは同じです。会議や転送をテストする必要がある場合は、通常どおり測定を行い、会議がサードパーティーの転送エンドポイントでアクティブになっているときに別の測定を行います。

テスト結果の解釈

[overall_latency] の増加の影響は約 300 ミリ秒で目立つようになり、クロストークが 500 ミリ秒を超えることがあります。影響と、受け入れ可能なレイテンシーのレベルは、ユースケースによって異なります。レイテンシーを短縮するために推奨される修復作業については、「PSTN とエージェント接続のレイテンシー (p. 48)」を参照してください。

リリースノート

Amazon Connect の継続的な更新と機能強化を追跡するために、前月にリリースされた変更を説明するリリースノートを毎月発行しています。

毎月の更新

2019 年 2 月の更新

以下の更新を、2019 年 2 月にリリースしました。

カテゴリ別更新

問い合わせのルーティング

- まれに、一部の連絡先が最も長い時間利用可能なエージェントにルーティングされない問題を解決しました。
- [ルーティングプロファイル] ページの [Basic Routing Profile (基本ルーティングプロファイル)] で、[対応エージェントの数] に表示される値が正しくないユーザーインターフェイスの問題を解決しました。ルーティングプロファイルが正しい数のエージェントは、[ユーザー管理] ページに表示されていました。

問い合わせフロー

- Chrome でインテントを追加するときに、問い合わせフローエディターで発生していた問題を解決しました。
- ルーティングの優先順位と、キューに入れられたコールバックの期間が保存されない問題を解決しました。
- アウトバウンドのウィスパーフローの問い合わせ属性が保存されない問題を解決しました。

メトリクスとレポート

- [EnqueueTimestamp]、[Duration]、および [DequeueTimestamp] をコールバック問い合わせの問い合わせ追跡レコード (CTR) に追加しました。
- コールバック問い合わせの InitiationTimestamp が、コールバックが作成された時刻と一致しない問題を解決しました。
- ユーザーにレポートを編集するアクセス権限がない場合に、誤ったメッセージが表示される問題を解決しました。

問い合わせコントロールパネル (CCP)

- CCP でコールバックの呼び出し音が鳴らない問題を解決しました。

2019 年 1 月の更新

以下の更新を、2019 年 1 月にリリースしました。

カテゴリ別更新

- 問い合わせのルーティング (p. 51)
- 問い合わせフロー (p. 51)
- メトリクスとレポート (p. 51)

問い合わせのルーティング

- エージェントの転送がまれに失敗する問題を解決しました。

問い合わせフロー

- エージェントの転送が失敗する問題を解決しました。
- 問い合わせフローログ発行の定期的な遅延の原因になっていた問題を解決しました。

メトリクスとレポート

- [平均キュー応答時間] の計算が間違ってページに表示される、リアルタイムのメトリクスレポートの問題を解決しました。
- エージェントイベントストリームに一部のイベントがない問題を解決しました。

2018 年 12 月の更新

以下の更新を、2018 年 12 月にリリースしました。

カテゴリ別更新

- メトリクスとレポート (p. 52)
- 問い合わせコントロールパネル (CCP) (p. 52)

メトリクスとレポート

- ログインおよびログアウトイベント中にエージェントイベントストリームにエージェントスナップショットがない問題を解決しました。
- 問い合わせ追跡レコードの詳細ページで、検索ページで選択されたタイムゾーンを使用したタイムスタンプが表示された問題を解決しました。
- AfterContactWork のステータスが上書きされた問題を解決しました。
- お客様を保留中にエージェントが誤って切断したときにタイムスタンプが正しくなくなる問題を解決しました。

問い合わせコントロールパネル (CCP)

- エージェント設定が破損したか null のときに初期化で発生する断続的な問題を解決しました。
- Enter キーを使用した通話の転送が機能しない問題を解決しました。

2018 年 11 月の更新

以下の更新は、2018 年 11 月にリリースされました。

カテゴリ別更新

全般

- 監査に関する問題を解決しました。
- エージェントへの接続時に問い合わせが切断されると、エージェントがデフォルト状態になるという問題を解決しました。
- ユーザーアカウントの作成直後にログイン試行が行われた場合、新しく作成されたエージェントが正しくログインできないという問題を解決しました。

問い合わせフロー

- 新しいループブロックを追加しました。このブロックでは、有効なデータが入力されていない場合に顧客情報を追加でリクエストするなど、問い合わせフローのセグメントをループすることができます。

メトリクスとレポート

- 処理されたコールバックが履歴レポートの着信問い合わせの数には含まれていたが、スケジュールレポートに含まれていなかった問題を解決しました。処理されたコールバックは、履歴レポートで処理された着信問い合わせの数に含まれなくなりました。
- インスタンス内に多数のキューとエージェントがレポートにある場合のレポート生成のパフォーマンスが向上しました。
- ACW の報告方法に関する問題を解決し、9 月、10 月、および 11 月の ACW データを修正するためにお客様のインスタンスのデータをバックフィルしました。

2018 年 10 月更新

以下の更新は、2018 年 10 月にリリースされました。

カテゴリ別更新

全般

- メディアセッションが停止する問題を解決しました。

メトリクスとレポート

- 履歴レポートにエージェント名が正しく表示されない問題を解決しました。
- エージェントの補助状態に関するデータが誤って上書きされる問題を解決しました。

API

- `GetCurrentMetrics` オペレーションでメトリクス `OLDEST_CONTACT_AGE` が秒単位ではなくミリ秒単位で返るという問題を解決しました。

2018 年 9 月更新

以下の更新は、2018 年 9 月にリリースされました。

カテゴリ別更新

全般

- [ユーザー管理] ページの読み込み時間を短縮しました。
- キューに関連付けられたクイック接続が多数あると、[キュー] ページの読み込み時に問題が生じていた問題を解消しました。

API

- Amazon Connect API の UpdateContactAttributes オペレーションをリリース。

2018 年 8 月更新

以下の更新は、2018 年 8 月にリリースされました。

カテゴリ別更新

全般

- インスタンス作成時に作成される管理者アカウントのパスワード長を 64 文字までにする制限を追加。
- 保存されたオペレーション時間の設定に日付が設定されていない場合にオペレーション時間ページがロードされない問題を解決。

問い合わせのルーティング

- エージェントが着信通知の用意をしなくて済むように、発信とキューに保存されたコールバックに対するウィスパーのタイムアウトを 2 分に延長。

メトリクスとレポート

- コールバックへの転送が中止された問い合わせとしてカウントされないように、問い合わせの値がメトリクスを中止した方法を修正。

2018 年 7 月更新

以下の更新は、2018 年 7 月にリリースされました。

カテゴリ別更新

機能のリリース

- 動的アウトバウンド発信者 ID
- Amazon Lex ボットをインスタンスに追加する (p. 24)
- ユーザー管理 API
- キュー間転送

全般

- インスタンス作成中にユーザー名として「Administrator」を使って管理者ユーザーを作成しようとした場合のエラーメッセージを追加。ユーザー名「Administrator」は内部使用に予約済みで、Amazon Connect のユーザーアカウントの作成には使用できません。
- 連続したダッシュを含むディレクトリユーザー名の対応を追加。

- インスタンスでセキュリティプロファイルを表示時に、25 件を超えるセキュリティプロファイルを表示できるようページ分割処理を追加。
- `StartOutboundVoiceContact` API を使用時のレイテンシーを低減するパフォーマンス最適化。

メトリクスとレポート

- 追加フィルターの適用時に適用フィルターが設定ページ内に表示されなかったリアルタイムメトリクスレポートの問題を解決。適用されたフィルターが設定ページで正しく表示されるようになりました。

問い合わせフロー

- 問い合わせフローで属性が簡単に参照できるよう、問い合わせ属性にドロップダウンメニューを追加。

2018 年 6 月更新

以下の更新を、2018 年 6 月にリリースしました。

カテゴリ別更新

全般

- 読みやすくするため、UI のフォントを Amazon Ember に変更。

テレフォニーおよび音声

- 米国西部 (オレゴン) リージョンの Amazon Connect で Amazon Lex ボットを使用するサポートを導入。
- エージェントに接続する通話と同様に ループプロンプトが発生したときに通話が落ちる原因になっていたバグを修正。

問い合わせフロー

- キューの設定 ブロックを 作業キューの設定 に名称変更。
- ARN を簡単にコピーできるよう、問い合わせフローの ARN の横にクリップボードにコピー ボタンを追加。ARN を表示するには、デザイナーの問い合わせフローの名前の下にある 追加フロー情報の表示 を選択してください。
- アウトバウンドウィスパーフローで発信者 ID として表示される電話番号をインスタンスから選べるように、電話番号発信 ブロックを新規追加。詳細については、「問い合わせフローの電話番号発信ブロックを使用する」を参照してください。
- 問い合わせフローの新しい メトリクスの取得ブロックなど、システムメトリクス用の問い合わせ属性をリリース。詳細については、「システムメトリクス属性を使用する」をご覧ください。

メトリクスとレポート

- 履歴メトリクスレポート用のフィルター設定の検索フィールドが誤った表示を行う原因となる問題を解決。
- コールバックであった通話電話番号を一覧の代わりに空白が表示されていたダウンロードされたレポートの問題を解決。
- ログイン/ログアウトレポートが、レポート生成あたり 20,000 行に対応 (現在は 10,000 行)。

問い合わせコントロールパネル (CCP)

- エージェントがアクティブ通話をミュート/ミュート解除できるよう、CCP にミュートボタンを追加、Streams API には mute 関数を追加。

2018 年 4 月、5 月更新

以下の更新は、2018 年 4 月と 5 月にリリースされました。

カテゴリ別更新

全般

- 起動直後に、新しい Amazon Polly 音声が Amazon Connect で自動で使用可能。問い合わせフローで Matthew や Léa など、新しい音声を使用できます。
- インスタンス生成中に作成される Amazon Connect 管理者アカウントの要件に合わせるため、Amazon Connect ユーザーアカウントに対するパスワードの適用を更新。
- 既存のユーザーアカウントを更新時に E メールアドレスが保存されなくなることがある問題を解決。

テレフォニーおよび音声

- 日本のテレフォニー向けにレイテンシーを減少し、発信者 ID を向上させるサービス最適化。
- 顧客によるチャンネル諸島のジャージーとガーンジーへ発信可能。
- Amazon Connect 問い合わせフローで使用時に、Amazon Lex ボットに数値キーパッド入力対応を追加。詳細については、Amazon Connect が Amazon Lex チャットボット、キーパッド入力に対応をご覧ください。
- 問い合わせコントロールパネルのレイテンシーが減少し、エージェントのユーザーエクスペリエンスを改善。

問い合わせフロー

- 問い合わせフローの中で AWS Lambda 関数ブロックが使用され、パラメータの入力タイプが、システム属性付きで属性を送信するからテキストを送信するに変更された場合の、問い合わせフローの公開に関する問題を解決。このような問い合わせフローは正常に公開されるようになりました。
- エージェントと顧客のウィスパーがキューに保存されたコールバックで維持。
- 属性がキューのコールバックで正しく維持。
- キューフローのループプロンプトブロック使用時に問い合わせ属性を維持。

メトリクスとレポート

- レポートに最新データを組み込めるように、スケジュールされたレポートのデータを 15 分だけ遅延。これまでは、スケジュールされたレポート間隔中の最終 15 分間のレポートデータが、そのレポートに含まれないことがありました。これはレポートタイプすべてに適用されます。
- メトリクスの計算で、エージェントが着信通話前にアイドル状態である場合、着信通話が呼び出す時間はアイドル時間扱い。
- エージェントの連絡時間 メトリクスに、エージェントが補助ビジー状態で費やした時間を追加。
- Amazon Connect メトリクスに関する新しいドキュメントを公開。

問い合わせコントロールパネル (CCP)

- エージェントがデスクフォンを使用時の CCP 用設定メニューに保存 ボタンを追加。保存 ボタンはセッション間でデスクフォン設定を保存します。
- エージェントのユーザー名が Amazon Connect ストリーム API のエージェント設定データの一部として使用可。
- キューに保存されたコールバックの後のスクリーンポップに対して streams.js (Streams API) を使用時に、問い合わせ属性を使用可。
- 自動着信の場合に、通話の着信および参加後もエージェントに呼び出し音が聞こえ続けることがある問題を解決。

Amazon Connect サービスの制限

新しい Amazon Connect インスタンスのデフォルトの制限を以下の表に示します。制限は時間の経過とともに調節されるため、ご使用のアカウントに設定された制限はここで説明される制限と異なる場合があります。アカウントで作成されたインスタンス間で異なる場合があります。たとえば、アクティブな呼び出しの同時実行数のデフォルトの制限が 10 に設定されている場合にインスタンスを作成すると、そのインスタンスのアクティブな呼び出しの同時実行数は 10 に制限されます。今日新しいインスタンスを作成すると、インスタンスのアクティブな呼び出しの同時実行数の制限は 100 です。API リクエストの制限については、「Amazon Connect API スロットリングの制限 (p. 59)」を参照してください。

まず、Amazon Connect が利用できる各 AWS リージョンの AWS アカウントごとに、インスタンスを 5 つ作成できます。さらにインスタンスが必要な場合、またはサービス制限の変更が必要な場合は、「Amazon Connect サービス上限緩和申請」を使用して、変更を申請することができます。この申請にアクセスするには、AWS アカウントにサインインしている必要があります。

米国の電話番号を現在のキャリアから Amazon Connect への移植要求を提出するには同じ申請を使用してください。電話番号の移植の詳細については、現在の電話番号を移植する (p. 13) を参照してください。

また、インスタンスからの発信通話をかけられる国々にも、サービス制限があります。インスタンスがすでにある場合、これまでにサービス制限に変更が加えられてきたため、電話をかけることができる国々が、以下の表に示されている国々と異なることがあります。その他の国々に電話をかけられるようにサービス制限の増加をリクエストすることも、インスタンスから電話をかけられる国々を制限するリクエストを送信することもできます。

> Note
>
> Amazon Connect は、インドで Amazon Internet Services Pvt. Lt (AISPL) を介して Amazon Web Services を使用しているお客様にはご利用いただけません。。Amazon Connect でインスタンスを作成しようとすると、エラーメッセージが表示されます。

項目	デフォルトの制限
アカウントあたりの Amazon Connect インスタンス数	5
インスタンスあたりのユーザー数	500
インスタンスあたりの電話番号数	10
インスタンスあたりのキュー数	50
ルーティングプロファイルあたりのキュー数	50
インスタンスあたりのルーティングプロファイル数	100
インスタンスあたりのオペレーション時間	100
インスタンスあたりのクイック接続数	100
インスタンスあたりのプロンプト数	500
インスタンスあたりのエージェントステータス	50 この制限を増やすことはできません。

項目	デフォルトの制限
インスタンスあたりのセキュリティプロファイル数	100
インスタンスあたりの問い合わせフロー数	100
インスタンスあたりのエージェント階層グループ	50
インスタンスあたりのレポート数	500
インスタンスあたりのスケジュールされたレポート数	50
インスタンスあたりのアクティブな同時呼び出しの数	100
電話番号の移植	現在のキャリアから Amazon Connect に米国の電話番号を移植することができます。電話番号の移植方法の詳細については、現在の電話番号を移植する (p. 13) を参照してください。
発信通話用に国コードをホワイトリストに追加する	インスタンスを新しく作成すると、以下のダイアルコードに電話を発信できます。 • オーストラリア • カナダ • 中国 • ドイツ • 香港 • イスラエル • 日本 • メキシコ • シンガポール • スウェーデン • アメリカ合衆国 • 英国 †

† 447 をプレフィックスとするイギリスの電話番号は、デフォルトでは許可されません。このようなイギリスの携帯電話番号に発信するには、サービス上限緩和申請を行う必要があります。

Amazon Connect API スロットリングの制限

Amazon Connect API を使用する場合、1 秒あたりのリクエスト数は次のように制限されます。

- `GetMetricData` および `GetCurrentMetricData` オペレーションでは、1 秒 5 リクエスト (RateLimit) と、1 秒あたり 8 リクエスト (BurstLimit) になります。
- その他のオペレーションではすべて、1 秒 2 リクエスト (RateLimit) と、1 秒あたり 5 リクエスト (BurstLimit) になります。

ドキュメント履歴

次の表は、Amazon Connect のドキュメントの更新履歴をまとめたものです。

変更	説明	日付
お客様のオーディオストリームに対してライブメディアストリーミングを有効にするステップを追加します。	お客様のオーディオストリームに対してライブメディアストリーミングを有効にするステップが含まれるように、データストレージ (p. 21)コンテンツを更新しました。	2018 年 12 月 21 日
アジアパシフィック (東京) リージョン での Amazon Connect の使用に関するトピックを追加しました。	トピック「アジアパシフィック (東京) リージョン の Amazon Connect (p. 16)」を追加しました。このトピックには、アジアパシフィック (東京) リージョン で Amazon Connect を使用する場合に固有の情報が含まれます。	2018 年 12 月 10 日
トラブルシューティングとベストプラクティスのトピックを追加	新しいトピック「Amazon Connect のトラブルシューティングとベストプラクティス (p. 39)」を追加しました。このトピックでは、CCP を使用したエージェント接続のベストプラクティスと、Amazon Connect における接続と通話の品質の問題のトラブルシューティングについて説明します。	2018 年 10 月 18 日
Amazon Connect のサービスにリンクされたロールの使用に関するトピックを追加しました。	トピック「Amazon Connect のサービスにリンクされたロールの使用 (p. 26)」を追加しました。このトピックでは、Amazon Connect のサービスにリンクされたロールの使用について説明しています。	2018 年 10 月 17 日
Amazon Lex ボットをインスタンスに追加する手順を更新しました。	「Amazon Lex ボットをインスタンスに追加する (p. 24)」セクションを更新して、別のリージョンからボットを選択する手順を追加しました。	2018 年 7 月 30 日
リリースノートのトピックを追加。	前月中の Amazon Connect の変更および更新がリストされたリースノートのトピックを公開しました。詳細については、「リリースノート (p. 50)」を参照してください。	2018 年 11 月 6 日

変更	説明	日付
Amazon CloudWatch Logs に送信されるメトリクスについてのトピックを更新。	「Amazon Connect インスタンスの CloudWatch メトリクス (p. 28)」のトピックを更新し、追加されたメトリクスを含め、すべてのメトリクスの説明を更新しました。	2018 年 4 月 19 日
ID 管理に SAML を使用する方法についてのコンテンツを追加。	ID 管理に SAML を使用するようにインスタンスを設定する方法について説明した新しいトピックを追加しました。また、SAML を使用して、シングルサインオンを有効にすることもできます。詳細については、「Amazon Connect での ID 管理用に SAML を設定する (p. 7)」を参照してください。	2018 年 3 月 30 日
AWS Lambda 関数を Amazon Connect で使用する方法についてのトピックを更新。	既存のコンテンツを新しい情報および例に置き換えました。詳細については、「Amazon Connect で AWS Lambda 関数を使用する (p. 32)」を参照してください。	2018 年 1 月 5 日
「現在の電話番号を移植する」を追加。	現在の電話番号を Amazon Connect に移植する方法についての情報を追加しました。詳細については、「現在の電話番号を移植する (p. 13)」を参照してください。	2017 年 11 月 10 日
Salesforce との統合についての情報を更新。	Amazon Connect を Salesforce と統合して設定を明確にする手順を更新しました。詳細については、「Amazon Connect と Salesforce との統合 (p. 36)」を参照してください。	2017 年 10 月 27 日
初回リリース	『Amazon Connect 管理者ガイド』の初回リリース。	2017 年 3 月 28 日