Citrix Cloud Japan

Contents

Citrix Cloud Japan

December 20, 2023

Citrix Cloud Japan は Citrix Cloud から独立したクラウドであり、日本のお客様は、Citrix が管理する専用環境で特定の Citrix Cloud サービスをご利用いただけます。

Citrix Cloud Japan のドキュメントには、アカウントとサポートされているサービスの設定に関する詳細が記載されています。このドキュメントでは、他の Citrix Cloud リージョンと比較した Citrix Cloud Japan のサービスと機能の違いについても説明します。Citrix Cloud Japan と Citrix Cloud の両方で機能が同一である場合、このドキュメントでは Citrix Cloud ドキュメントにおける既存の情報へのリンクを提供します。

使用可能なサービス

Citrix Cloud Japan では、次のサービスを利用できます:

- Citrix Gateway
- Citrix DaaS（Virtual Apps and Desktops の新名称）
- License Usage Insights（Citrix パートナーのみ）
- Secure Browser
- Citrix Workspace
- Workspace Environment Management サービス（Citrix Cloud Connector バージョン `6.29.0.58841` 以降が必要）

詳しくは、「サービスの機能の可用性」を参照してください。

リージョンに依存しないデータ

顧客によるクラウドサービスの使用に関連する情報を含む特定のログは、本質的にリージョンに依存しません。このデータは、サポートやトラブルシューティング、パフォーマンスの監視、セキュリティ、監査、リージョン間認証の許可など、クラウドサービスをサポートするために、必要に応じてリージョンに関係なく複製およびアクセスされる場合があります。

ログは、サービスを実行するために必要に応じて、Citrix のサードパーティサプライヤーによってリージョンに関係なく処理される場合があります。詳しくは、「Citrix Cloud サービスのデータ保護の概要」（英語）を参照してください。

サードパーティ通知

Citrix Cloud Japan には、サードパーティソフトウェアが含まれている可能性があります。このサードパーティソフトウェアは、サードパーティ製品についての通知ドキュメントで定義されたプラットフォームおよびサポートされ

るサービスに関する条件の下でライセンスが有効になっています。詳しくは、「Citrix Cloud サードパーティ通知」を参照してください。

新機能

Citrix は、Citrix Cloud Japan の顧客に、新機能と更新情報をいち早くお届けするよう取り組んでいます。新しいリリースでは、より便利な機能をご利用いただけます。今すぐ更新してください。

このプロセスは、わかりやすいものになっています。最初の更新は、Citrix 内部サイトのみに適用され、その後徐々に顧客環境に適用されます。段階的に更新することによって、製品の品質と可用性を最大化しています。

クラウドの規模とサービスの可用性に関するサービスレベルアグリーメントについて詳しくは、Citrix Cloud のサービスレベルアグリーメントを参照してください。サービスの中断および定期メンテナンスを監視するには、Service Health Dashboardを参照してください。

2023 年 **10** 月

App Protection： Citrix Cloud Japan が Workspace App Protection サービスをサポートするようになりました。詳しくは、「App Protection」を参照してください。

2022 年 **8** 月

管理者の管理インターフェイスの向上： Citrix Cloud Japan では、個別の管理者および管理者グループを追加するためのインターフェイスが向上しました。詳しくは、次の記事を参照してください：

- 個別の管理者を招待する
- AD から Citrix Cloud Japan に管理者を追加する

2022 年 **7** 月

管理者（プレビュー）の **SAML** 認証： Citrix Cloud Japan は、AD の管理者グループに対する SAML 認証の使用をサポートするようになりました。詳しくは、「SAML を ID プロバイダーとして Citrix Cloud Japan に接続する」を参照してください。

2022 年 **4** 月

顧客ダッシュボードへのアクセスを有効または無効にする： Citrix Cloud Japan は、管理者が顧客ダッシュボードへの表示専用アクセスを有効にすることをサポートするようになりました。詳しくは、「パートナー向けの Citrix Cloud」を参照してください。

Citrix DaaS のライセンスを解放するプロセスの向上： Citrix Cloud Japan では、割り当てられたライセンスを一括で解放するためのワークフローが向上しました。詳しくは、「Citrix DaaS のライセンスとアクティブな使用状況の監視（ユーザー/デバイス）」を参照してください。

2022 年 **3** 月

システムログの一般提供：システムログが一般提供されるようになりました。システムログには、Citrix Cloud Japan で発生したイベントがタイムスタンプ付きで一覧表示されます。過去 90 日間のイベントを表示しイベントをエクスポートして、組織の法規制の遵守要件を満たしたり、セキュリティ分析をサポートしたりします。詳しくは、「システムログ」を参照してください。

2022 年 **2** 月

ID プロバイダーとしての **SAML** のサポート： Citrix Cloud Japan は、選択した SAML プロバイダーを使用した Citrix Workspace への利用者の認証をサポートするようになりました。詳しくは、「SAML を ID プロバイダーとして Citrix Cloud Japan に接続する」を参照してください。

2021 年 **12** 月

Citrix Gateway サービスの一般提供： Citrix Gateway は Citrix Workspace の外部ユーザーにセキュアなリモートアクセスを提供します。詳しくは、「Citrix Cloud Japan での Citrix Gateway サービス」を参照してください。

2021 年 **11** 月

Azure Active Directory グループへの管理者の追加： Citrix Cloud Japan は、Azure AD グループを使用した Citrix Cloud Japan アカウントへの管理者の追加をサポートするようになりました。詳しくは、「管理者グループを管理する」を参照してください。

2021 年 **10** 月

Workspace Environment Management のサポート： Citrix Cloud Japan は、Workspace Environment Management サービスをサポートするようになりました。このサービスは、インテリジェントなリソース管理およびプロファイル管理テクノロジを使用して、Citrix DaaS の展開で可能な限り最高のパフォーマンス、デスクトップログオン、およびアプリケーション応答時間を提供します。このサービスのサポートには、Citrix Cloud Connector バージョン`6.29.0.58841`以降が必要です。

2021 年 **9** 月

Citrix Workspace および **Citrix Gateway** サービスの サポート： Citrix Cloud Japan は、次のサービスをサポートするようになりました：

- Citrix Workspace を使用すると、組織内の個人の役割に関連する情報、アプリ、およびその他のコンテンツへのセキュアなアクセスを提供できます。ユーザーは、利用可能なサービスをサブスクライブし、場所とデバイスを選ばずにアクセスできます。
- Citrix Gateway サービスは、Citrix Workspace の外部ユーザーにセキュアなリモートアクセスを提供します。

詳しくは、「サービスの機能の可用性」を参照してください。

2021 年 **6** 月

システムログのプレビュー： Citrix Cloud Japan では、Citrix Cloud Japan で発生したイベントのタイムスタンプ付き一覧を表示するシステムログプレビュー機能を提供するようになりました。過去 90 日間のイベントを表示しイベントをエクスポートして、組織の法規制の遵守要件を満たしたり、セキュリティ分析をサポートしたりします。詳しくは、「システムログ」を参照してください。

サポートされているサービスの機能の可用性

November 21, 2023

一般的にサービスの可用性とは、関連するすべてのサービス機能が利用可能であることを意味します。ただし、Citrix Cloud Japan にサービスが含まれている場合、特定のサービス機能がすぐに利用できないことがあります。

この記事のセクションでは、Citrix Cloud Japan でサポートされているサービスについて説明します。また、現在利用できないサービス機能も記載されています。この記事に含まれていない機能は、Citrix Cloud Japan でも利用可能であり、Citrix Cloud の場合と同じように機能します。利用可能な機能について詳しく知るために、この記事には各サービスのドキュメントへのリンクが含まれています。

Citrix Gateway

Citrix Gateway サービスは、Citrix Workspace の外部ユーザーにセキュアなリモートアクセスを提供します。

Citrix Gateway サービスは、Citrix Cloud Japan の顧客が一般的に利用できます。次のサービス機能は利用できません：

- SaaS アプリおよびエンタープライズ Web アプリのサポート
- コンテキストに基づくアクセス

詳しくは、「Citrix Cloud Japan での Citrix Gateway サービス」を参照してください。

Citrix DaaS

Citrix DaaS（Citrix Virtual Apps and Desktops サービスの新名称）を使用すると、セキュアな仮想アプリとデスクトップを配信でき、インストール、セットアップ、アップグレードの大半は Citrix によって実行されます。どのデバイスに対しても最高のユーザーエクスペリエンスを提供しながら、アプリケーション、ポリシー、ユーザーを完全に制御できます。

Citrix DaaS は、Citrix Cloud Japan の顧客が一般的に利用できます。すべてのサービス機能が利用可能であり、Citrix Cloud の場合と同じように機能します。

詳しくは、Citrix DaaSドキュメントを参照してください。

App Protection

App Protection 機能は、Citrix Virtual Apps and Desktops および Citrix DaaS（Citrix Virtual Apps and Desktops サービスの新名称）の使用時にセキュリティを強化する機能です。この機能により、キーロガーや画面キャプチャマルウェアによりクライアントが侵害される可能性が制限されます。App Protection では、画面に表示されるユーザーの資格情報や個人情報などの機密情報の流出を防ぎます。この機能を使うと、ユーザーおよび攻撃者がスクリーンショットを撮る、またはキーロガーを使用することにより機密情報を収集、悪用することを防ぐことができます。
App Protection は、Citrix Cloud Japan のお客様が一般的に利用できます。すべてのサービス機能が利用可能であり、Citrix Cloud の場合と同じように機能します。

詳しくは、「App Protection」のドキュメントを参照してください。
App Protection でサポートされている機能の詳細については、App Protection の互換性マトリックスドキュメントを参照してください。

License Usage Insights

Citrix Cloud の License Usage Insights サービスは、Citrix Service Provider が製品のライセンスと使用状況を把握し報告するために役立つ無料のクラウドサービスです。このサービスは、Citrix Cloud Japan の顧客が一般的に利用できます。すべてのサービス機能が利用可能であり、Citrix Cloud の場合と同じように機能します。

詳しくは、Citrix Cloud ドキュメントの「Citrix Service Provider 用のライセンス」を参照してください。

Secure Browser

Citrix Secure Browser サービスは、Web 閲覧アクティビティを分離することにより、ブラウザーベースの攻撃から企業のネットワークを保護します。ユーザーデバイスを構成する必要なく、インターネットでホストされた Web アプリケーションに一貫してセキュアにリモートアクセスすることができます。

Secure Browser サービスは、Citrix Cloud Japan の顧客が一般的に利用できます。すべてのサービス機能が利用可能であり、Citrix Cloud の場合と同じように機能します。

詳しくは、Citrix Cloud ドキュメントの「Secure Browser サービス」を参照してください。

Citrix Workspace

Citrix Workspace は、組織内の個人の役割に関連する情報、アプリ、その他のコンテンツへのセキュアなアクセスを提供する、完全なデジタルワークスペースソリューションです。ユーザーは、利用可能なサービスをサブスクライブし、場所とデバイスを選ばずにアクセスできます。

Citrix Workspace サービスは、Citrix Cloud Japan の顧客が一般的に利用できます。次のサービス機能は利用できません:

- Citrix Workspace アプリのカスタムの外観テーマ
- Web ブラウザー経由でワークスペースにアクセスする利用者のパフォーマンスを向上させるキャッシュ
- 利用者が Workspace アプリにサインインしたままでいられる（再度サインインする必要が生じるまでの）再認証時間。
- Microsoft Teams と Workspace の統合
- Workspace のアクティビティフィード

詳しくは、Citrix Workspaceのドキュメントを参照してください。

Workspace Environment Management

Workspace Environment Management は、インテリジェントなリソース管理テクノロジと Profile Management テクノロジによって、Citrix DaaS 展開環境で最適なパフォーマンス、デスクトップへのログオン、アプリケーション応答時間を可能にします。

Workspace Environment Management サービスは、Citrix Cloud Japan の顧客に一般提供されています。このサービスには、Citrix Cloud Connector バージョン`6.29.0.58841`以降が必要です。すべてのサービス機能が利用可能であり、Citrix Cloud の場合と同じように機能します。

詳しくは、Workspace Environment Managementサービスのドキュメントを参照してください。

セキュリティで保護された **Citrix Cloud Japan** の展開ガイド

November 21, 2023

セキュリティで保護された Citrix Cloud Japan の展開ガイドには、Citrix Cloud Japan を使用するときのセキュリティのベストプラクティスの概要と、Citrix が収集し管理する情報が記載されています。

その他のサービスのセキュリティの技術概要

Citrix Cloud Japan サービス内のデータセキュリティについて詳しくは、次の記事を参照してください:

- Citrix Gateway サービスのセキュリティの技術概要
- Citrix DaaS のセキュリティの技術概要（Virtual Apps and Desktops サービスの新名称）
- Workspace Environment Management サービスの顧客データ管理

管理者向けガイダンス

- 強力なパスワードを使用し、定期的にパスワードを変更してください。
- 顧客アカウント内のすべての管理者は、他の管理者を追加および削除できます。信頼できる管理者だけが Citrix Cloud Japan にアクセスできるようにしてください。
- 顧客の管理者には、デフォルトですべてのサービスへのフルアクセス権があります。サービスによっては、管理者のアクセスを制限する機能があります。詳しくは、サービスごとのドキュメントを参照してください。
- Citrix Cloud Japan と Azure Active Directory との統合により、管理者の 2 要素認証が実現します。

パスワードコンプライアンス

Citrix Cloud Japan は、次のいずれかの条件にあてはまる場合、管理者にパスワードを変更するよう要求します:

- 現在のパスワードが、サインインに使用されずに 60 日経った。
- 現在のパスワードが、侵害されたパスワードの既知のデータベースにリストされている。

新しいパスワードは、次のすべての基準を満たす必要があります:

- 文字数は最低 8 文字（最大 128 文字）
- 大文字と小文字をそれぞれ 1 つ以上含む
- 数字を 1 つ以上含む
- 特殊文字を 1 つ以上含む: ! @ # $ % ^ * ? + = -

パスワードの変更ルール:

- 現在のパスワードを新しいパスワードとして使用することはできません。
- 直近で使用した 5 個のパスワードは再利用できません。
- 新しいパスワードは、アカウントのユーザー名に似たものにすることはできません。
- 新しいパスワードが、侵害されたパスワードの既知のデータベースにリストされているものであってはいけません。Citrix Cloud は、新しいパスワードがこの条件に違反しているかどうかをhttps://haveibeenpwned.com/で提供されているリストを使用して判断します。

暗号化とキー管理

Citrix Cloud Japan のコントロールプレーンには機密の顧客情報は保存されません。代わりに、Citrix Cloud Japan は管理者のパスワードなどの情報をオンデマンドで取得します（管理者に明示的に要求します）。重要なデータや暗号化されたデータは保存されていないため、キーを管理する必要はありません。

実行中のデータには、業界標準の TLS 1.2 と最も強力な暗号の組み合わせが Citrix では使用されます。Citrix Cloud Japan は Citrix 所有の cloud.jp ドメインでホストされているため、顧客は使用中の TLS 証明書を管理できません。Citrix Cloud Japan にアクセスするには、TLS 1.2 対応のブラウザーを使用して、承認済みの強力な暗号の組み合わせを構成している必要があります。

- Windows Server 2016、Windows Server 2019、または Windows Server 2022 から Citrix Cloud コントロールプレーンにアクセスする場合、次の強力な暗号をお勧めします: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384、TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- Windows Server 2012 R2 から Citrix Cloud コントロールプレーンにアクセスする場合、強力な暗号は使用できないため、次の暗号を使用する必要があります: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384、TLS_DHE_RSA_WITH_AES_128_GCM_SHA256、TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384、TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

各クラウドサービスの暗号化とキー管理について詳しくは、サービスごとのドキュメントを参照してください。

TLS 1.2 構成について詳しくは、次の記事を参照してください:

- CTX245765 Monitoring Service の OData エンドポイントにクエリするときに、エラー:「基になっている接続が閉じられました: 送信時に予期しないエラーが発生しました。」
- Microsoft Docs Web サイトで TLS1.2 をサポートするように、.NET Framework を更新および構成します。

データ主権

Citrix Cloud Japan コントロールプレーンは、日本でホストされています。顧客は管理できません。

顧客は、Citrix Cloud Japan で使用するリソースの場所を所有および管理します。リソースの場所は、顧客が選択したデータセンター、クラウド、場所、または地理的な場所に作成できます。すべての重要なビジネスデータ（ドキュメント、スプレッドシートなど）はリソースの場所に保存され、顧客が管理します。

セキュリティ問題に関する情報

Web サイトstatus.cloud.comでは、顧客に継続的な影響を与えるセキュリティ問題について確認できます。このサイトは状態と稼働時間に関する情報を記録します。また、プラットフォームや個別サービスへの更新をサブスクライブするオプションがあります。

Citrix Cloud Connector

インストール

Citrix では、セキュリティとパフォーマンスの観点から、ドメインコントローラーに Cloud Connector ソフトウェアをインストールしないことをお勧めします。

さらに、Cloud Connector ソフトウェアがインストールされているマシンは、DMZ（Delimitarized Zone：非武装地帯）ではなく、顧客のプライベートネットワーク内に配置することを Citrix では強くお勧めします。ネットワークとシステムの要件、および Cloud Connector のインストール手順については、「リソースの場所の作成」を参照してください。

構成

顧客は、Cloud Connector がインストールされているコンピューターを Windows のセキュリティ更新プログラムで最新の状態に保つ責任があります。

Cloud Connector は、ウイルス対策ソフトとともに使用できます。Citrix では McAfee VirusScan Enterprise + AntiSpyware Enterprise 8.8 でテスト済みです。これ以外の業界標準のウイルス対策製品も Citrix では使用できます。

顧客の Active Directory（AD）では、Cloud Connector のマシンアカウントを読み取り専用アクセスに制限する必要があります。これは Active Directory のデフォルトの構成です。さらに、Cloud Connector のマシンアカウントで AD ログおよび監査を有効にして、すべての AD アクセスアクティビティを監視できます。

Cloud Connector をホストしているマシンへのログオン

Cloud Connector を使用すると、機密性の高いセキュリティ情報を Citrix Cloud サービスの他のプラットフォームコンポーネントに渡すことができますが、次の機密情報も保存されます：

- Citrix Cloud と通信するためのサービスキー
- Citrix DaaS の電源管理に使用するハイパーバイザーサービスの資格情報

この機密情報は、Cloud Connector をホストしている Windows Server 上のデータ保護 API（DPAPI）を使用して暗号化されます。最も権限のある管理者だけが、Cloud Connector マシンに（メンテナンス操作のためなどに）ログオンできるようにすることを Citrix では強くお勧めします。通常、Citrix 製品を管理するために、管理者がこれらのマシンにログオンする必要はありません。Cloud Connector には、自己管理機能があります。

Cloud Connector をホストしているマシンには、エンドユーザーがログオンできないようにしてください。

Cloud Connector マシンへの追加ソフトウェアのインストール

顧客は、Cloud Connector がインストールされているマシン上にウイルス対策ソフトウェアと（仮想マシンにインストールされている場合）ハイパーバイザーツールをインストールできます。ただし、Citrix は、これらのマシンに他のソフトウェアをインストールしないことをお勧めします。他のソフトウェアによって、セキュリティ攻撃の可能性を高めることになり、Citrix Cloud Japan ソリューション全体のセキュリティが低下することがあります。

送受信ポートの構成

Cloud Connector では、インターネットへのアクセスに送信ポート 443 を開く必要があります。Cloud Connector にインターネットからアクセスするための受信ポートは必要ありません。

顧客は、送信インターネット通信を監視するために、Web プロキシの背後に Cloud Connector を配置できます。ただし、Web プロキシは SSL/TLS 暗号化通信で動作する必要があります。

Cloud Connector には、インターネットにアクセスできる追加の送信ポートがある場合もあります。追加のポートが利用可能な場合、ネットワーク帯域幅とパフォーマンスを最適化するために、Cloud Connector は幅広いポートにわたってネゴシエートします。

Cloud Connector は、内部ネットワーク内で、広範囲の受信ポートと送信ポートを開く必要があります。次の表は、開放する必要があるポートの基本セットです。

クライアントポート	サーバーポート。	サービス
49152～65535/UDP	123/UDP	W32Time
49152～65535/TCP	135/TCP	RPC エンドポイントマッパー
49152～65535/TCP	464/TCP/UDP	Kerberos パスワードの変更
49152～65535/TCP	49152～65535/TCP	LSA、SAM、Netlogon の RPC（*）
49152～65535/TCP/UDP	389/TCP/UDP	LDAP
49152～65535/TCP	3268/TCP	LDAP GC
49152～65535/TCP	3269/TCP	LDAP GC SSL
53、49152～65535/TCP/UDP	53/TCP/UDP	DNS
49152～65535/TCP	49152～65535/TCP	FRS RPC（*）
49152～65535/TCP/UDP	88/TCP/UDP	kerberos
49152～65535/TCP/UDP	445/TCP	SMB

Citrix Cloud Japan 内で使用される各サービスによっては、必要なオープンポート一覧は拡張されます。詳しくは、「Citrix Cloud Japan の接続の要件」を参照してください。

外部通信の監視

Cloud Connector は、ポート 443 上で Citrix Cloud Japan サーバーと Microsoft Azure Service Bus サーバーの両方でインターネットと通信します。

Cloud Connector は、ホストコンピューターが存在する Active Directory フォレスト内にあるローカルネットワーク上のドメインコントローラーと通信します。

通常の操作では、Cloud Connector は Citrix Cloud Japan ユーザーインターフェイスの［**ID** およびアクセス管理］ページで無効になっていないドメイン内のドメインコントローラーとのみ通信します。

Citrix Cloud Japan 内のサービスごとに、Cloud Connector が通常の操作の過程で通信する可能性があるサーバーと内部リソースの一覧は拡張されます。また、Cloud Connector が Citrix に送信するデータを顧客が管理することはできません。サービスの内部リソースと Citrix に送信されるデータについて詳しくは、次のドキュメントを参照してください：

- 各サービスのセキュリティの技術概要（この記事の冒頭に記載されています）
- サポートされているクラウドサービスの接続要件

Cloud Connector ログの表示

管理者に関連する情報、または対応が必要な情報は、Cloud Connector マシンの Windows イベントログで確認できます。

次のディレクトリで Cloud Connector のインストールログを表示します：

- %AppData%\Local\Temp\CitrixLogs\CloudServicesSetup
- %windir%\Temp\CitrixLogs\CloudServicesSetup

Cloud Connector がクラウドに送信するログは、%ProgramData%\Citrix\WorkspaceCloud\Logs にあります。

WorkspaceCloud\Logs ディレクトリのログは、指定したサイズのしきい値を超えると削除されます。管理者は、HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CloudServices\AgentAdministration\MaximumLogSpaceMegabytes のレジストリキー値を調整することによって、このサイズのしきい値を制御できます。

SSL/TLS 構成

Cloud Connector をホストする Windows Server では、「暗号化とキー管理」で説明されている暗号を有効にする必要があります。

Cloud Connector が、Citrix Cloud SSL/TLS 証明書および Microsoft Azure Service Bus SSL/TLS 証明書で使用される証明機関（CA）を信頼する必要があります。Citrix と Microsoft は今後、証明書と CA を変更する可能性がありますが、Windows の標準の信頼された発行元一覧にある CA を常に使用します。

Citrix Cloud Japan 内の各サービスの SSL 構成要件は異なることがあります。詳しくは、各サービスのセキュリティの技術概要（この記事の冒頭に記載されています）を参照してください。

コネクタの更新

Citrix ソフトウェアの更新が利用可能になると、デフォルトでは、Cloud Connector が自己管理します。更新スケジュールの構成について詳しくは、「Connector の更新」を参照してください。

再起動を無効にしたり、Cloud Connector に他の制限を設定したりしないでください。こうした操作により、重要な更新があるときに Cloud Connector がアップデートされなくなります。

顧客側で、セキュリティ上の問題に対応するための特別な操作は必要ありません。Cloud Connector により、Citrix ソフトウェアのセキュリティ上の修正プログラムと更新が自動的に適用されます。

不正使用されたアカウントの処理に関するガイダンス

- Citrix Cloud Japan の管理者リストを監査し、信頼されていない管理者を削除してください。
- 社内の Active Directory 内の侵害されたアカウントを無効にしてください。
- Citrix に連絡して、すべての顧客の Cloud Connector に格納されている認証シークレットのローテーションを要求してください。違反の重大度に応じて、次の処置を講じてください。
  - 低リスク： Citrix は、経過時間によってシークレットをローテーションできます。Cloud Connector は引き続き通常どおりに機能します。古い認証シークレットは 2〜4 週間で無効になります。この間 Cloud Connector を監視して、予期しない操作がないことを確認します。
  - 進行中の高リスク： Citrix はすべての古いシークレットを取り消すことができます。既存の Cloud Connector は機能しなくなります。通常の操作を再開するには、該当するすべてのマシンで Cloud Connector をアンインストールして再インストールする必要があります。

ヘルプとサポートの利用

November 21, 2023

アカウントにログインする

Citrix Cloud Japan アカウントへサインインに問題がある場合は、次の手順を実行します:

- https://citrix.citrixcloud.jp/にサインインして、サインインページに Citrix Cloud Japan のロゴが表示されていることを確認します。Citrix Cloud Japan のサインイン URL では、トップレベルドメインに `.com` ではなく、`.jp` を使用しています。

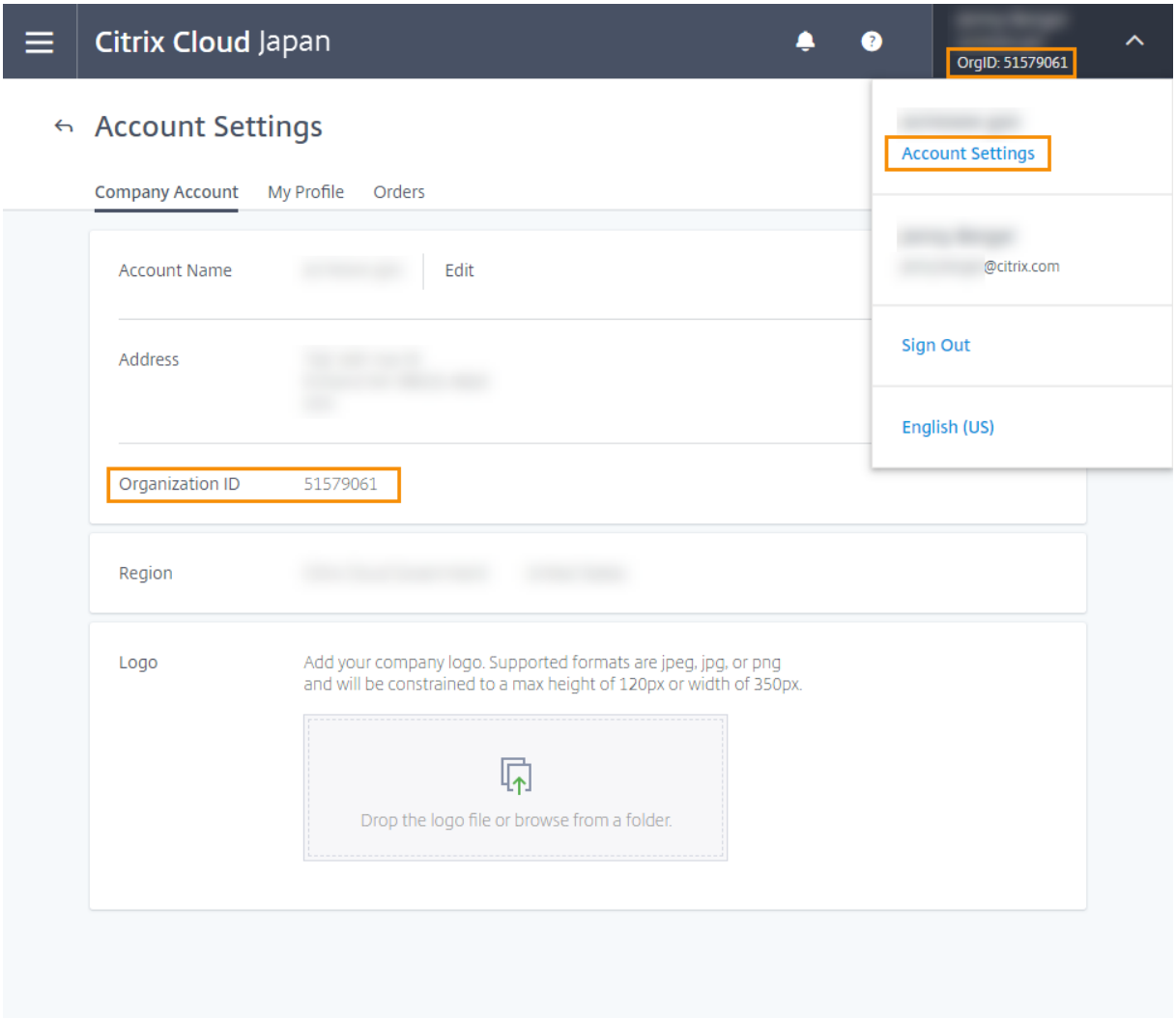
- アカウントに新規登録したときに指定したメールアドレスとパスワードを使用してサインインしてください。アカウントの登録に使用できるメールアドレスについて詳しくは、「Citrix Cloud Japan に登録する」を参照してください。
- 組織が Citrix Cloud Japan 管理者の ID プロバイダーとして Azure AD を使用している場合は、［組織の資格情報でサインイン］をクリックし、組織のサインイン URL を入力します。次に、組織の資格情報を入力すると、組織の Citrix Cloud Japan アカウントにアクセスできます。組織のログイン URL がわからない場合、組織の管理者に問い合わせてください。

> 注:
>
> アカウントの ID プロバイダーとして Azure Active Directory が有効になっている場合は、組織の資格情報を使用してサインインできます。Azure Active Directory を ID プロバイダー（IDP）として使用する方法について詳しくは、「Azure Active Directory を ID プロバイダーとして接続」を参照してください。

サービスの購入

https://www.citrix.com/buy/にアクセスして、サービストライアルから製品版サービスに移行するか、既存のサブスクリプションを更新または延長してください。

購入を完了するには、Citrix Cloud Japan 管理コンソールで利用可能な組織 ID が必要です。



60 日間のトライアル期間終了までに購入しない場合、サービスは終了し、すべてのデータと設定は 90 日間 Citrix にアーカイブされます。

サブスクリプション期間が終了する前に購入しない場合:

- サービスの有効期限が切れてから 30 日後に、管理者とユーザーがサービスにアクセスできなくなります。
- サービスの有効期限が切れてから 90 日後にサービスが終了し、Citrix は残りのデータをすべて削除します。

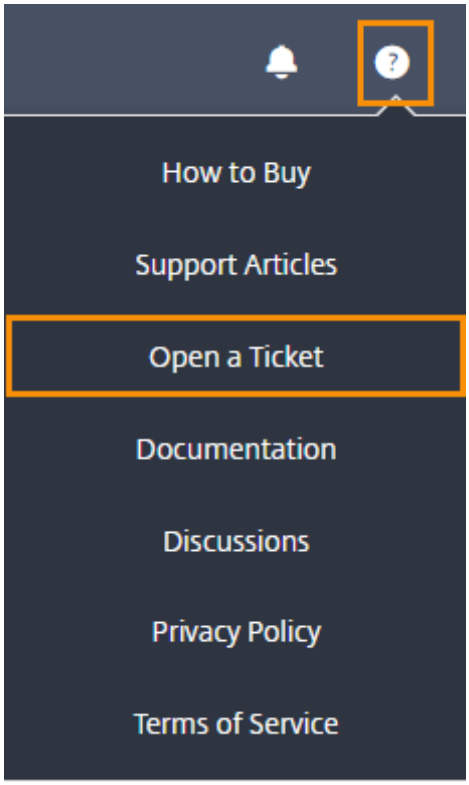
90 日間の期間内に購入すると、期限切れのサービスが製品版サービスとして再度アクティブになります。

サブスクリプションの更新または延長についてさらにサポートが必要な場合は、Citrix カスタマーサービスにお問い合わせください。

テクニカルサポート

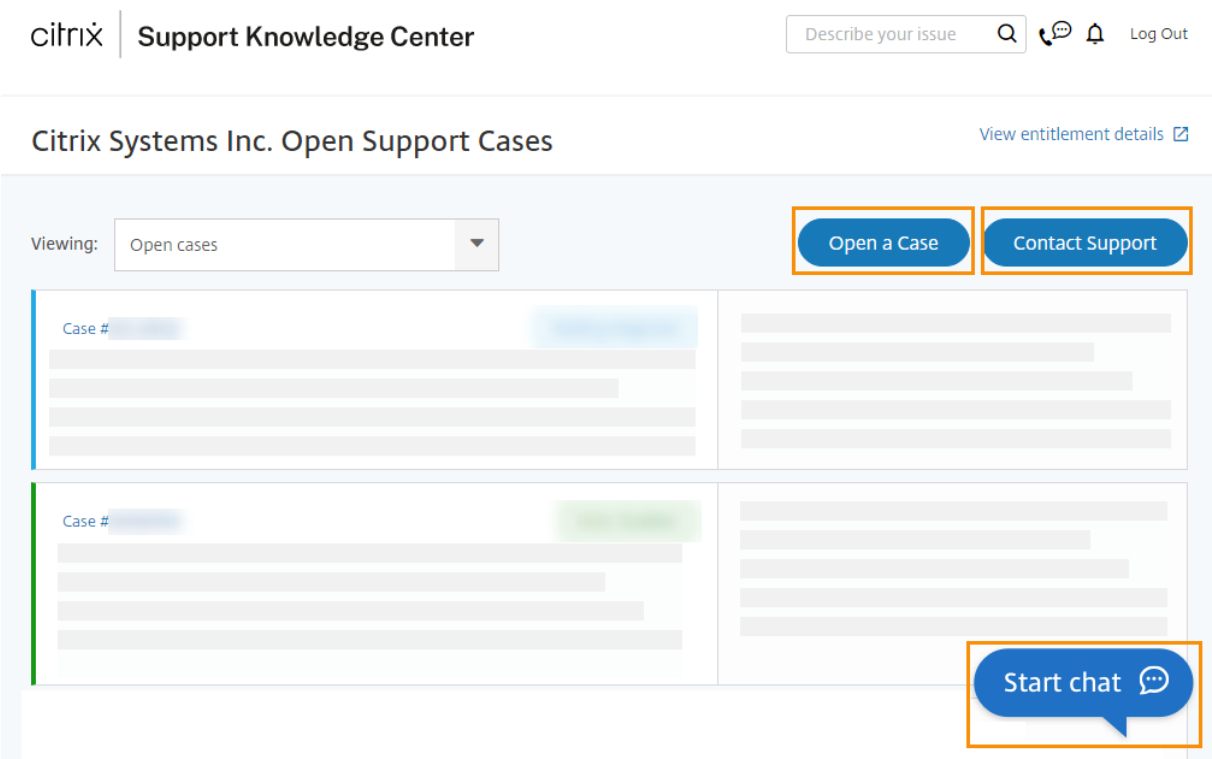
テクニカルサポートが必要な問題が発生した場合は、Citrix Support Knowledge Center にアクセスしてサポートケースを開くか、Citrix テクニカルサポートの担当者にご相談ください。

Support Knowledge Center を利用するには、https://support.citrix.com/case/manageにアクセスしてください。または、Citrix Cloud Japan 管理コンソールで、画面の右上にある ヘルプ アイコンをクリックし、［チケットを開く］**>**［**My Support** に移動］を選択します。その後、Citrix アカウントでサインインできます。



サインイン後、次のいずれかの方法を使用して Citrix テクニカルサポートに連絡してください：

- サポートケースを開始する：［**Open a Case**］を選択し、発生している問題の詳細を入力します。
- 電話：［サポートに連絡］を選択して、Citrix テクニカルサポートへの電話に使用できるリージョンの電話番号一覧を表示します。
- ライブチャット：ページの右下隅にある ［チャットを開始］を選択して、Citrix テクニカルサポートの担当者とチャットします。



サポートフォーラム

Citrix Discussions は Citrix の技術エキスパートのコミュニティであり、Citrix 製品およびサービスに関するヘルプを要求したり、自分の知識を提供したりできます。Citrix Cloud コミュニティ（https://discussions.citrix.com/forum/1704-citrix-cloud/）にアクセスするか、Citrix Cloud Japan の管理コンソールで ［ヘルプ］**>**［ディスカッション］を選択します。

サポート記事とドキュメント

Citrix Cloud Japan を活用し、Citrix 製品で発生する可能性のある問題を解決するための豊富な製品およびサポートコンテンツが用意されています。

Citrix Knowledge Center

特定の技術的な問題に関するヘルプについては、Citrix Knowledge Centerを検索してください。使用している製品を選択するか、問題の説明を入力するだけです。Knowledge Center に、検索内容に関連した記事、セキュリティ情報、更新が表示されます。

Citrix Tech Zone

Citrix Tech Zoneには、Citrix 製品およびサービスの詳細を知るために役立つさまざまな情報が含まれています。ここから、Citrix テクノロジの設計、構築、展開に関する知識情報を提供するリファレンスアーキテクチャ、図、ビデオ、技術資料を参照することができます。

Citrix Cloud Japan に登録する

November 21, 2023

ここでは、Citrix Cloud Japan に登録し、アカウントの登録に必要なタスクを確実に実行するプロセスについて説明します。

OrgID とは何ですか?

OrgID は、Citrix Cloud Japan アカウントに割り当てられた一意の識別子です。OrgID は物理的なサイトアドレス（通常は所属する会社のビジネスアドレス）に関連付けられています。そのため組織には通常、1 つの OrgID があります。ただし、ブランチオフィスが異なる場合や、部門ごとに資産を個別に管理する場合などは、Citrix では単一の組織が複数の OrgID を所有できます。

Citrix Cloud Japan アカウントとは何ですか?

Citrix Cloud Japan アカウントを使うと、1 つまたは複数の Citrix Cloud サービスによって、アプリケーションとデータを安全に配信できます。また、Citrix Cloud Japan アカウントは、OrgID によって一意に識別されます。同じ OrgID で購入と管理者のアクセスを継続できるよう、組織が OrgID をセットアップした方法に基づいて、適切な Citrix Cloud Japan アカウントを選択することが重要です。

多要素認証の要件

Citrix Cloud Japan では、アカウントを安全に保つため、すべてのお客様に対して多要素認証の登録を必須としています。登録に必要なものは、Citrix SSO などの認証アプリがインストールされた、コンピューターやモバイルデバイスなどのデバイスのみです。

Citrix の既存の顧客の場合、Citrix Cloud Japan でサインアップページにアクセスし、Citrix.com アカウントに関連付けられている資格情報を使って登録するように求められます。Citrix を初めて使用する場合は、Citrix Cloud Japan のサインアッププロセスにおいて、Citrix アカウントを作成した後に登録するように求められます。

登録ページへのアクセス

https://onboarding.citrixcloud.jp/にアクセスして、登録フォームに記入します。

Citrix Cloud Japan では、サインイン時に業務用のメールアドレスをユーザー名として使用します。指定の業務用メールアドレスは、次の要件を満たしている必要があります:

- 他の **Citrix Cloud** アカウント（**Citrix Cloud Japan** を含む）で既に使用しているメールアドレスとは異なるアドレスを指定する必要があります。たとえば、別の Citrix Cloud アカウント（citrix.cloud.com）の管理者である場合、Citrix Cloud はそのメールアドレスを記録しています。登録済みのメールアドレスで Citrix Cloud Japan に新規登録することはできません。
- **Citrix Cloud Japan** で既に使用しているメールアドレスとは異なるアドレスを指定する必要があります。たとえば、Citrix Cloud Japan アカウントの管理者としての招待を承諾した場合、Citrix Cloud Japan はそのメールアドレスを記録します。登録済みのメールアドレスで Citrix Cloud Japan に新規登録することはできません。
- **citrix.com** ドメインのメールアドレスは使用できません。Citrix Cloud Japan は、citrix.com ドメインのメールアドレスを承認しません。

利用規約への同意

登録フォームを送信すると、Citrix Cloud Japan にホームリージョンが表示されます。現在、Citrix Cloud Japan には地理的なリージョンが 1 つしかないため、このリージョンのみが表示されます。

利用規約に同意し、［続行］をクリックします。Citrix Cloud Japan で確認ページが表示され、確認メールが送信されます。これでアカウントのパスワードが設定できるようになります。

メールアドレスの確認

確認メールの ［サインイン］リンクをクリックします。数分経っても確認メールが届かない場合は、Web ブラウザーの Citrix Cloud Japan の確認ページにある ［再送信］リンクをクリックしてください。

パスワードの作成とサインイン

Citrix Cloud Japan アカウントで使用する強力なパスワードを入力して確認し、［アカウントの作成］をクリックします。アカウントの最初の管理者は、このパスワードとメールアドレスを使用して Citrix Cloud Japan にサインインします。

その後、上記で選択したメールアドレスとパスワードを使用してCitrix Cloud Japanにサインインできます。

多要素認証に登録する

Citrix Cloud Japan では、管理者アカウントの安全を確保するため、サインイン時に多要素認証の使用を必須としています。多要素認証に登録することで、管理者アカウントへの不正アクセスを防止でき、必要なのは Citrix SSO などの時間ベースのワンタイムパスワード標準に準拠した認証アプリがインストールされたコンピューターやモバイルデバイスなどのデバイスのみになります。

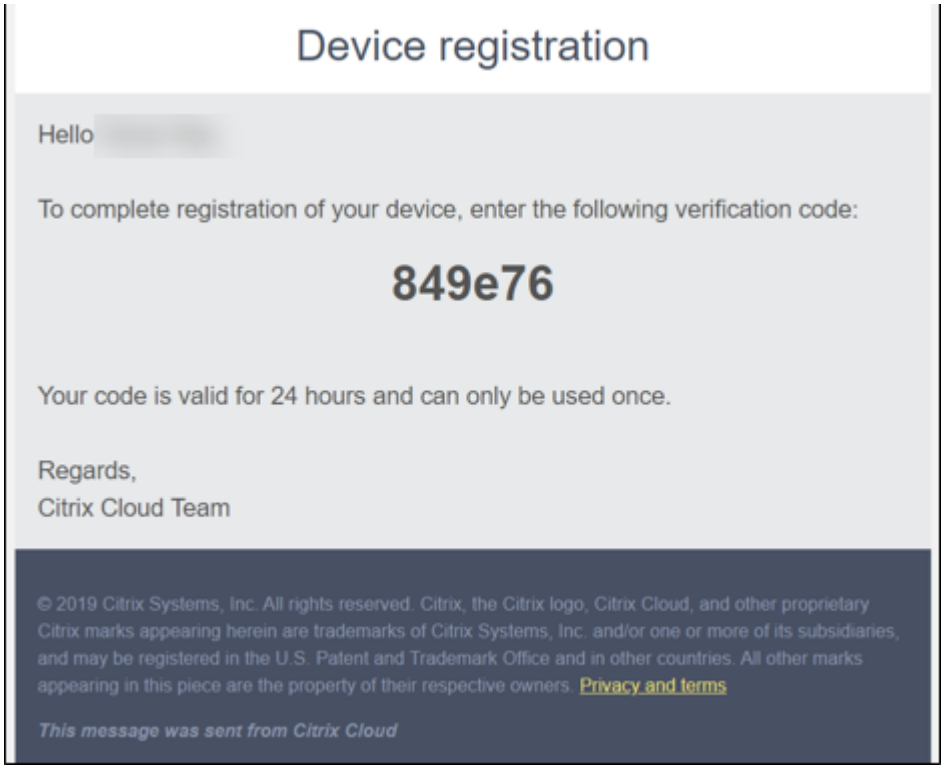
多要素認証に登録していない場合、サインイン時に登録するよう Citrix Cloud Japan から求められます。

登録時に、QR コードとキーが Citrix Cloud Japan により提示されます。認証アプリに応じて、QR コードをスキャンするか、キーを入力してデバイスを登録できます。スムーズな登録処理のために、Citrix ではこのアプリを事前にデバイスにダウンロードしてインストールすることをお勧めします。Citrix Cloud Japan はまた、デバイスを紛失した場合や認証アプリを使用できない場合にアカウントにアクセスするための、1 回のみ使用できるバックアップコードを生成します。

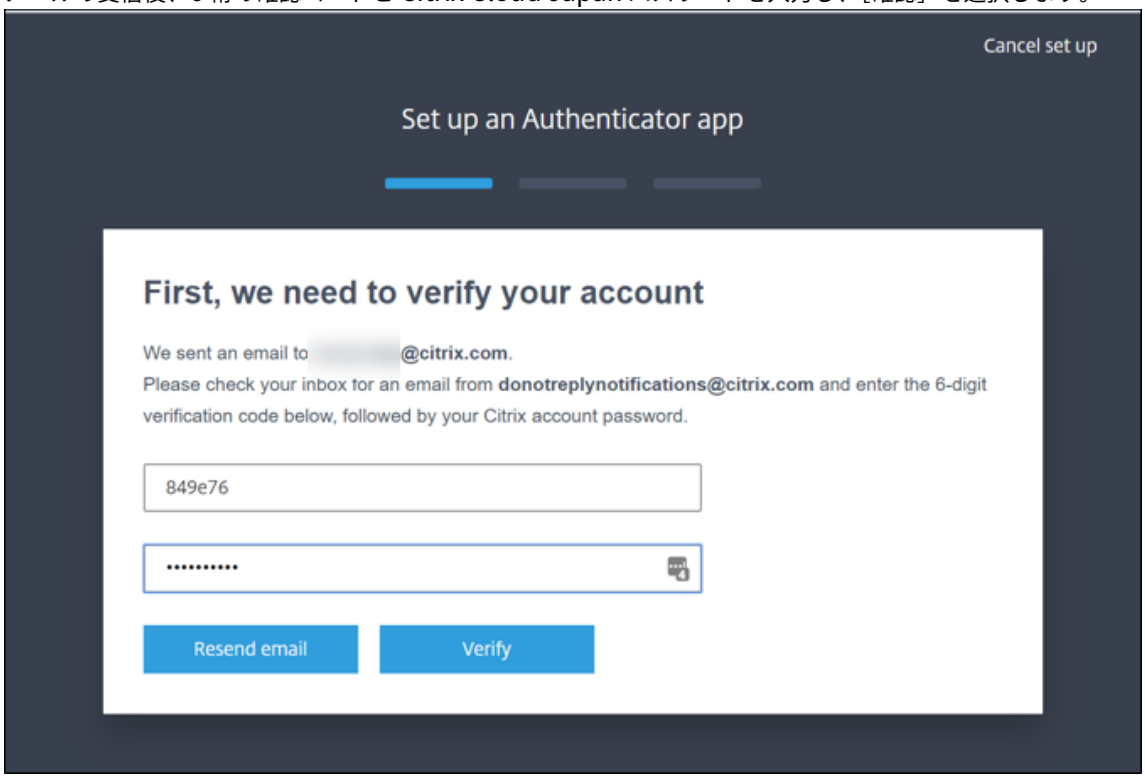
> 注:
>
> - Citrix Cloud Japan 経由で多要素認証に登録できるのは、Citrix ID プロバイダーの管理者のみです。Azure AD を使用して Citrix Cloud Japan 管理者を管理する場合、Azure ポータルを使用して多要素認証を構成できます。詳しくは、Microsoft Web サイトの「Azure AD Multi-Factor Authentication の設定を構成する」を参照してください。
> - 登録後、Citrix Cloud Japan 管理者が所属するすべての顧客組織に多要素認証が適用されます。登録プロセスの完了後に多要素認証を無効にすることはできません。
> - 登録できるデバイスは 1 つだけです。後から別のデバイスを登録すると、Citrix Cloud Japan は現在のデバイス登録を削除し、新しいデバイスに置き換えます。詳しくは、「プライマリ MFA メソッドを管理する」を参照してください。

デバイスを多要素認証に登録するには

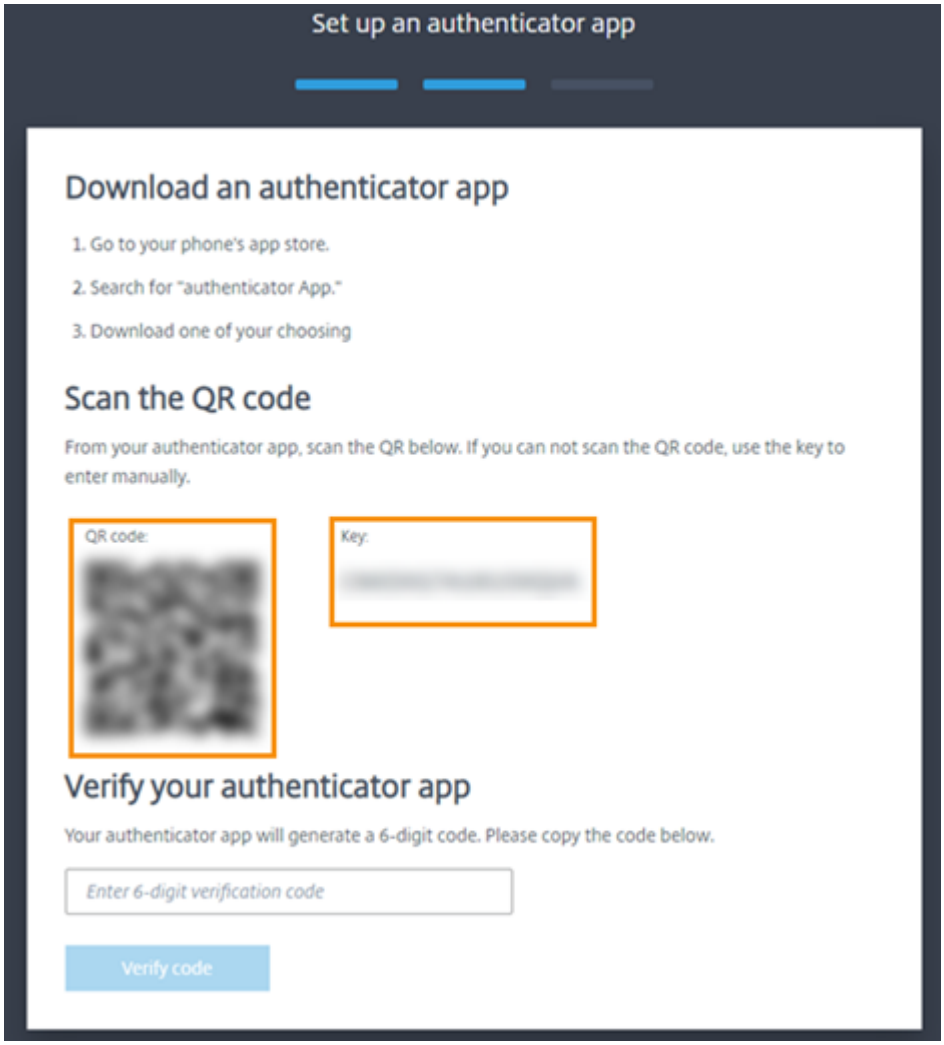
1. https://citrix.citrixcloud.jpにアクセスして、Citrix Cloud Japan の資格情報を入力してください。
2. 多要素認証に登録するよう求められたら、［今すぐ登録］を選択します。Citrix Cloud Japan から、確認コードが記載されたメールが送信されます。



3. メールの受信後、6 桁の確認コードと Citrix Cloud Japan パスワードを入力し、［確認］を選択します。

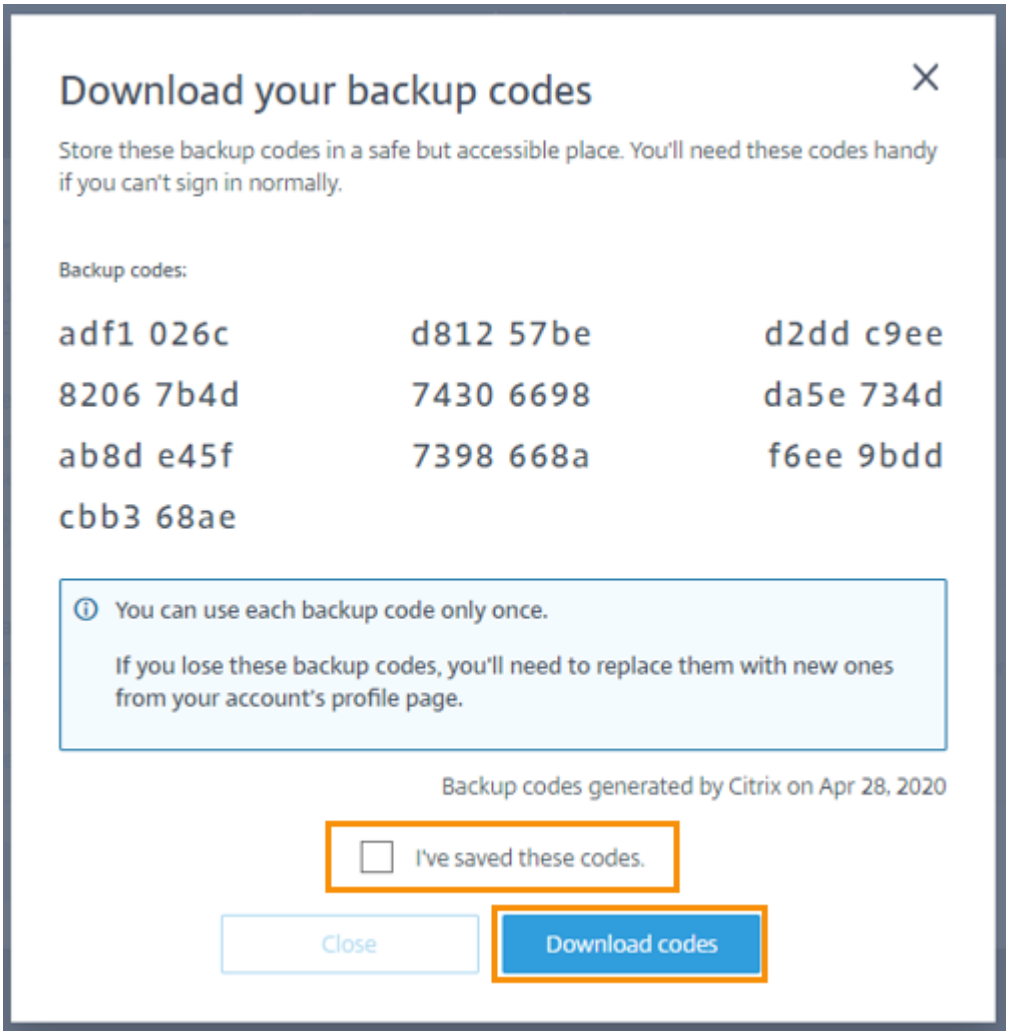


4. 認証アプリで QR コードをスキャンするか、キーを手動で入力します。認証アプリが Citrix Cloud Japan のエントリを表示し、6 桁のコードを生成します。



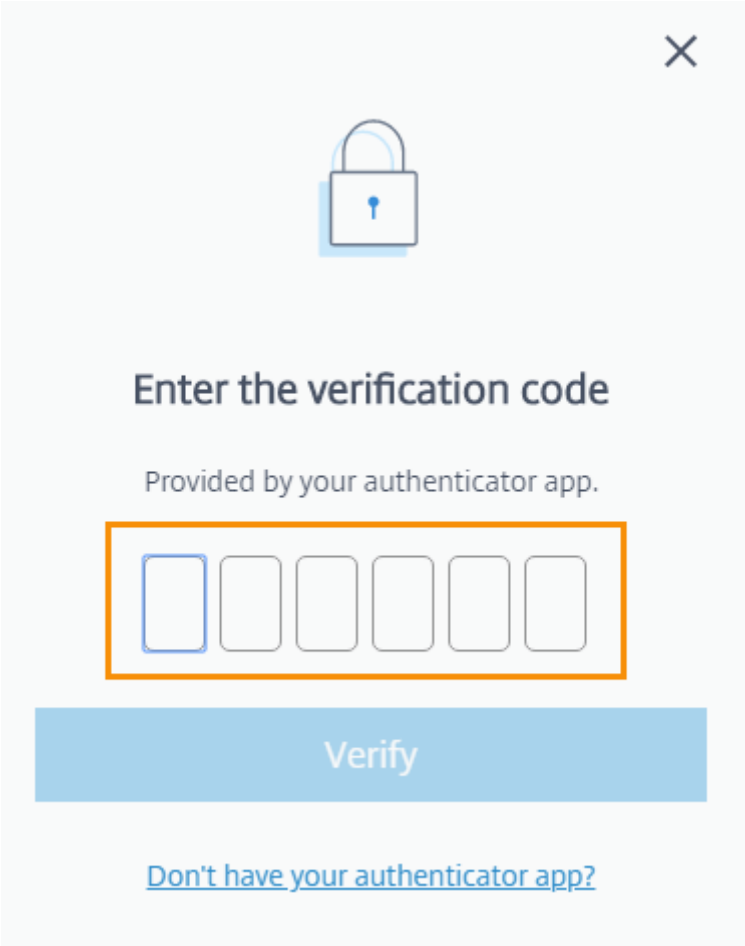
5. ［認証アプリを確認する］で認証アプリのコードを入力して ［コードを確認する］を選択します。
6. デバイスを紛失した場合、または認証アプリを使用できない場合のために、以下のアカウントの復旧方法を構成します:

   - 復旧用の電話番号（必須）:［復旧用の電話番号を追加する］を選択して、Citrix サポートがユーザーの本人確認のために連絡できる電話番号を入力します。Citrix サポートは、サインインのサポートに必要な場合にのみこの電話番号を使用します。固定電話の電話番号を使用することを Citrix ではお勧めします。
   - バックアップコード（必須）: 認証アプリを使用できない場合のサインインに役立つ 1 回のみ使用できるバックアップコードのセットを作成するには、［バックアップコードを生成する］を選択します。メッセージが表示されたら、［コードをダウンロードする］を選択して、バックアップコードをテキストファイルとしてダウンロードします。次に、［バックアップコードを保存しました。］、［閉じる］を選択します。



7. ［完了］を選択して登録を完了します。

次に Citrix Cloud Japan 管理者の資格情報でサインインすると、認証アプリからの確認コードの入力が求められます。



デバイスの登録を管理する

あとで別のデバイスを登録したり、バックアップコードを追加で生成したり、復旧用の電話番号を更新したりする必要がある場合は、［マイプロファイル］ページからこれらのタスクを実行できます。手順については、以下の記事を参照してください:

- プライマリ MFA メソッドを管理する
- MFA の復旧方法を管理する

Citrix Cloud Japan の購入

組織で Citrix Cloud Japan を購入するには、Citrix の営業担当者にお問い合わせください。注文を完了すると、アカウントを設定するためのリンクが記載された確認メールが届きます。アカウントを設定するときに、注文時のメールアドレスと指定したパスワードを使用して最初のアカウント管理者を作成します。

注文を確認する

注文の確認メールのリンクをクリックします。Citrix Cloud Japan セットアップページが Web ブラウザーのウィンドウに表示され、注文の詳細が示されます。［続行］をクリックします。

パスワードを作成する

Citrix Cloud Japan アカウントで使用する強力なパスワードを入力して確認し、［続行］をクリックします。アカウントの最初の管理者は、注文時のこのパスワードとメールアドレスを使用して Citrix Cloud Japan にサインインします。

Citrix Cloud Japan の資格情報でサインインする

1. 注文時に使用したメールアドレスと上記で選択したパスワードを使用して、https://citrix.citrixcloud.jpで Citrix Cloud Japan にサインインします。Citrix Cloud Japan にホームリージョンが表示されます。現在、Citrix Cloud Japan には地理的なリージョンが 1 つしかないため、このリージョンのみが表示されます。
2. 利用規約に同意し、［続行］をクリックします。Citrix Cloud Japan 管理コンソールが開きます。

Citrix Cloud Japan のサービストライアル

November 21, 2023

個別のクラウドサービスのトライアルは、Citrix Cloud Japan プラットフォームで配信されます。サービストライアルの機能は、製品版サービスと同じであるため、概念実証（POC）、パイロットなどの用途に適しています。

エクスペリエンスをカスタマイズして、ユーザーに必要なサービスを提供するために、トライアルへのアクセスはサービスごとに管理されています。

サービスを購入する場合、トライアルを製品版アカウントに移行します。再構成したり、製品版アカウントを別途作成する必要はありません。

サービストライアルに関する事実

		Citrix Cloud Japan トライアル
	許可される利用者の数	25
	最大使用日数	60 暦日。サービスのトライアルをリクエストできるのは一度のみです。

		Citrix Cloud Japan トライアル
	可用性	制限された可用性
	リソースの場所	顧客が提供および構成
	ユーザーセッションの長さ	無制限
	ローカルの Microsoft Active Directory との統合	はい
	リソースの場所の選択	はい
	オンプレミスへの展開	はい
	Citrix DaaS	完全な機能セット
	カスタマイズ可能	はい

サービストライアルの要求

サービストライアルをリクエストするには、シトリックスの営業担当者に相談し、組織 ID（OrgID）を提供する必要があります。営業担当者は、サービスの使用を開始するために必要なすべての情報を確実に入手できるようにします。

トライアルをリクエストして OrgID を確認するには、次の手順を実行します:

1. Citrix Cloud Japan アカウントにサインインします。
2. ［使用可能なサービス］で、試したいサービスを見つけて、［トライアルのリクエスト］をクリックします。
3. 表示される通知に記載された OrgID を書き留めます。
4. ［営業担当者に相談する］をクリックして、トライアルのリクエストを登録します。

トライアルが承認され使用の準備が整うと、メールの通知が届きます。トライアルの完了まで、60 日間使用できます。

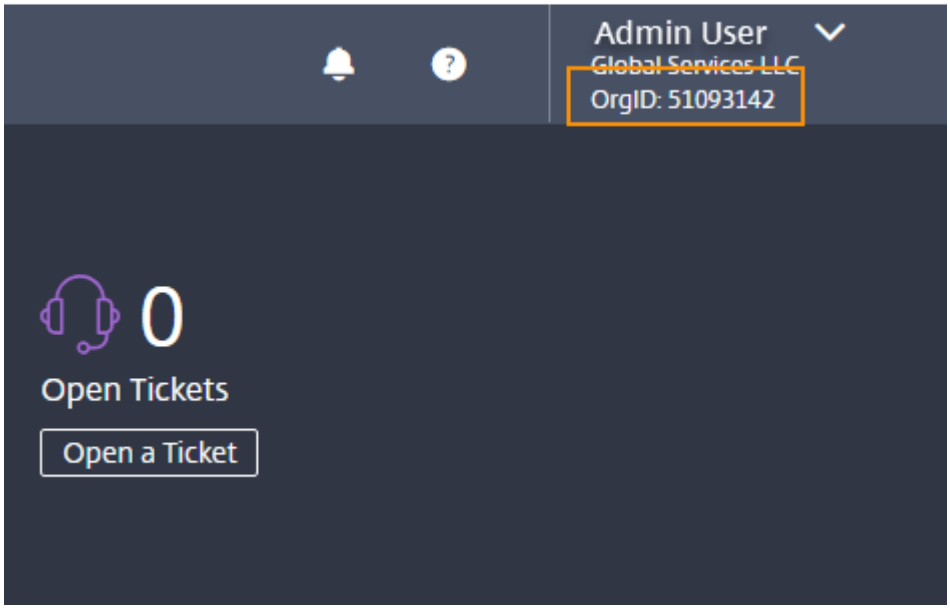
> 注:
>
> カスタマーエクスペリエンスを最大化するために、シトリックスにはトライアルに一度に参加できるユーザー数を制限する権利があります。

サービスの購入

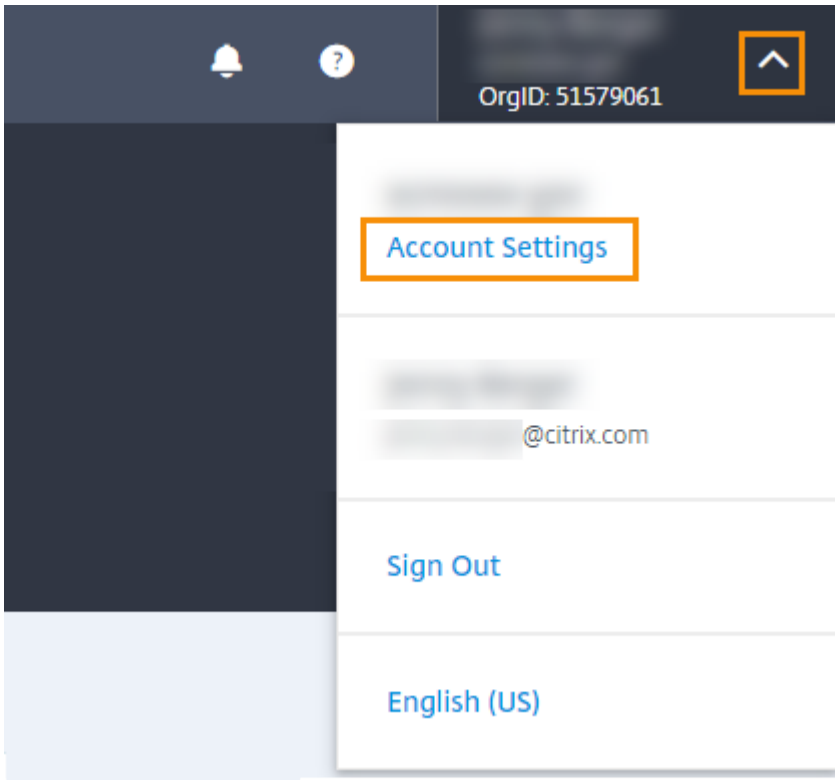
トライアルを製品版サービスに移行する場合は、https://www.citrix.com/buy/にアクセスしてください。

購入を完了するには、Citrix Cloud Japan 管理コンソールで利用可能な OrgID が必要です。OrgID は次の場所に表示されます:

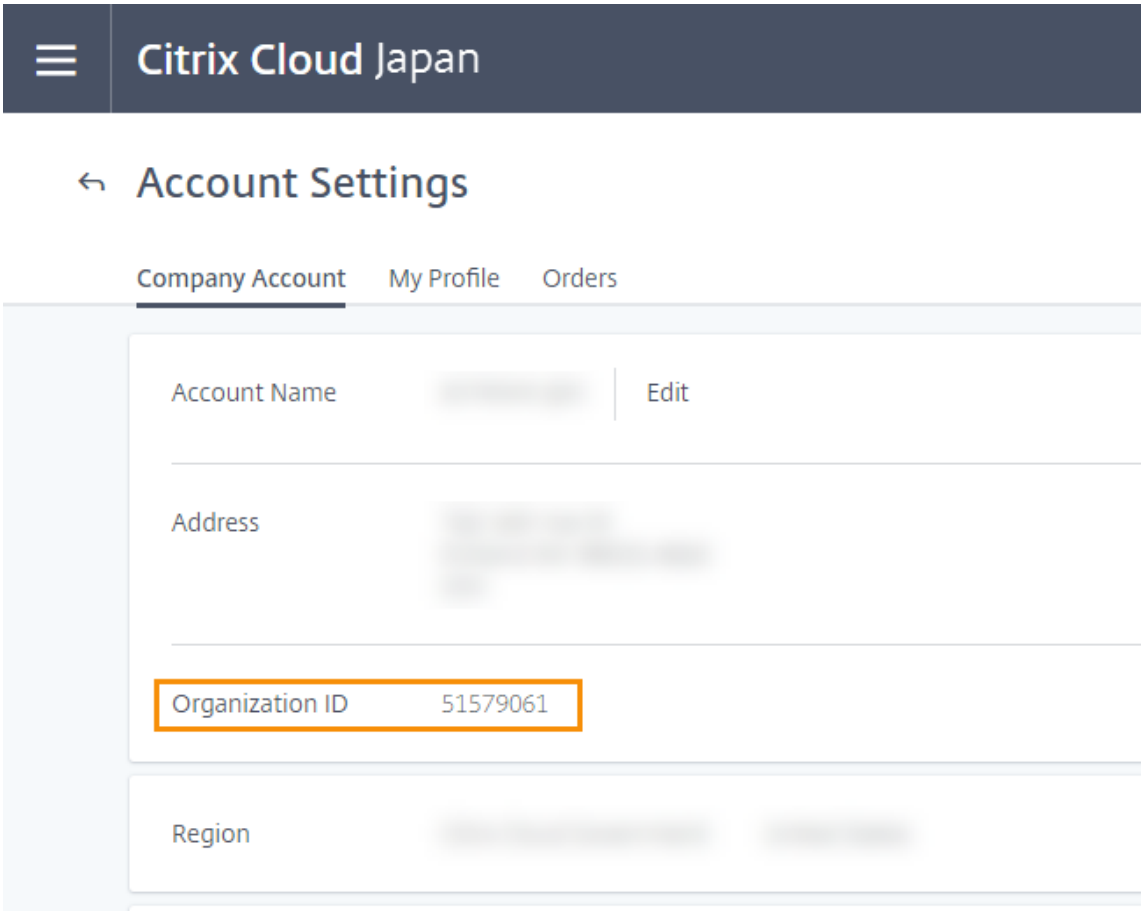
- 管理コンソールの右上隅に、OrgID がアカウント名の下に表示されます。



- 右上のメニューから、［アカウント設定］をクリックします。



組織 ID フィールドに OrgID が表示されます。



> 重要:
>
> 60 日間のトライアル期間終了までに購入しない場合、サービスは終了し、すべてのデータと設定は 90 日間 Citrix にアーカイブされます。90 日間の期間内に購入すると、トライアルが再度アクティブになり、製品版サービスに移行されます。

システム要件

November 21, 2023

このトピックで説明されていないシステム要件コンポーネント（Workspace アプリなど）については、各コンポーネントのドキュメントを参照してください。

Windows サーバーにインストール可能な製品コンポーネントと機能に関しては、Server Core のインストールは、別途記載がない限りサポートされていません。

ハードウェアの提供は複雑かつ動的であるため、デスクトップおよびアプリケーションを配信する仮想マシンのサイジングについて、特定の推奨事項を示すことはできません。すべての展開には、固有のニーズがあります。通常、仮想

マシンのサイジングはユーザーのワークロードではなくハードウェアに基づきます（RAM 以外。より多く消費するアプリケーションにはより多くの RAM が必要です）。仮想マシンのサイジングに関するガイダンスについては、Citrix Tech Zone Web サイトの以下のリソースを参照してください：

- 設計上の決定事項：Azure での Citrix DaaS 提供のスケーラビリティと経済性
- Google Cloud Compute Engine での VDA インスタンスのサイジング
- リファレンスアーキテクチャ：Citrix DaaS - AWS
- 技術概要：Citrix Desktops-as-a-Service（DaaS）のローカルホストキャッシュ/高可用性モード

最小システム要件

Citrix Cloud Japan には、次のコンポーネントが必要です：

- Active Directory ドメイン
- Citrix Cloud Connector ソフトウェアがインストールされたドメインに参加している 2 つの物理マシンまたは仮想マシン。詳しくは、「Citrix Cloud Connector の技術詳細」を参照してください。
- ユーザーに提供するサービスに必要なワークロードやその他のコンポーネントをホストするための、ドメインに参加している物理マシンまたは仮想マシン。

サポートされる **Web** ブラウザー

- 最新バージョンの Google Chrome
- 最新バージョンの Mozilla Firefox
- 最新バージョンの Microsoft Edge
- 最新バージョンの Apple Safari

Transport Layer Security（**TLS**）の要件

Citrix Cloud Japan は、コンポーネント間の TCP ベースの接続で TLS（Transport Layer Security）1.2 をサポートしています。Citrix Cloud Japan は、TLS 1.0 または TLS 1.1 を介した通信を許可していません。

Citrix Cloud Japan にアクセスするには、TLS 1.2 対応のブラウザーを使用して、承認済みの暗号の組み合わせを構成している必要があります。詳しくは、「暗号化とキー管理」を参照してください。

追加要件

- サービス接続：接続要件
- Citrix Cloud Connector：Citrix Cloud Connector の要件
- Citrix DaaS（Virtual Apps and Desktops サービスの新名称）：システム要件
- Workspace アプリ：要件はプラットフォームによって異なります。詳しくは、Workspace アプリのドキュメントを参照してください。

サービス接続要件

June 18, 2024

Citrix Cloud Japan では、管理機能（Web ブラウザー経由）および顧客の展開環境のリソースに接続される（他のインストールされたコンポーネントからの）操作要求を使用できます。ここでは、展開のリソースと Citrix Cloud Japan との接続を確立するための要件および考慮事項を定義します。

データセンターからインターネットへの接続に必要なのは、発信接続のためにポート 443 を開くことです。ただし、インターネットのプロキシサーバーまたはファイアウォールの制限がある環境で操作するには、追加の構成が必要です。詳しくは、「Citrix Cloud Connector のプロキシとファイアウォールの構成」を参照してください。

管理コンソール

Citrix Cloud Japan 管理コンソールは、https://citrix.citrixcloud.jpにサインインすると使用できる Web ベースのコンソールです。コンソールの Web ページでは、サインイン時またはその後に特定の操作を実行するために、インターネットの他のリソースが必要になります。

プロキシとファイアウォールの構成

プロキシサーバー経由で接続すると、管理コンソールは使用している Web ブラウザーに適用された構成と同じ構成で機能します。コンソールは、ユーザー環境で機能するため、ユーザー認証を必要とするプロキシサーバーの構成は通常どおりに機能します。

管理コンソールを機能させる場合、発信接続のためにポート 443 を開いている必要があります。コンソール内を移動して、一般的な接続性をテストできます。

詳しくは、「Citrix Cloud Connector のプロキシとファイアウォールの構成」を参照してください。

コンソール通知

管理コンソールは Pendo を使用して、重要なアラート、新機能に関する通知、一部の機能とサービスに関する製品内ガイダンスを表示します。管理コンソール内で Pendo のコンテンツを表示できるようにするために、Citrix ではアドレス`https://citrix-cloud-content.customer.pendo.io/`を利用できるようにすることをお勧めします。

以下サービスは、Pendo コンテンツを表示します:

- Citrix DaaS（旧称 Virtual Apps and Desktops サービス）
- Citrix Workspace

Pendo は、Citrix が顧客にクラウドサービスおよびサポートサービスを提供するために使用するサードパーティのサブプロセッサです。これらのサブプロセッサの完全な一覧については、「Sub-Processors for Citrix Cloud & Support Services and Citrix Affiliates」を参照してください。

セッションのタイムアウト

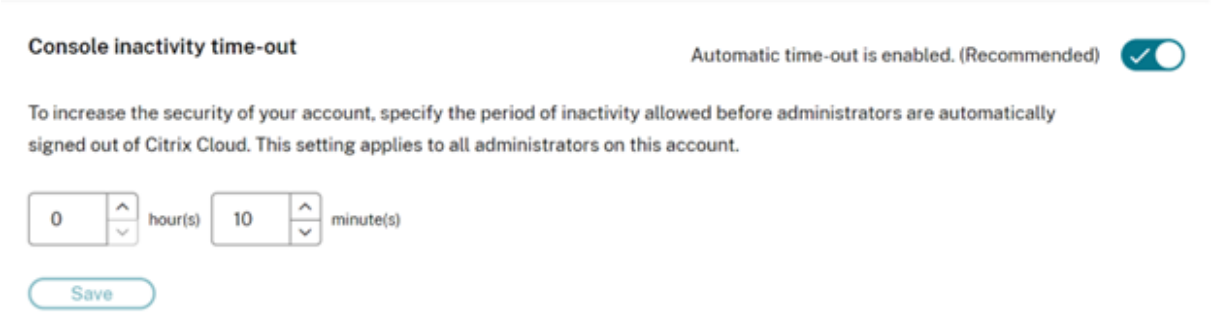
管理者が Citrix Cloud Japan にサインインした後、次の間隔が経過すると、管理コンソールセッションがタイムアウトします:

- アイドルセッション（コンソールアクティビティが検出されない）: 60 分
- 最大セッションタイムアウト（コンソールアクティビティに関係なく）: 24 時間

最大セッションタイムアウトが経過すると、保存されていない構成の変更はすべて失われ、管理者は再度サインインする必要があります。

コンソールの非アクティブタイムアウトを設定可能

フルアクセス管理者は、管理者が自動的にサインアウトされるまでの Citrix Cloud コンソールでの非アクティブ期間を構成できます。一度構成されると、指定されたタイムアウト期間は Citrix Cloud アカウントのすべての管理者に適用されます。



この機能を有効にすると、管理者は設定された非アクティブ期間後にログアウトされ、その後のログインごとにセッションタイムアウトがリセットされます。

この機能が無効になっている場合、非アクティブタイマーは存在せず、管理者は 72 時間のセッション制限に達した場合にのみログアウトされます。

> 注:
>
> - デフォルトでは、この機能は無効になっています。
> - 構成可能な非アクティブタイムアウトは 10 分から 12 時間です。
> - 非アクティブタイムアウトのデフォルト値は 60 分間です。

Citrix Cloud Connector

Citrix Cloud Connector は、Microsoft Windows サーバーで実行されるサービスセットを展開するソフトウェアパッケージです。Cloud Connector をホストするマシンは、Citrix Cloud Japan で使用するリソースが存在するネットワーク内にあります。Cloud Connector は Citrix Cloud Japan に接続し、必要に応じてリソースを操作および管理することができます。

Cloud Connector をインストールするための要件については、「Citrix Cloud Connector の要件」を参照してください。操作には、Cloud Connector がポート 443 を使用して発信する必要があります。インストール後、使用されているクラウドサービスに応じて、Cloud Connector にアクセス要件が追加される場合があります。

一般的なサービス接続要件

次の表では、ほとんどの Citrix Cloud Japan サービスや機能に共通したアドレスを表示します。Citrix Cloud Japan サービスは動的であり、IP アドレスは定期的に変更されるため、これらのアドレスはドメイン名としてのみ提供されます。

必要なアドレス	機能
`https://*.citrixworkspacesapi.jp`	サービスが使用する Citrix Cloud API へのアクセスを提供します。
`https://*.citrixcloud.jp`	Citrix Cloud Japan サインインインターフェイスへのアクセスを提供します。
`https://*.blob.core.windows.net`	Citrix Cloud Connector の更新を格納する Azure Blob Storage へのアクセスを提供します。
`https://*.servicebus.windows.net`	ログおよび Active Directory エージェントに使用される Azure Service Bus へのアクセスを提供します。

ベストプラクティスとして、グループポリシーを使用してこれらのアドレスを構成して管理します。また、組織で消費するサービスに適用できるアドレスのみを構成してください。

証明書の検証

Cloud Connector が通信する Cloud Connector バイナリおよびエンドポイントは、ソフトウェアのインストール時に検証された X.509 証明書で保護されています。これらの証明書を検証するには、各 Cloud Connector マシンが次の要件を満たしている必要があります:

- HTTP ポート 80 が *.digicert.com に対して開かれている。このポートは、Cloud Connector のインストール時と定期的な証明書失効一覧チェック中に使用されます。
- 次のアドレスは通信可能である必要があります:


```
- http://*.digicert.com
- https://*.digicert.com
- https://dl.cacerts.digicert.com/DigiCertAssuredIDRootCA.crt
- https://dl.cacerts.digicert.com/DigiCertSHA2AssuredIDCodeSigningCA
  .crt
```

これらの証明書について詳しくは、「証明書の検証要件」を参照してください。

SSL 暗号化解除

一部のプロキシで SSL 暗号化解除を有効にすると、Cloud Connector が Citrix Cloud Japan に正常に接続できなくなる可能性があります。この問題の解決について詳しくは、CTX221535を参照してください。

Citrix Gateway

- 一般的なサービス接続要件
- `https://*.*.nssvc.jp`

すべてのサブドメインを有効にできない顧客は、代わりに次のアドレスを使用できます:

- `https://*.g.nssvc.jp`
- `https://*.c.nssvc.jp`

Citrix DaaS

> 注:
>
> Citrix DaaS は、Virtual Apps and Desktops サービスの新名称です。

Citrix リソースの場所/Cloud Connector:

- 一般的なサービス接続要件
- `https://*.citrixworkspacesapi.jp`
- `https://*.citrixcloud.jp`
- `https://*.blob.core.windows.net`
- `https://*.citrixworkspacesapi.net`
- `https://*.servicebus.windows.net`
- 新機能や重要なコミュニケーションを含む製品内メッセージの場合: `https://citrix-cloud-content.customer.pendo.io/`

Cloud Connector がサービスと通信する方法の概要については、Citrix Tech Zone の Web サイトにある「Citrix DaaS の図」を参照してください。

管理コンソール:

- https://*.citrixworkspacesapi.jp
- https://*.citrixcloud.jp
- https://*.blob.core.windows.net
- https://*.apps.citrixworkspacesapi.net

Citrix Workspace

- https://*.citrixcloud.jp
- https://*.citrixdata.com
- 新機能や重要なコミュニケーションを含む製品内メッセージの場合: https://citrix-cloud-content.customer.pendo.io/

Workspace Environment Management サービス

- https://*.wem.citrixcloud.jp

Citrix Cloud Connector の要件

March 27, 2024

Citrix Cloud Connector は、Windows Server 2016、Windows Server 2019、または Windows Server 2022 にインストールされた Windows サービスで構成されています。

システム要件

Cloud Connector をホストするマシンは、次の要件を満たしている必要があります: 高可用性を確保するため、Citrix では、それぞれのリソースの場所に Cloud Connector を 2 つ以上インストールすることを強くお勧めします。

Citrix DaaS での Cloud Connector マシンの構成に関するベストプラクティスについては、「Cloud Connector のスケールおよびサイズの考慮事項」を参照してください。

オペレーティングシステム

次のオペレーティングシステムがサポートされています:

- Windows Server 2022
- Windows Server 2019

- Windows Server 2016

Cloud Connector は、Windows Server Core での使用はサポートされていません。

.NET の要件

Microsoft .NET Framework 4.7.2 以降が必要です。

サーバーの要件

次の要件は、Cloud Connector がインストールされているすべてのマシンに適用されます。

- Cloud Connector をホストするために専用のマシンを使用します。そのマシンには他のコンポーネントをインストールしないでください。
- マシンが Active Directory ドメインコントローラーとして構成されていないこと。ドメインコントローラーへの Cloud Connector のインストールはサポートされていません。
- サーバークロックを正しい UTC 時間に設定済み。
- Internet Explorer のセキュリティ強化の構成（IE ESC）がオフになっていること。Internet Explorer のセキュリティ強化の構成が有効な場合、Cloud Connector が Citrix Cloud Japan との接続を確立できないことがあります。
- Cloud Connector をホストしているすべてのマシンで、Windows Update を有効にすることを Citrix では強くお勧めします。Windows Update を構成するときに、自動的に更新プログラムをダウンロードしてインストールするようにしてください。ただし、自動再起動は許可しないでください。Citrix Cloud Japan プラットフォームの処理により、必要に応じて一度に 1 つの Cloud Connector のみに対応してマシンの再起動が行われます。グループポリシーを使用して更新後にマシンが再起動するタイミングを制御することもできます。詳しくは、https://docs.microsoft.com/en-us/windows/deployment/update/waas-restartを参照してください。

証明書の検証要件

Cloud Connector が通信する Cloud Connector バイナリとエンドポイントは、広く評価された商用証明機関（CA）が発行した X.509 証明書で保護されています。公開キー基盤（PKI）の証明書の検証機能には、証明書失効一覧（CRL）があります。クライアントは証明書を受け取ると、証明機関の信頼性を検証し、証明書が証明書失効一覧（CRL）にあるかどうかを確認します。
証明書が CRL にある場合は失効し、有効であると表示された場合でも信頼できないと判断されます。

CRL サーバーは、ポート 443 の HTTPS ではなくポート 80 の HTTP を使用します。Cloud Connector コンポーネント自体は、外部のポート 80 とは通信しません。外部ポート 80 が必要となるのは、オペレーティングシステムが実行する証明書検証プロセスのためです。

X.509 証明書は、Cloud Connector のインストール時に検証されます。そのため、すべての Cloud Connector マシンは、これらの証明書を信頼するように構成して、Cloud Connector ソフトウェアを正常にインストールできるようにする必要があります。

Citrix Cloud Japan エンドポイントは、DigiCert によって発行された証明書、または Azure によって使用されるルート証明機関の 1 つにより保護されています。Azure で使用されるルート証明機関について詳しくは、https://docs.microsoft.com/ja-jp/azure/security/fundamentals/tls-certificate-changesを参照してください。

証明書を検証するには、各 Cloud Connector マシンが次の要件を満たしている必要があります:

- HTTP ポート 80 が、以下のアドレスに対して開かれている。このポートは、Cloud Connector のインストール時と定期的な CRL チェック中に使用されます。CRL および OCSP 接続をテストする方法について詳しくは、DigiCert Web サイトのhttps://www.digicert.com/kb/util/utility-test-ocsp-and-crl-access-from-a-server.htmを参照してください。
  - http://cacerts.digicert.com/
  - http://dl.cacerts.digicert.com/
  - http://crl3.digicert.com
  - http://crl4.digicert.com
  - http://ocsp.digicert.com
  - http://www.d-trust.net
  - http://root-c3-ca2-2009.ocsp.d-trust.net
  - http://crl.microsoft.com
  - http://oneocsp.microsoft.com
  - http://ocsp.msocsp.com
- 以下のアドレスとの通信が有効になっている:
  - https://*.digicert.com
- 以下のルート証明書がインストールされている:
  - https://cacerts.digicert.com/DigiCertAssuredIDRootCA.crt
  - https://cacerts.digicert.com/DigiCertGlobalRootG2.crt
  - https://cacerts.digicert.com/DigiCertGlobalRootCA.crt
  - https://cacerts.digicert.com/DigiCertTrustedRootG4.crt
  - https://cacerts.digicert.com/BaltimoreCyberTrustRoot.crt
  - https://www.d-trust.net/cgi-bin/D-TRUST_Root_Class_3_CA_2_2009.crt
  - https://www.microsoft.com/pkiops/certs/Microsoft%20RSA%20Root%20Certificate%20Authority%202017.crt
  - https://www.microsoft.com/pkiops/certs/Microsoft%20EV%20ECC%20Root%20Certificate%20Authority%202017.crt

  - https://www.microsoft.com/pkiops/certs/Microsoft%20ECC%20Root%20Certificate%20Authority%202017.crt

- 以下の中間証明書がインストールされている:
  - https://cacerts.digicert.com/DigiCertTrustedG4CodeSigningRSA4096SHA384.crt
  - https://cacerts.digicert.com/DigiCertSHA2AssuredIDCodeSigningCA.crt

いずれかの証明書がない場合、Cloud Connector インストーラーはhttp://cacerts.digicert.comから該当する証明書をダウンロードします。

証明書をダウンロードおよびインストールする手順について詳しくは、CTX223828を参照してください。

Active Directory の要件

- ユーザー用のオファリングを作成するために使用するリソースとユーザーを含む Active Directory ドメインに参加済み。
- Citrix Cloud Japan で使用する予定の各 Active Directory フォレストには、常に 2 つの Cloud Connector がアクセスできるようにする必要があります。
- Cloud Connector は、子ドメインコントローラーだけでなく親ドメインコントローラーにもアクセスできる必要があります。これは、Cloud Connector がインストールされている Active Directory ワークフローを完了するために不可欠です。

詳しくは、次の Microsoft サポート記事を参照してください:
- Active Directory ドメインと信頼のファイアウォールを構成する方法
- システムサービスのポート

ネットワークの要件

- リソースの場所で使用するリソースに接続できるネットワークに接続済み。詳しくは、「Cloud Connector のプロキシとファイアウォールの構成」を参照してください。
- インターネットに接続済み。詳しくは、「インターネット接続の要件」を参照してください。

サポートされる **Active Directory** の機能レベル

Citrix Cloud Connector は、Active Directory フォレストとドメインの以下の機能レベルをサポートします。

フォレスト機能レベル	ドメイン機能レベル	サポートされるドメインコントローラー
Windows Server 2008 R2	Windows Server 2008 R2	Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016
Windows Server 2008 R2	Windows Server 2012	Windows Server 2012、Windows Server 2012 R2、Windows Server 2016
Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2012 R2、Windows Server 2016
Windows Server 2008 R2	Windows Server 2016	Windows Server 2016
Windows Server 2012	Windows Server 2012	Windows Server 2012、Windows Server 2012 R2、Windows Server 2016
Windows Server 2012	Windows Server 2012 R2	Windows Server 2012 R2、Windows Server 2016
Windows Server 2012	Windows Server 2016	Windows Server 2016
Windows Server 2012 R2	Windows Server 2012 R2	Windows Server 2012 R2、Windows Server 2016
Windows Server 2012 R2	Windows Server 2016	Windows Server 2016
Windows Server 2016	Windows Server 2016	Windows Server 2016、Windows Server 2019、Windows Server 2022

FIPS（Federal Information Processing Standard）のサポート

Cloud Connector は現在、FIPS 対応のマシンで使用される、FIPS 検証済みの暗号化アルゴリズムをサポートしています。このサポートは、Citrix Cloud Japan で利用可能な Cloud Connector ソフトウェアの最新バージョンにのみ含まれています。お使いの環境に既存の Cloud Connector マシンがあり（2018 年 11 月より前にインストール）、そのマシンで FIPS モードを有効にする場合は、次の操作を実行します：

1. リソースの場所にある各マシンで Cloud Connector ソフトウェアをアンインストールします。
2. 各マシンで FIPS モードを有効にします。
3. FIPS 対応の各マシンに最新バージョンの Cloud Connector をインストールします。

> 重要：
>
> - 既存の Cloud Connector インストールを最新バージョンにアップグレードしないでください。必ず古

> い Cloud Connector をアンインストールしてから、新しい Cloud Connector をインストールします。
> - 古いバージョンの Cloud Connector をホストするマシンでは、FIPS モードを有効にしないでください。バージョン 5.102 より古い Cloud Connector は FIPS モードをサポートしていません。古い Cloud Connector がインストールされているマシンで FIPS モードを有効にすると、Citrix Cloud Japan が Cloud Connector の定期的なメンテナンス更新を実行できなくなります。

Cloud Connector の最新バージョンをダウンロードする手順については、「タスク 3: Cloud Connector のインストール」を参照してください。

Cloud Connector で許可されている FQDN

Cloud Connector がアクセスする完全修飾ドメイン名（FQDN）の完全な一覧については、次の場所にある JSON ファイルを参照してください: https://fqdnallowlistsa.blob.core.windows.net/fqdnallowlist-japan/allowlist.json。この一覧は製品ごとに編成されており、FQDN のグループごとに変更ログがあります。

これらの FQDN の一部は、顧客に固有のものであり、角かっこで囲まれたテンプレート化されたセクションがあります。これらのテンプレート化されたセクションは、使用する前に実際の値に置き換える必要があります。たとえば、<CUSTOMER_ID>.xendesktop.netの場合、<CUSTOMER_ID>を Citrix Cloud アカウントの実際の顧客 ID に置き換えます。顧客 ID は、[**ID** およびアクセス管理] の [**API** アクセス] タブの上部に表示されます。

インストール要件

- Cloud Connector ソフトウェアは、Citrix Cloud Japan からのみダウンロードし、準備されたマシンにインストールします。デフォルトでは、Cloud Connector インストーラーは、ダウンロード元のコントロールプレーンとの接続を試みます。そのため、Citrix Cloud（citrix.cloud.com）アカウントからダウンロードしたソフトウェアをインストールしようとすると、インストーラーは Citrix Cloud Japan に接続しません。
- Cloud Connector ソフトウェアがダウンロードされるように、ブラウザーが実行可能ファイルのダウンロードを許可するようにしておく必要があります。

クローンマシンに関する考慮事項

Cloud Connector をホストする各マシンには、一意の SID とコネクタ ID が必要です。これにより、Citrix Cloud Japan がリソースの場所内のマシンと通信できるようになります。（複製前に）Cloud Connector をマシンテンプレートにインストールすることはサポートされていません。Cloud Connector をインストールしたマシンを複製すると、Cloud Connector サービスが実行されなくなり、マシンは Citrix Cloud Japan に接続できなくなります。

リソースの場所の複数のマシンで Cloud Connector をホストし、クローンマシンを使用する場合は、次の手順を実行します:

1. 使用環境に合わせてマシンテンプレートを準備します。
2. Cloud Connector として使用する数のマシンをプロビジョニングします。

3. 手動またはサイレントインストールモードを使用して、各マシンに Cloud Connector をインストールします。

使用に関する重要な注意事項

- すべての Cloud Connector の電源を常にオンにして、Citrix Cloud Japan への常時接続を確保します。
- 以前にインストールした Cloud Connector を新しいバージョンにアップグレードしないでください。古い Cloud Connector をアンインストールしてから、新しいバージョンをインストールしてください。
- Cloud Connector をホストしているすべてのマシンで、Windows Update を有効にすることを Citrix では強くお勧めします。
- 各リソースの場所に少なくとも 2 つの Cloud Connector をインストールすることを Citrix では強くお勧めします。一般に、インストールする必要がある Cloud Connector の数は N+1 です。ここで、N はリソースの場所内のインフラストラクチャをサポートし、いずれかの Cloud Connector が使用できなくなった場合でも Citrix Cloud Japan とリソースの場所の間の接続が損なわれないようにするために必要な処理能力を有する数です。
- Citrix Cloud Japan で使用する予定の各 Active Directory フォレストには、常に 2 つの Cloud Connector がアクセスできるようにする必要があります。
- インストール後、Cloud Connector をホストしているマシンを別のドメインに移動しないでください。マシンが別のドメインに参加する必要がある場合は、Cloud Connector をアンインストールし、ドメインに参加した後に再インストールします。

Cloud Connector でインストールされるサービス

このセクションでは、Cloud Connector とともにインストールされるサービスとそのシステム権限について説明します。

インストール中に、Citrix Cloud Connector 実行可能ファイルがインストールされ、機能に必要なサービス構成がデフォルトに設定されます。デフォルトの構成を手動で変更すると、Cloud Connector が正常に動作しない可能性があります。この場合、更新プロセスを処理するサービスが引き続き機能できると仮定すると、次の Cloud Connector 更新が発生したときに、構成はデフォルトの状態にリセットされます。

Citrix Cloud Agent System は、他の Cloud Connector サービスが機能するために必要なすべての呼び出しを昇格させ、ネットワーク上で直接通信しません。Cloud Connector 上のサービスがローカルシステム権限が要求されるアクションを実行する必要がある場合、Citrix Cloud Agent System によって可能な事前定義された一連の操作によって実行します。

サービス名	説明	実行アカウント
Citrix Cloud Agent System	オンプレミスエージェントに必要なシステムコールを処理します。インストール、再起動、レジストリアクセスが含まれます。Citrix Cloud Services Agent WatchDog によってのみ呼び出すことができます。	ローカルシステム
Citrix Cloud Services Agent WatchDog	オンプレミスエージェント（エバーグリーン）を監視およびアップグレードします。	ネットワークサービス
Citrix Cloud Services Agent Logger	Citrix Cloud Connector サービスのサポートログフレームワークを提供します。	ネットワークサービス
Citrix Cloud Services AD Provider	インストールされている Active Directory ドメインアカウントに割り当てられたリソースを Citrix Cloud Japan で容易に管理できます。	ネットワークサービス
Citrix Cloud Services Agent Discovery	XenApp および XenDesktop のレガシーオンプレミス製品を Citrix Cloud Japan で容易に管理できます。	ネットワークサービス
Citrix Cloud Services Credential Provider	暗号化されたデータの保存と取得を処理します。	ネットワークサービス
Citrix Cloud Services WebRelay Provider	WebRelay Cloud サービスから受信した HTTP 要求をオンプレミスの Web サーバーに転送できます。	ネットワークサービス
Citrix CDF Capture Service	すべての構成済み製品およびコンポーネントから CDF トレースをキャプチャします。	ネットワークサービス
Citrix Config Synchronizer Service	仲介の構成をローカルに高可用性モードでコピーします。	ネットワークサービス
Citrix High Availability Service	中央サイトの停止中にサービスの継続性を提供します。	ネットワークサービス
Citrix ITSM Adapter Provider	Virtual Apps and Desktops のプロビジョニングと管理を自動化します。	ネットワークサービス

サービス名	説明	実行アカウント
Citrix NetScaler Cloud Gateway	受信ファイアウォール規則を開いたり、DMZ にコンポーネントを展開したりする必要なく、オンプレミスのデスクトップおよびアプリケーションにインターネット接続を提供します。	ネットワークサービス
Citrix Remote Broker Provider	ローカルの VDA および StoreFront サーバーからリモートの Broker Service への通信を有効にします。	ネットワークサービス
Citrix Remote HCL Server	Delivery Controller と 1 つまたは複数のハイパーバイザー間の通信をプロキシ接続します。	ネットワークサービス
Citrix Session Manager Proxy	匿名の事前起動セッションを管理し、セッション数情報をクラウドベースのセッションマネージャーサービスにアップロードします。	ネットワークサービス
Citrix WEM Cloud Authentication Service	Citrix WEM エージェントがクラウドインフラストラクチャサーバーに接続するための認証サービスを提供します。	ネットワークサービス
Citrix WEM Cloud Messaging Service	Citrix WEM クラウドサービスがクラウドインフラストラクチャサーバーからメッセージを受信するためのサービスを提供します。	ネットワークサービス

イベントメッセージとログ

Cloud Connector は、Windows イベントビューアーに表示できる特定のイベントメッセージを生成します。優先する監視ソフトウェアを有効にしてこれらのメッセージを検索する場合は、ZIP アーカイブとしてダウンロードできます。この ZIP アーカイブは、次の XML ファイルにこれらのメッセージを含みます:

- Citrix.CloudServices.Agent.Core.dll.xml（Connector Agent Provider）
- Citrix.CloudServices.AgentWatchDog.Core.dll.xml（Connector AgentWatchDog Provider）

Cloud Connector のイベントメッセージをダウンロードします。（ZIP ファイル）

トラブルシューティング

Cloud Connector の問題を診断するための最初の手順は、イベントメッセージとイベントログを確認することです。Cloud Connector がリソースの場所に表示されない、または「接続していない」場合は、イベントログに初期情報が表示されます。

インストール

Cloud Connector が「エラー」状態の場合、Cloud Connector のホストに問題がある可能性があります。Cloud Connector を新しいマシンにインストールしてください。問題が解決されない場合は、Citrix サポートに連絡してください。Cloud Connector のインストールまたは使用に関する一般的な問題のトラブルシューティングについては、CTX221535を参照してください。

展開の計画と構築

December 13, 2022

Citrix Cloud Japan に登録した後、以下の手順で Citrix Cloud Japan への接続をセットアップします。事前にプロセスの全体像を確認しておくことで、行う操作を把握できます。

リソースの場所を設定する

リソースの場所には、インフラストラクチャサーバー（Active Directory ドメインや Cloud Connector など）と、ユーザーにアプリケーションやデスクトップを提供するマシンが含まれています。Citrix DaaS（Virtual Apps and Desktops サービスの新名称）を使用するには、リソースの場所を設定する必要があります。

手順については、「リソースの場所の作成」を参照してください。

次のビデオで、リソースの場所の作成と Cloud Connector の追加に関するデモをご覧いただけます。

これは埋め込みビデオです。リンクをクリックしてビデオを見る

ID プロバイダーを接続する

ID プロバイダーは、Citrix Cloud Japan 管理者およびワークスペース利用者を認証し、利用者にライブラリオファリングを割り当てるためのユーザー一覧へのアクセスを提供するために使用されます。

サポートされる ID プロバイダーについて詳しくは、「ID およびアクセス管理」を参照してください。

Citrix DaaS をセットアップする

Citrix DaaS の使用を開始するには、次のタスクを完了します:

1. サブスクリプションをお持ちでない場合は、サービストライアルをリクエストします。サービストライアルは 60 日間有効で、製品版サービスとすべて同じ機能を備えています。
2. Citrix DaaS 環境の顧客管理コンポーネントのシステム要件を確認し、それに応じてマシンを準備します。
3. Citrix DaaS ドキュメントの「展開の計画と構築」にある一連のタスクを確認し、各タスクの手順に従います。

Citrix Workspace をセットアップする

エンドユーザー用のワークスペースの設定には、次のタスクが含まれます:

1. ワークスペース構成で Virtual Apps and Desktops サービス統合を有効にします。
2. ワークスペース認証方法として、先ほど接続した ID プロバイダーを選択します。
3. エンドユーザーに提供するワークスペース機能を構成します。

Citrix Cloud Japan の Citrix Workspace アプリで使用できる機能について詳しくは、「ワークスペースのセットアップ」を参照してください。

リソースの場所の作成

March 1, 2024

Citrix Cloud Japan に登録した後、リソースの場所を作成してアカウントのセットアップを続行します。

リソースの場所とは何ですか**?**

リソースの場所には、ユーザーにサービスを提供するために必要なリソースが含まれます。リソースの場所に含まれるリソースは、提供するサービスによって異なります。たとえば、Citrix DaaS（Virtual Apps and Desktops サービスの新名称）を通じてアプリケーションとデスクトップを配信する場合、リソースの場所には次のものが含まれます:

- アプリケーションとデスクトップにアクセスするユーザーを認証および承認するための Active Directory ドメイン。
- 1 つまたは複数の Citrix Virtual Delivery Agent（VDA）が必要です。これらは、アプリケーションをホストするマシンと、配信するデスクトップとの間の接続を管理します。また、それらのリソースへのアクセスに使用されるデバイスもカバーします。
- アプリケーションとデスクトップを提供する仮想マシンをプロビジョニングするための、Citrix XenServer や Microsoft Azure などのサポートされているハイパーバイザーやクラウドサービス。

デフォルトのリソースの場所

Citrix Cloud Japan アカウントにリソースの場所がなく、ドメインに Cloud Connector をインストールする場合:

- Citrix Cloud Japan はリソースの場所を作成します。
- この作成されたリソースの場所が、デフォルトのリソースの場所になります。

アカウントに設定できるデフォルトのリソースの場所は 1 つだけです。必要に応じて、Citrix Cloud Japan に追加のリソースの場所を作成できます。これによって、他のドメインに Cloud Connector をインストールするときにいずれかを選択できます。

または、最初にコンソールで必要なリソースの場所を作成してから、ドメインに Cloud Connector をインストールすることもできます。Cloud Connector インストーラーは、インストール中に、必要なリソースの場所を選択するよう求めます。

タスク **1**: マシンの準備

1. 次に関するCitrix Cloud Connector の要件を確認します:
    - 要件
    - 重要な注意事項
    - サポートされる Active Directory の機能レベル
    - トラブルシューティング情報。
2. 構成要件を満たすマシンを準備します。
3. 準備したマシンをドメインに参加させます。

タスク **2**: 接続の確認

データセンターからインターネットへの接続に必要なのは、発信接続のためにポート 443 を開くことです。ただし、インターネットのプロキシサーバーまたはファイアウォールの制限がある環境で操作するには、追加の構成が必要です。

1. 利用できるサービスの接続可能なアドレス一覧については、「接続の要件」を確認してください。
2. ポート 443（HTTPS）が発信接続用に開放されていることを確認します。
3. クラウドサービスの操作と利用を可能にするために必要なアドレスに到達できることを確認します。
4. Web プロキシでの Cloud Connector の使用については、「Citrix Cloud Connector のプロキシとファイアウォールの構成」を参照してください。

タスク **3**: **Cloud Connector** のインストール

> 注:
>
> Connector Appliance は Citrix Cloud Japan では使用できません。

インストール中、Cloud Connector は次のことを行うためにクラウドにアクセスする必要があります

- ユーザーの ID を確認してインストールプロセスを承認する
- インストーラーの権限を確認する
- Cloud Connector が提供するサービスをダウンロードして構成する。

インストールは、インストールを開始するユーザーの権限で行われます。

1. Citrix Cloud Japan メニューから ［リソースの場所］を選択します。
2. ［ダウンロード］をクリックして、Cloud Connector インストーラーをダウンロードします。
3. インストーラーをダブルクリックします。Citrix Cloud Japan が最初の接続性チェックを実行すると、Citrix Cloud Japan 管理者のユーザー名とパスワードの入力を求められます。
4. ウィザードに従って、Cloud Connector をインストールして構成します。インストールが完了すると、Citrix Cloud Japan は最終的な接続性チェックを実行して、Cloud Connector が Citrix Cloud Japan と通信できることを検証します。

インストール後、Citrix Cloud Japan の ［**ID** およびアクセス管理］に管理者のドメインが登録されます。

> メモ:
>
> - 複数の組織アカウントの管理者である場合、Citrix Cloud Japan が Cloud Connector に関連付けるアカウントを選択するよう要求します。
> - 組織アカウントに複数のリソースの場所が既に存在する場合､Citrix Cloud Japan が Cloud Connector に関連付けるリソースの場所を選択するよう要求します。
> - 一定期間にわたって同じ Cloud Connector インストーラーを使用して繰り返しインストールすることはお勧めしません。Citrix Cloud コンソールの［リソースの場所］ページから新しい Cloud Connector をダウンロードします。

追加のリソースの場所を作成

1. Citrix Cloud Japan 管理コンソールでメニューボタンをクリックし、［リソースの場所］を選択します。
2. ［リソースの場所］をクリックして、フレンドリ名を入力します。
3. ［保存］をクリックします。Citrix Cloud Japan は、新しいリソースの場所のタイルを表示します。
4. ［**Cloud Connector**］、［ダウンロード］の順にクリックして、Cloud Connector ソフトウェアを入手します。
5. 準備した各マシンで、インストールウィザードまたはコマンドラインインストールを使用して Cloud Connector ソフトウェアをインストールします。

Cloud Connector のインストールログ

Cloud Connector のインストールログは**%LOCALAPPDATA%\Temp\CitrixLogs\CloudServicesSetup** にあります。

インストール後は**%ProgramData%\Citrix\WorkspaceCloud\InstallLogs** にすべてのログが追加されます。

コマンドラインから **Cloud Connector** をインストールする

March 27, 2024

Citrix Cloud Connector ソフトウェアは、手動（インタラクティブ）でインストールすることも、サイレントインストールまたは自動インストールを使用することもできます。

Cloud Connector のインストール時、ユーザーを認証し、権限を検証し、サービスをダウンロードして構成するために、クラウドアクセスが必要です。インストールは、インストールを開始するユーザーの権限で行われます。

> 重要:
>
> 長期間にわたって同じインストーラーで繰り返しインストールしないでください。代わりに、Citrix Cloud Japan コンソールの［リソースの場所］ページから新しい Cloud Connector を取得します。

要件

Citrix Cloud Japan でコマンドラインを使用してインストールするには、次の情報を入力する必要があります:

- Cloud Connector をインストールする Citrix Cloud Japan アカウントの顧客 ID。この ID は、［**ID** およびアクセス管理］の ［**API** アクセス］タブの上部に表示されます。
- Cloud Connector のインストールに使用するセキュア API クライアントのクライアント ID とシークレット。これらの値を取得するには、まずセキュアクライアントを作成する必要があります。クライアント ID とシークレットにより、Citrix Cloud API へのアクセスが適切に保護されます。セキュアクライアントを作成すると、クライアントは、作成者と同じ管理者権限で動作します。Cloud Connector をインストールするには、フルアクセス権限を持つ管理者によって作成されたセキュアクライアントを使用します。これによって、フルアクセス権限を利用できます。
- Cloud Connector に関連付けるリソースの場所の ID。この値を取得するには、［リソースの場所］ページのリソースの場所の名前の下にある ［**ID**］ボタンを選択します。この値を指定しない場合、Citrix Cloud Japan ではデフォルトのリソースの場所の ID が使用されます。

セキュアクライアントの作成

セキュアクライアントを作成する場合、Citrix Cloud Japan により一意のクライアント ID とシークレットが生成されます。コマンドラインから API を呼び出すときに、これらの値を指定する必要があります。

1. Citrix Cloud Japan メニューから、[**ID** およびアクセス管理] を選択し、次に [**API** アクセス] を選択します。
2. [セキュアクライアント] タブから、クライアントの名前を入力し、[クライアントの作成] を選択します。Citrix Cloud Japan によりセキュアクライアントのクライアント ID とシークレットが生成され、表示されます。
3. [ダウンロード] を選択して、クライアント ID とシークレットを CSV ファイルとしてダウンロードし、安全な場所に保存します。または、[コピー] を選択して、それぞれの値を手動で取得します。完了したら [閉じる] を選択してコンソールに戻ります。

サポートされているパラメーター

セキュアクライアントのセキュリティの詳細では、インストーラーには JSON 構成ファイルが必要です。インストール完了後、このファイルは削除してください。サポートされている構成ファイルの値は次のとおりです:

- **customerName**: 必須。顧客 ID は、Citrix Cloud Japan コンソールの [API アクセス] ページに表示されます。
- **clientId**: 必須。管理者が作成したセキュアクライアント ID は、[API アクセス] ページにあります。
- **clientSecret**: 必須。セキュアクライアントが作成された後にダウンロードできるセキュアクライアントシークレットは、[API アクセス] ページにあります。
- **resourceLocationId**: 推奨。既存のリソースの場所の一意の識別子。Citrix Cloud コンソールの [リソースの場所] ページで、ID ボタンを選択してリソースの場所の ID を取得します。値を指定しない場合、Citrix Cloud はアカウント内の最初のリソースの場所の ID を使用します。
- **acceptTermsOfService**: 必須。**true** に設定する必要があります。

サンプル構成ファイル:

```
{

"customerName": "*CustomerID*",
"clientId": "*ClientID*",
"clientSecret": "*ClientSecret*",
"resourceLocationId": "*ResourceLocationId*"
"acceptTermsOfService": "true",
 }

<!--NeedCopy-->
```

パラメーターファイルを使用してインストールするサンプルコマンドライン:

```
CWCConnector.exe /q /ParametersFilePath:c:\cwcconnector_install_params.
   json
<!--NeedCopy-->
```


エラーが発生した場合に可能性のあるエラーコードを調べるには、「**Start /Wait CWCConnector.exe /ParametersFilePath:value**」を使用します。インストール完了後は、標準的なメカニズムである「**echo %ErrorLevel%**」を使用できます。

トラブルシューティング

インストールログ

インストールログは**%LOCALAPPDATA%\Temp\CitrixLogs\CloudServicesSetup** にあります。

また、インストール後は**%ProgramData%\Citrix\WorkspaceCloud\InstallLogs** にすべてのログが追加されます。

終了コード

- 1603 - 予期しないエラーが発生しました。
- 2 - 前提条件チェックが不合格でした。
- 0 - インストールが正常に完了しました。

Citrix Cloud Connector のプロキシとファイアウォールの構成

November 21, 2023

HTTP トラフィックを使用するポート 443、送信のみ。接続の完全な詳細については、次の記事を参照してください:

- 接続の要件
- Citrix Cloud Connector の要件

Cloud Connector は、Web プロキシサーバー経由のインターネットへの接続をサポートします。インストーラー、インストールするサービス共に Citrix Cloud Japan への接続が必要です。この両方が、インターネットアクセスを利用できるようにする必要があります。

> 重要:
>
> 一部のプロキシで SSL 暗号化解除を有効にすると、Cloud Connector が Citrix Cloud Japan に正常に接続できなくなる可能性があります。この問題の解決について詳しくは、CTX221535を参照してください。

ワイルドカード文字と **FQDN** を使用したトラフィックの除外

Cloud Connector トラフィックを除外するようにプロキシサーバーを構成する場合は、Citrix Cloud Japan のallowlist.jsonに含まれる許可された Cloud Connector の FQDN を使用します。このタイプのトラフィックを除外するためにワイルドカード文字を使用しないでください。

次のコマンドは、Citrix Cloud Connector で許可される FQDN を使用してトラフィックを除外する例です:

```
netsh winhttp set proxy bypass-list agenthub-jp.citrixworkspacesapi.jp
<!--NeedCopy-->
```

詳しくは、「Cloud Connector で許可される FQDN」を参照してください

ワイルドカード文字のアドレスを使用して Cloud Connector トラフィックを除外することはサポートされていません。ワイルドカード文字を使用してバイパスリストを構成すると、これらのアドレスは無視され、Cloud Connector トラフィックが引き続き表示される可能性があります。

インストーラー

インストーラーは、インターネット接続用に構成された設定を使用します。マシンからインターネットを閲覧できるのであれば、インストーラーも機能します。

プロキシ設定の構成について詳しくは、「Windows でのプロキシサーバー設定の変更」を参照してください。

ランタイムのサービス

ランタイムサービスは、ローカルサービスのコンテキストで動作します。上記で説明するように、ユーザー用の設定は使用されません。ブラウザーから設定をインポートする必要があります。

これに合わせてプロキシ設定を構成するには、コマンドプロンプトウィンドウを開き、次のように **netsh** を実行します。

```
netsh winhttp import proxy source =ie
<!--NeedCopy-->
```

コマンドを実行した後、サービスがこのプロキシ設定で起動するように Cloud Connector をホストするマシンを再起動します。

詳しくは、「Netsh Commands for Windows Hypertext Transfer Protocol（WINHTTP）」を参照してください。

> 注:
>
> 自動検出および PAC スクリプトはサポートされていません。

クラウドサービス用の **Connector Appliance**

March 27, 2024

Connector Appliance は、ハイパーバイザーでホストされる Citrix コンポーネントです。Citrix Cloud とリソースの場所との間の通信チャネルとして機能し、複雑なネットワークやインフラストラクチャ構成を必要とせずにクラウドを管理できます。Connector Appliance を使用することで、リソースを管理しながら、ユーザーに価値を提供するリソースに集中することができます。

Connector Appliance は、次の機能を備えています:

- **Active Directory** を **Citrix Cloud** に接続することで、AD の管理を有効にし、リソースの場所内で AD のフォレストとドメインを使用できるようにします。これによって、さらに AD 信頼関係を追加する必要はなくなります。詳しくは、「Connector Appliance を使用した Active Directory」を参照してください。

ただし、次のような Connector Appliance を使用するプレビュー段階のサービスがほかにも存在する可能性があります:

- Image Portability Service
- Citrix Secure Private Access

Connector Appliance プラットフォームは Citrix Cloud Platform および Citrix Identity Platform の一部であり、次の情報を含むデータを処理できます:

- IP アドレスまたは FQDN
- デバイス、ユーザー、およびリソースの場所の識別子
- Timestamp
- イベントデータ
- Active Directory からのユーザーとグループの詳細（ユーザーとグループの認証と検索などに使用されます）

Connector Appliance の可用性と負荷管理

継続的な可用性を確保して負荷を管理するために、各リソースの場所に複数の Connector Appliance をインストールします。Citrix では、各リソースの場所に少なくとも 2 つの Connector Appliance を使用することをお勧めします。ある Connector Appliance を一定期間使用できない場合、他の Connector Appliance がその接続を維持できます。各 Connector Appliance はステートレスであるため、使用可能なすべての Connector Appliance に負荷を分散できます。この負荷分散機能を構成する必要はありません。この機能は自動化されています。少なくとも 1 つの Connector Appliance が利用可能である限り、Citrix Cloud との通信は失われません。

リソースの場所に対してコネクタが 1 つのみ構成されている場合、Citrix Cloud では ［リソースの場所］ページと［コネクタ］ページの両方に警告が表示されます。

Connector Appliance の更新

Connector Appliance は自動的に更新されます。コネクタを更新するためにアクションを実行する必要はありません。

更新が利用可能になるとすぐに適用するか、指定した保守期間中に適用するかをリソースの場所で構成できます。

更新中に、Connector Appliance を一時的に利用できなくなります。更新は、リソースの場所の Connector Appliance に対して、一度に 1 つずつのみに適用されます。そのため、各リソースの場所に少なくとも 2 つの Connector Appliance を登録し、少なくとも 1 つの Connector Appliance を常に利用できるようにしてください。

Connector Appliance の通信

Connector Appliance は、Citrix Cloud とリソースの場所の間ですべての通信を認証および暗号化します。インストールされると、Connector Appliance は発信接続を介して Citrix Cloud との通信を開始します。すべての接続が、標準 HTTPS ポート（443）と TCP プロトコルを使用して Connector Appliance からクラウドに対して確立されます。受信接続は許可されません。

次の表は、Connector Appliance がサービスにアクセスするために必要なポートの一覧です：

サービス	ポート	サポートされるドメインプロトコル	構成の詳細
DNS	53	TCP/UDP	このポートがローカル環境に対して開いている必要があります
NTP	123	UDP	このポートがローカル環境に対して開いている必要があります
HTTPS	443	TCP	Connector Appliance には、このポートへの送信アクセスが必要です

Connector Appliance を構成するには、IT 管理者が Connector Appliance のポート 443（HTTPS）の管理インターフェイスにアクセスできる必要があります。

> 注：
>
> 注：IP アドレスの先頭に`https://`を追加する必要があります。

Connector Appliance はリソースの場所にあるオンプレミスシステムと外部システムのどちらとも通信できます。Connector Appliance の登録時に 1 つ以上の Web プロキシを定義すると、Connector Appliance から外部シス

テムへのトラフィックのみがこの Web プロキシ経由でルーティングされます。オンプレミスシステムがプライベートアドレス領域にある場合、Connector Appliance からこのシステムへのトラフィックは Web プロキシを経由してルーティングされません。

Connector Appliance では、プライベートアドレス領域が以下の IPv4 アドレス範囲として定義されます:

- 10.0.0.0 –10.255.255.255
- 172.16.0.0 –172.31.255.255
- 192.168.0.0 –192.168.255.255

インターネット接続の要件

データセンターからインターネットへの接続に必要なのは、発信接続のためにポート 443 を開くことです。ただし、インターネットのプロキシサーバーまたはファイアウォールの制限がある環境で操作するには、追加の構成が必要です。

Citrix Cloud サービスを適切に操作し消費するには、以下のアドレスが変更していない HTTPS 接続と通信可能である必要があります:

- https://*.cloud.jp
- https://*.citrixworkspacesapi.jp
- https://*.citrixnetworkapi.jp
- https://*.nssvc.net
  - すべてのサブドメインを有効にできない顧客は、代わりに次のアドレスを使用できます:
    - https://*.g.nssvc.net
    - https://*.c.nssvc.net
- https://*.servicebus.windows.net
- https://iwsprodeastusuniconacr.azurecr.io
- https://iwsprodeastusuniconacr.eastus.data.azurecr.io

ネットワークの要件

環境の構成が以下の要件を満たしていることを確認します:

- ネットワークにより、Connector Appliance は DHCP を使用して、DNS および NTP サーバー、IP アドレス、ホスト名、およびドメイン名を取得できます。または、Connector Appliance コンソールでネットワーク設定を手動で設定することもできます。
- このネットワークは、Connector Appliance によって内部的に使用される 169.254.0.1/24、169.254.64.0/18、または 169.254.192.0/18 というリンクローカル IP 範囲を使用するようには構成されていません。

- ハイパーバイザークロックが協定世界時（UTC）に設定され、タイムサーバーと同期されるか、DHCP が NTP サーバー情報を Connector Appliance に提供します。
- Connector Appliance でプロキシを使用する場合、プロキシは認証されていない、または基本認証が使用されている必要があります。

システム要件

Connector Appliance は、次のハイパーバイザーでサポートされています：

- Citrix Hypervisor 8.2 CU1 LTSR
- VMware ESXi バージョン 7 Update 2
- Windows Server 2016、Windows Server 2019、または Windows Server2022 上の Hyper-V。
- Nutanix AHV
- Microsoft Azure
- AWS
- Google Cloud Platform

ハイパーバイザーは以下の最低要件を満たしている必要があります：

- 20GB ルートディスク
- 2 つの vCPU
- 4GB のメモリ
- IPv4 ネットワーク

同じハイパーバイザーホストで複数の Connector Appliance をホストできます。同じホスト上の Connector Appliance の数は、ハイパーバイザーとハードウェアの制限によってのみ制限されます。

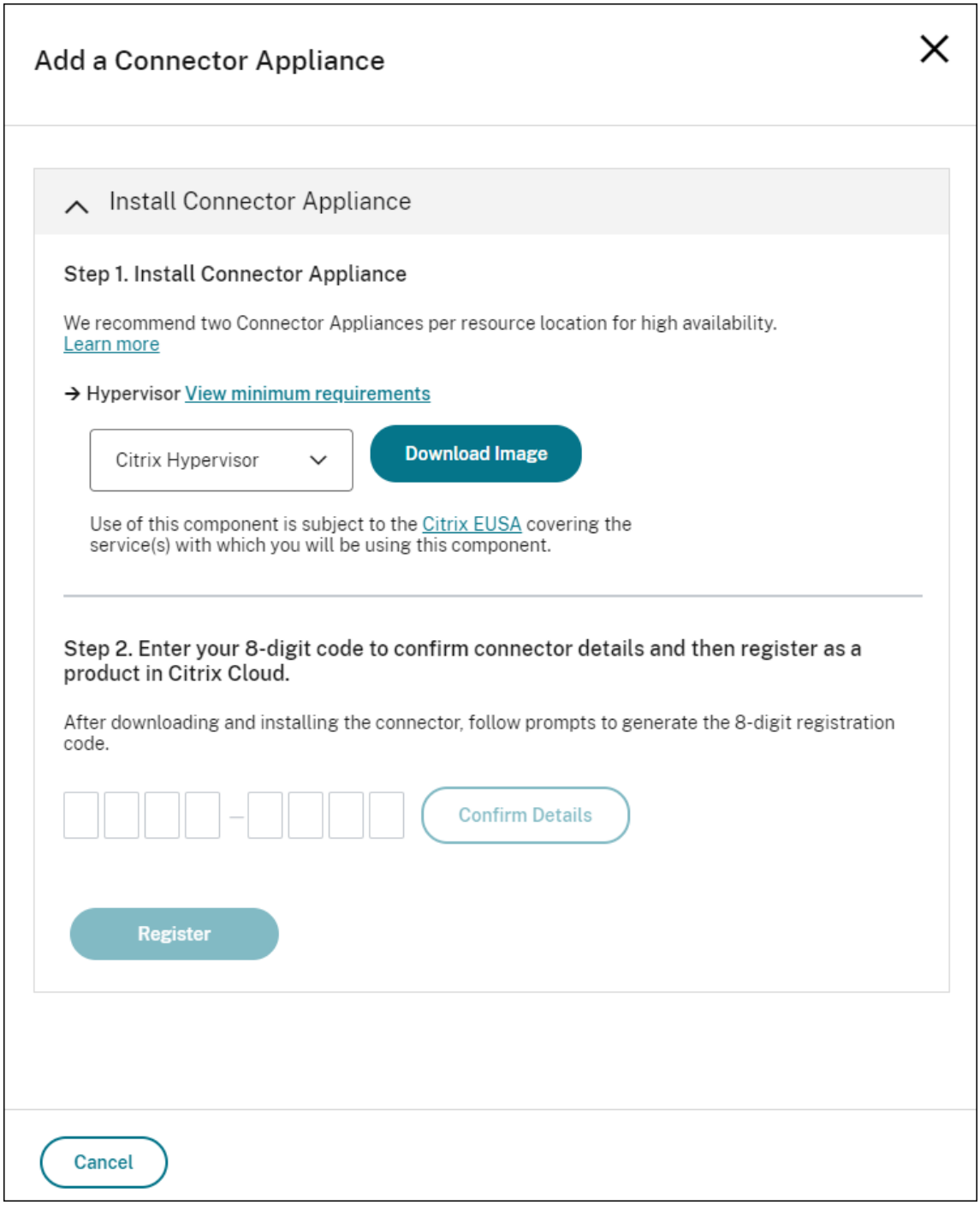
> 注：
>
> Connector Appliance VM のスナップショットの複製、一時停止、および作成はサポートされていません。

Connector Appliance の入手

Citrix Cloud 内から Connector Appliance ソフトウェアをダウンロードします。

1. Citrix Cloud にサインインします。
2. 画面左上のメニューで、［リソースの場所］を選択します。
3. リソースの場所がない場合は、プラスアイコン（+）をクリックするか、［リソースの場所を追加する］を選択します。
4. Connector Appliance を登録するリソースの場所で、［**Connector Appliance**］プラスアイコン（+）をクリックします。

［**Connector Appliance** を追加する］タスクが開きます。



5. ［手順 **1**］の ［ハイパーバイザー］リストから、Connector Appliance をホストするために使用するハイパーバイザーまたはクラウドプロバイダーのタイプを選択します。

   - オンプレミスのハイパーバイザーとクラウド環境の場合、Connector Appliance は Citrix Cloud からダウンロードできます:

     a) ［画像のダウンロード］をクリックします。

b) Citrix エンドユーザーサービス契約を確認して、同意する場合は ［同意して続行する］を選択します。

c) プロンプトが表示されたら、提供された Connector Appliance ファイルを保存します。

Connector Appliance ファイルのファイル拡張子は、選択するハイパーバイザーによって異なります。

- 一部のクラウド環境では、次のマーケットプレイスから Connector Appliance を入手することができます:
  - AWS
  - Microsoft Azure
  - Google Cloud

6. ［**Connector Appliance** のインストール］タスクは開いたままにします。Connector Appliance をインストールした後、［手順 **2**］に登録コードを入力します。

［コネクタ］ページから ［**Connector Appliance** のインストール］タスクに移動することもできます。プラスアイコン（+）を選択してコネクタを追加し、Connector Appliance を追加します。

ハイパーバイザーへの **Connector Appliance** のインストール

- Citrix Hypervisor
- VMware ESXi
- Hyper-V
- Nutanix AHV
- Microsoft Azure
- Google Cloud Platform
- AWS

Citrix Hypervisor

このセクションでは、XenCenter を使用して Citrix Hypervisor サーバーに Connector Appliance をインポートする方法について説明します。

1. ダウンロードした Connector Appliance の XVA ファイルにアクセスできるシステムで XenCenter を使用し、Citrix Hypervisor サーバーまたはプールに接続します。
2. ［ファイル］>［インポート］の順に選択します。
3. Connector Appliance の XVA ファイルが存在するパスを指定または参照します。［次へ］をクリックします。
4. Connector Appliance をホストする Citrix Hypervisor サーバーを選択します。また、Connector Appliance をホストするプールを選択することもできます。それにより、Citrix Hypervisor で適切な使用可能サーバーが選択されます。［次へ］をクリックします。

5. Connector Appliance に使用するストレージリポジトリを指定します。［インポート］をクリックします。
6. ［追加］をクリックし、新しい仮想ネットワークインターフェイスを追加します。［ネットワーク］リストで、使用する Connector Appliance のネットワークを選択します。［次へ］をクリックします。
7. Connector Appliance の展開に使用するオプションを確認します。誤りがある場合は、［戻る］を使用してこれらのオプションを変更します。
8. ［インポート完了後すぐに新規 **VM** を自動的に起動する］が選択されていることを確認します。［完了］をクリックします。

Connector Appliance が展開され、正常に起動すると、そのコンソールに Connector Appliance の IP アドレスを含むランディングページが表示されます。この IP アドレスを使用して Connector Appliance 管理ページに接続し、登録プロセスを完了します。

デフォルトでは、Connector Appliance は DHCP を使用してネットワーク構成を設定します。ご使用の環境で DHCP を使用できない場合は、Connector Appliance 管理コンソールにアクセスする前に、Connector Appliance コンソールでネットワーク構成を設定する必要があります。詳しくは、「Connector Appliance コンソールを使用したネットワーク構成の設定」を参照してください。

次の手順：Connector Appliance を Citrix Cloud に登録する。

VMware ESXi

このセクションでは、VMware vSphere Client を使用して、VMware ESXi ホストに Connector Appliance を展開する方法について説明します。

1. ダウンロードした Connector Appliance の OVA ファイルにアクセスできるシステムで vSphere Client を使用し、ESXi ホストに接続します。
2. ［ファイル］>［**OVF** テンプレートの展開…］の順に選択します。
3. Connector Appliance の OVA ファイルが存在するパスを指定または参照します。［次へ］をクリックします。
4. テンプレートの詳細を確認します。［次へ］をクリックします。
5. Connector Appliance インスタンスに対する一意の名前を指定できます。デフォルトでは、名前は「**Connector Appliance**」に設定されています。Connector Appliance のこのインスタンスを、この ESXi ホストでホストされている他のインスタンスと区別する名前を選択してください。［次へ］をクリックします。
6. Connector Appliance に使用するストレージを指定します。［次へ］をクリックします。
7. 仮想ディスクを保存する形式を選択します。［次へ］をクリックします。
8. Connector Appliance の展開に使用するオプションを確認します。誤りがある場合は、［戻る］を使用してこれらのオプションを変更します。
9. ［展開後に電源を入れる］を選択します。［完了］をクリックします。

Connector Appliance が展開され、正常に起動すると、そのコンソールに Connector Appliance の IP アドレスを含むランディングページが表示されます。この IP アドレスを使用して Connector Appliance 管理ページに接続し、登録プロセスを完了します。

デフォルトでは、Connector Appliance は DHCP を使用してネットワーク構成を設定します。ご使用の環境で DHCP を使用できない場合は、Connector Appliance UI にアクセスする前に、Connector Appliance コンソールでネットワーク構成を設定する必要があります。詳しくは、「Connector Appliance コンソールを使用したネットワーク構成の設定」を参照してください。

次の手順：Connector Appliance を Citrix Cloud に登録する。

Hyper-V

このセクションでは、Hyper-V ホストで Connector Appliance を展開する方法について説明します。Hyper-V マネージャーまたは付属の PowerShell スクリプトを使用して仮想マシンを展開できます。

Hyper-V マネージャーを使用した **Connector Appliance** の展開

1. Hyper-V ホストに接続します。
2. Connector Appliance の ZIP ファイルを Hyper-V ホストにコピーするかダウンロードします。
3. ZIP ファイルの内容を展開します。ZIP ファイルには、PowerShell スクリプトと connector-appliance.vhdx ファイルが含まれています。
4. VHDX ファイルを VM ディスクを保持する場所にコピーします。例：`C:\ConnectorApplianceVMs`。
5. Hyper-V マネージャーを開きます。
6. サーバー名で右クリックして ［新規］**>**［仮想マシン］を選択します。
7. 仮想マシンの新規作成ウィザードの ［名前と場所の指定］パネルで Connector Appliance を識別する一意の名前を入力します。［次へ］をクリックします。
8. ［世代の指定］パネルで ［第 **1** 世代］を選択します。［次へ］をクリックします。
9. ［メモリの割り当て］パネルで次の設定を構成し、［次へ］をクリックします：
    a) 4GB の RAM を割り当てる。
    b) 動的メモリを無効にする。
10. ［ネットワークの構成］パネルで一覧からスイッチ（Default Switch など）を選択します。［次へ］をクリックします。
11. ［仮想ハードディスクの接続］パネルで ［既存の仮想ハードディスクを使用する］を選択します。
12. connector-appliance.vhdx ファイルの場所を参照して、ファイルを選択します。［次へ］をクリックします。
13. ［要約］パネルで選択した値を確認し、［完了］をクリックして仮想マシンを作成します。
14. ［仮想マシン］パネルで Connector Appliance VM を右クリックして、［設定］を選択します。
15. ［設定］ウィンドウで、［ハードウェア］**>**［プロセッサ］を選択して次のアクションを実行します：

a) ［仮想プロセッサの数］の値を **2** に変更します。
b) ［適用］をクリックします。
c) ［**OK**］をクリックします。

16. ［仮想マシン］パネルで作成した Connector Appliance VM を右クリックして、［開始］を選択します。
17. Connector Appliance VM を右クリックして ［接続］を選択してコンソールを開きます。

Connector Appliance が展開されて正常に起動した後、Hyper-V マネージャーを使用してコンソールに接続します。コンソールのランディングページに Connector Appliance の IP アドレスが表示されます。この IP アドレスを使用して Connector Appliance 管理ページに接続し、登録プロセスを完了します。

デフォルトでは、Connector Appliance は DHCP を使用してネットワーク構成を設定します。ご使用の環境で DHCP を使用できない場合は、Connector Appliance UI にアクセスする前に、Connector Appliance コンソールでネットワーク構成を設定する必要があります。詳しくは、「Connector Appliance コンソールを使用したネットワーク構成の設定」を参照してください。

次の手順：Connector Appliance を Citrix Cloud に登録する。

PowerShell スクリプトを使用した **Connector Appliance** の展開　connector-appliance.zip ファイルには、新しい仮想マシンを作成して起動する PowerShell スクリプトが含まれています。

> 注：
>
> この無署名の PowerShell スクリプトを実行する場合、Hyper-V システムでの実行ポリシーの変更が必要な場合があります。詳しくは、https://go.microsoft.com/fwlink/?LinkID=135170を参照してください。また、提供されたスクリプトは独自のローカルスクリプトを作成するか修正するためのベースにも使用できます。

1. Hyper-V ホストに接続します。
2. Connector Appliance の ZIP ファイルを Hyper-V ホストにコピーするかダウンロードします。
3. ZIP ファイルのコンテンツを抽出：PowerShell スクリプトおよび VHDX ファイル。
4. PowerShell コンソールで ZIP ファイルのコンテンツが保存される現在のディレクトリを変更して、次のコマンドを実行します：

```
.\connector-appliance-install.ps1
<!--NeedCopy-->
```

5. プロンプトが表示されたら、仮想マシンの名前を入力するか、**Enter** キーを選択してデフォルト値「**Connector Appliance**」を使用します。
6. プロンプトが表示されたら、ルートディスク用の場所を入力するか、Enter キーを押してシステムのデフォルトの VHD ディレクトリを使用します。
7. プロンプトが表示されたら、ルートディスクのファイル名を入力するか、**Enter** キーを選択して connector-appliance.vhdx のデフォルト値を使用します。

8. プロンプトが表示されたら、使用するスイッチを選択します。**Enter** キーを選択します。
9. 仮想マシンのインポート情報の概要を表示します。情報が正しければ、**Enter** キーを押して続行します。スクリプトが Connector Appliance VM を作成し、起動します。

Connector Appliance が展開され、正常に起動すると、そのコンソールに Connector Appliance の IP アドレスを含むランディングページが表示されます。この IP アドレスを使用して Connector Appliance に接続し、登録プロセスを完了します。

次の手順：Connector Appliance を Citrix Cloud に登録する。

Nutanix AHV

このセクションでは、Nutanix Prism Web コンソールを使用して、`connector-appliance.vhdx`ファイルから Nutanix AHV ホストに Connector Appliance を展開する方法について説明します。

1. Nutanix Prism Web コンソールのメインメニューで、［**Storage**］ビューを選択します。
2. ［**+ Storage Container**］をクリックして、Connector Appliance イメージファイルを格納するストレージコンテナを作成します。または、既存のストレージコンテナを使用することもできます。
3. `connector-appliance.vhdx`ファイルをストレージコンテナにアップロードします。
   a) Web コンソールのメインメニューで、［**Settings**］を選択します。
   b) ［**Image Configuration**］タブを選択して、［**+ Upload Image**］をクリックします。
   c) ［**Create Image**］で、イメージの ［**Name**］を指定します。
   d) ［**Image Type**］一覧で、［**DISK**］を選択します。
   e) ［**Storage Container**］一覧で、作成したストレージコンテナを選択します。
   f) ［**Upload a file**］を選択します。
   g) ［**Choose file**］をクリックして、ローカルシステムの`connector-appliance.vhdx`ファイルに移動します。
   h) ［保存］をクリックします。
4. イメージが作成され、［**Image Configuration**］ページでその状態が ［**ACTIVE**］と表示されるまで待ちます。
5. ［**Network Configuration**］タブを選択します。
6. ［**+ Create Network**］を作成して、Connector Appliance が使用するネットワークを作成します。
7. ［**Create Network**］ページで、次の情報を指定します：
   - ネットワーク名。
   - ネットワーク VLAN ID。
8. Web コンソールのメインメニューで、［**VM**］ビューを選択します。

9. [**+ Create VM**] をクリックして、Connector Appliance インスタンスを作成します。
10. [**Create VM**] で、次の情報を指定します:
    - VM（仮想マシン）名
    - vCPU（仮想 CPU）の数
    - メモリ量（GiB）
11. [**Legacy BIOS**] を使用することを選択します。
12. [**+ Add New Disk**] をクリックして、VM にディスクを追加します。
13. [**Add Disk**] で、次の情報を入力します:
    a) [**Type**] で [**DISK**] を選択します。
    b) [**Operation**] で [**Clone from Image Service**] を選択します。
    c) [**Bus Type**] で [**SCSI**] を選択します。
    d) [**Image**] で、Connector Appliance ファイルをアップロードしたときに作成したイメージを選択します。
14. [**Add**] をクリックして、ディスクの追加を完了します。
15. [**Create VM**] で [**+ Add New NIC**] をクリックします。
16. [**Create NIC**] で、VM を追加するネットワークを選択します。
17. [**Network Connection State**] で [**Connected**] を選択します。
18. [**Add**] をクリックして、NIC の追加を完了します。
19. [**Save**] をクリックして、VM を作成します。

    デフォルトでは、新しい VM の電源はオフになっています。
20. [**VM**] ビューで VM を選択し、[**Power on**] をクリックします。
21. VM が起動するまで待ちます。このプロセスには数分かかる場合があります。

Connector Appliance が展開され、正常に起動すると、次のいずれかの場所で Connector Appliance の IP アドレスを確認できます:

- Nutanix Prism Web コンソールの [**VM**] ビュー。
- Connector Appliance コンソール内。

この IP アドレスを使用して Connector Appliance 管理ページに接続し、登録プロセスを完了します。

次の手順: Connector Appliance を Citrix Cloud に登録する。

Microsoft Azure

このセクションでは、Microsoft Azure で Connector Appliance を展開する方法について説明します。組み込みの PowerShell スクリプトを使用して、Azure Marketplace またはダウンロードしたディスクイメージから Connector Appliance を展開できます。

Azure Marketplace から Connector Appliance を展開する　Azure Marketplace から Connector Appliance を展開するには、次の手順を実行します:

1. Azure Marketplace にある Connector Appliance に移動する（Azure Marketplace）。

   または、Marketplace 検索で「Connector Appliance for Cloud Services」を検索して移動することもできます。

2. [**Get It Now**]、[**Create**] の順にクリックします。
3. クラウドサービス用の **Citrix Connector Appliance** の作成ページで、次の情報を入力します:

   - 使用する [**Subscription**] を選択します。
   - 使用する [**Resource group**] を選択します。
   - Connector Appliance を配置する [**Region**] を選択します。
   - [**VM name**] を指定します。
   - Connector Appliance を追加する [**Virtual network**] を選択します。このネットワークは、Citrix Cloud、ローカルリソース、Connector Appliance の管理ページにアクセスするために使用されます。このネットワークは後で変更できません。
   - [**Subnet**] の値を指定します。

   [**Next : Tags >**] をクリックします。

4. [**Tags**] タブで、必要に応じて必要なタグを追加します。

   [**Next : Review + create >**] をクリックします。

5. 環境の詳細を確認したら、[**Create**] をクリックします。

Connector Appliance が展開され、正常に起動すると、そのコンソールに Connector Appliance の IP アドレスを含むランディングページが表示されます。この IP アドレスを使用して Connector Appliance 管理ページに接続し、登録プロセスを完了します。

次の手順: Connector Appliance を Citrix Cloud に登録する。

PowerShell スクリプトを使用した Connector Appliance VM の展開　`connector-appliance-azure.zip`ファイルには、新しい仮想マシンを作成して起動する PowerShell スクリプトが含まれています。提供されているスクリプトは、独自のローカルスクリプトを作成したり修正したりするためのベースとして使用できます。

スクリプトを実行する前に、次の前提条件を満たしていることを確認してください:

- Az PowerShell モジュールをローカルの PowerShell 環境にインストールしてある。
- VHD ファイルが配置されているディレクトリで PowerShell スクリプトを実行する。

次の手順を実行します:

1. Connector Appliance の ZIP ファイルを Windows システムにコピーするかダウンロードします。
2. ZIP ファイルのコンテンツを抽出: PowerShell スクリプトと VHD ファイル。
3. 管理者として PowerShell コンソールを開きます。
4. ZIP ファイルのコンテンツが保存される現在のディレクトリを変更して、次のコマンドを実行します:

```
.\connector-appliance-upload-Azure.ps1
```

5. ダイアログボックスが表示され、Microsoft Azure にログインするよう求められます。資格情報を入力してください。
6. PowerShell スクリプトによってプロンプトが表示されたら、使用するサブスクリプションを選択します。Enter キーを押します。
7. スクリプトのプロンプトに従って、イメージをアップロードし、仮想マシンを作成します。
8. 最初の VM を作成した後、アップロードされたイメージから別の VM を作成するかどうかを尋ねられます。
    - 「y」と入力して、別の VM を作成します。
    - 「n」と入力して、スクリプトを終了します。

Connector Appliance が展開され、正常に起動すると、そのコンソールに Connector Appliance の IP アドレスを含むランディングページが表示されます。この IP アドレスを使用して Connector Appliance 管理ページに接続し、登録プロセスを完了します。

次の手順: Connector Appliance を Citrix Cloud に登録する。

AWS

このセクションでは、AWS で Connector Appliance を展開する方法について説明します。Connector Appliance は、AWS Marketplace で AMI として入手できます。AMI から Connector Appliance をインストールすることをお勧めします。または、AWS UI を使用するか、組み込みの PowerShell スクリプトを使用して、ダウンロードしたディスクイメージを展開できます。

ネットワークの前提条件　Connector Appliance を AWS に展開するには、Connector Appliance が作成されたサブネットから Citrix Cloud にアクセスできることを確認してください。

アプライアンスにはプライベート IP アドレスを使用することをお勧めします。これには、Citrix Cloud へのアクセスを提供するための特定の構成が必要です。この構成を実現するには、**AWS** マネジメントコンソールで次の手順を実行します:

1. NAT ゲートウェイを作成します。

   a) 上部のナビゲーションバーで、[**Services**] **>** [**VPC**] **>** [**NAT Gateways**] を選択します。

   b) 右上の [**Create NAT Gateway**] をクリックします。次の情報を入力します:

      - [**Name**] に入力します。
      - 一覧からサブネットを選択します。
      - [**Connectivity type**] を [**Public**] を設定します。
      - 一覧から [**Elastic IP allocation ID**] を選択します。使用できる Elastic IP がない場合は、[**Allocate Elastic IP**] をクリックし、指示に従って作成します。

   c) [**Create NAT Gateway**] をクリックします。

2. NAT ゲートウェイを含むルートテーブルエントリを作成します。

   a) 上部のナビゲーションバーで、[**Services**] **>** [**VPC**] **>** [**Route Tables**] を選択します。

   b) 右上の [**Create route table**] をクリックします。次の情報を入力します:

      - [**Name**] に入力します。
      - 一覧から、NAT ゲートウェイの作成時に選択したサブネットを含む VPC を選択します。

   c) [**Create route table**] をクリックします。

   d) 作成したルートテーブルの [**Routes**] タブで、[**Edit routes**] **>** [**Add route**] をクリックします。

   e) 新しいルートエントリの [**Destination**] と [**Target**] に入力します。

      - Destination（接続先）を「0.0.0.0/0」に設定します。
      - Target（ターゲット）については、作成した [**NAT Gateway**] を一覧から選択します。

   f) [**Save change**] をクリックします。

3. Connector Appliance に使用するサブネットをこのルートテーブルに接続します。

   a) 上部のナビゲーションバーで、[**Services**] **>** [**VPC**] **>** [**Route Tables**] を選択します。
   b) NAT ゲートウェイを含むルートテーブルを選択します。
   c) 表示されたページで、[**Subnet Associations**] タブに移動します。
   d) [**Edit subnet associations**] をクリックします。
   e) ルートテーブルに接続する 1 つまたは複数のサブネットを選択します。
   f) [**Save Associations**] をクリックします。

AWS Marketplace から **Connector Appliance** を展開する　開始前に、以下の前提条件を満たしていることを確認します:

- EC2 リソースを操作する権限がある。
- 「ネットワークの前提条件」で構成を完了してある。

- （オプション）Connector Appliance にアクセスできる IP アドレスを制限するセキュリティグループを作成できます。

次の手順を実行します：

1. **AWS** マネジメントコンソールにログインします。
2. AWS Marketplace で Connector Appliance AMI を見つけます。これは次のいずれかの方法で実行できます：
   - Citrix Cloud に表示される Marketplace リンクに従います（AWS Marketplace）。
   - AWS マネジメントコンソールで AMI を検索する：
     a) ［**Services**］**>** ［**Compute**］**>** ［**EC2**］**>** ［**AMIs**］に移動します。
     b) リージョン（米国東部（オハイオ））を確認します。
     c) ［**Public images**］で、「Citrix Connector Appliance」、または AMI ID の「ami-026eaf9b3b232577f」を検索します。
3. AMI ID（ami-026eaf9b3b232577f）と所有者 ID（414337923189）をチェックして、正しい AMI であることを確認します。
4. AMI を自分のサブスクリプションにコピーします：
   a) ［**Actions**］**>** ［**Copy AMI**］に移動します。
   b) ［**Copy AMI**］ダイアログボックスで、必要な ［**Destination Region**］を選択できます。
   c) ［**Copy AMI**］をクリックします。
5. コピーした AMI の概要ページで、［**Launch instance from AMI**］をクリックします。
6. ［**Launch an instance**］ダイアログボックスで、次の手順を完了します：
   a) 作成するインスタンスの数を選択します。回復性のために、各リソースの場所に 2 つ以上の Connector Appliance を用意することをお勧めします。
   b) インスタンスの名前を指定します。
   c) ［**Instance type**］で、［**t2.medium**］を選択します。この種類のインスタンスには、少なくとも 4GB と 2 つの CPU が必要です。
   d) ［**Key pair (login)**］で、［**Proceed without a key pair**］を選択します。Connector Appliance への SSH ログインは許可されないため、キーペアは必要ありません。
   e) ［**Network settings**］の ［**Firewall (security group)**］セクションで、次の設定を構成します：
      i. ［**Create security group**］または ［**Select existing security group**］を選択します。
      ii. ［**Allow SSH traffic from the internet**］の選択を解除します。
      iii. ［**Allow HTTPs traffic from the internet**］を選択します。
      iv. ［**Allow HTTP traffic from the internet**］を選択します。

   ［**Launch instance**］をクリックします。

7. インスタンスが作成されたら、[**Success**] セクションでインスタンス ID リンクをクリックして、Connector Appliance のインスタンスを表示します。

   または、このページの [**View All Instances**] ボタンをクリックするか、AWS マネジメントコンソールの [**Services**] > [**EC2**] > [**Instances**] に移動して、インスタンス一覧を表示します。

8. [**Instance state**] を [**Running**] に変更したらインスタンスの詳細ページに移動し、[**Private IPv4 address**] を使用して Connector Appliance 管理ページに接続し、登録プロセスを完了します。

踏み台ホストを使用して、Web ブラウザーから内部 IP アドレスにある Connector Appliance 管理ページに移動し、登録プロセスを完了する必要がある場合もあります。

デフォルトでは、Connector Appliance は DHCP を使用してネットワーク構成を設定します。このネットワーク構成は、Connector Appliance Web インターフェイスを使用して編集できます。詳しくは、「Connector Appliance 管理ページでのネットワーク設定の構成」ページを参照してください。

次の手順：Connector Appliance を Citrix Cloud に登録する。

AWS UI を使用した **Connector Appliance** の展開　開始前に、以下の前提条件を満たしていることを確認します：

- S3 リソースと EC2 リソースを操作する権限がある。
- VM インポートアクセス権限があるサービス役割とポリシーを作成してある。詳しくは、https://docs.aws.amazon.com/vm-import/latest/userguide/required-permissions.html#vmimport-roleを参照してください。

  > 注：
  >
  > サービス役割を作成するには、S3 バケットを作成する必要があります。ポリシーを作成するときに、VM インポートアクセスで作成した S3 バケットを設定します。

- AWS CloudShell へのアクセス権限がある。これは、特定のリージョンでのみご利用いただけます。AWS CloudShell がサポートされているリージョンの一覧については、「https://docs.aws.amazon.com/cloudshell/latest/userguide/supported-aws-regions.html」を参照してください。
- 「ネットワークの前提条件」で構成を完了してある。

次の手順を実行します：

1. ローカルシステムで、`connector-appliance-aws.zip`のコンテンツを抽出します。
2. **AWS** マネジメントコンソールにログインします。
3. 次の手順を実行して、ストレージバケットを作成します（または、これらの手順をスキップして、既存のストレージバケットを使用することもできます）。

   a) 上部のナビゲーションバーで、[**Services**] > [**S3**] > [**Create bucket**] を選択します。

b) バケットの一意の名前を入力します。Amazon S3 のバケットの命名規則については、「https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucketnamingrules.html」を参照してください。
c) バケットのリージョンを選択します。AWS リージョンと同じリージョンを選択していることを確認してください。これらのリージョンが異なる場合、バケット内のファイルを使用することはできません。
d) 残りの設定をデフォルトのままにして、[**Create bucket**] をクリックします。

4. 作成したバケットの名前をクリックします。[**Upload**] > [**Add files**] をクリックしてから、`connector-appliance.vhd`ファイルを選択します。残りの設定をデフォルトのままにして、[**Upload**] をクリックします。
5. アップロードしたファイルをクリックします。[**Copy S3 URI**] をクリックします。
6. 上部のナビゲーションバーにある **AWS CloudShell** アイコンをクリックして、次のコマンドを実行します:

a) VHD ファイルをスナップショットに変換するタスクを作成します:

```
aws ec2 import-snapshot --disk-container Format=VHD,Url="<S3_URI>"
```

プレースホルダーの値を、前の手順でコピーした S3 URI に置き換えます。例: `aws ec2 import-snapshot --disk-container Format=VHD,Url="s3://my-aws-bucket/connector-appliance.vhd"`。

このコマンドは、`"Status": "completed"`を含む JSON 文字列を以下のコマンドが返すときに完了します。JSON 出力の`ImportTaskId`値をメモします。

b) 次のコマンドを実行します:

```
aws ec2 describe-import-snapshot-tasks --import-task-ids <ImportTaskId>
```

プレースホルダーの値を、前の手順でコピーした`ImportTaskId`に置き換えます。例: `aws ec2 describe-import-snapshot-tasks --import-task-ids import-snap-0273h2836153itg5`。

7. **AWS** マネジメントコンソールの上部のナビゲーションバーで、[**Services**] > [**EC2**] を選択します。
8. 画面左側のメニューから、[**Snapshots**] をクリックします。
9. 作成したスナップショットを右クリックして、[**Create Image**] をクリックします。
10. 開いたペインで、次の手順を実行します:

a) AMI の名前を入力します。
b) [**Hardware-assisted virtualization**] を選択します。

[作成] をクリックします。

11. 画面左側のメニューから、[**AMI**] をクリックします。

12. 作成した AMI を右クリックし、[**Launch**] をクリックします。
13. 開いたペインで、次の手順を実行します:

    a) インスタンスの種類を選択します。
    b) (オプション) [**Configure Instance**] タブでネットワークをカスタマイズします。
    c) (オプション) [**Add Storage**] タブで別のボリュームを接続します。
    d) [**Configure Security Group**] タブでセキュリティグループ規則を設定します。

    インスタンスの起動を確認したら、[**Review and Launch**] をクリックします。

Connector Appliance が展開され、正常に起動したら、[**Services**] > [**EC2**] > [**Instances**] に移動し、作成したインスタンスを選択します。[**Private IPv4 address**] を使用して Connector Appliance 管理ページに接続し、登録プロセスを完了します。踏み台ホストを使用して、Web ブラウザーから内部 IP アドレスにある Connector Appliance 管理ページに移動し、インストールプロセスを続行する必要がある場合もあります。

デフォルトでは、Connector Appliance は DHCP を使用してネットワーク構成を設定します。このネットワーク構成は、Connector Appliance Web インターフェイスを使用して編集できます。詳しくは、「Connector Appliance 管理ページでのネットワーク設定の構成」ページを参照してください。

次の手順: Connector Appliance を Citrix Cloud に登録する。

PowerShell スクリプトを使用した **Connector Appliance** の展開　`connector-appliance-aws.zip`ファイルには、新しい仮想マシンを作成して起動する PowerShell スクリプトが含まれています。スクリプトを実行する前に、次の前提条件を満たしていることを確認してください:

- システムに AWS.Tools、AWSPowerShell.NetCore、または AWSPowerShell のいずれかがインストールされている。詳しくは、https://docs.aws.amazon.com/powershell/latest/userguide/pstools-getting-set-up.htmlを参照してください。
- VM インポートアクセス権限があるサービス役割とポリシーを作成してある。この PowerShell スクリプトを機能させるには、サービス役割とポリシーの両方に`vmimport`という名前を付ける必要があります。詳しくは、https://docs.aws.amazon.com/vm-import/latest/userguide/required-permissions.html#vmimport-roleを参照してください。

  > 注:
  >
  > サービス役割を作成するには、S3 バケットを作成する必要があります。ポリシーを作成するときに、VM インポートアクセスで作成した S3 バケットを設定します。

- Amazon EC2 セキュリティグループを作成してある。
- S3 権限と API アクセス権がある。
- 「ネットワークの前提条件」で構成を完了してある。

次の手順を実行します:

1. ローカルシステムで、connector-appliance-aws.zipのコンテンツをフォルダーに抽出します。
2. PowerShell で、次のコマンドを実行します:

   a) ローカル環境で AWS コマンドレットを実行できるようにするには、次のコマンドを実行して、AWS SDK ストアに新しいプロファイルを追加します:

   ```
   Set-AWSCredential -AccessKey <access_key_ID> -SecretKey <
       secret_key> -StoreAs MyProfile
   ```

   プレースホルダーの値をアクセスキーと秘密キーに置き換えます。一意のプロファイル名を入力します。入力例は、「MyProfile」です。

   b) プロファイルをデフォルトに設定します:

   ```
   Initialize-AWSDefaultConfiguration -ProfileName MyProfile
   ```

   c) 現在のディレクトリを、抽出したファイルが保存されているフォルダーに変更して、次のコマンドを実行します:

   ```
   .\connector-appliance-upload-aws.ps1
   ```

3. スクリプトのプロンプトに従って、Connector Appliance 展開用のリージョンを選択し、選択したバケットにイメージをアップロードして、VM の名前を入力します。

   - 以前に作成した VM インポートアクセスで、バケットを使用する必要があります。
   - 使用する VPC を選択するように求められたら、NAT ゲートウェイとルートテーブルが構成されている VPC を選択します。
   - 使用するサブネットを選択するように求められたら、NAT ゲートウェイを含むルートテーブルに接続されているサブネットを選択します。

   詳しくは、「ネットワークの前提条件」を参照してください。

Connector Appliance が展開され、正常に起動すると、スクリプトにより Connector Appliance のプライベート IP アドレスが表示されます。踏み台ホストを使用して、Web ブラウザーから内部 IP アドレスにある Connector Appliance 管理ページに移動し、登録プロセスを完了する必要がある場合もあります。

デフォルトでは、Connector Appliance は DHCP を使用してネットワーク構成を設定します。このネットワーク構成は、Connector Appliance Web インターフェイスを使用して編集できます。詳しくは、「Connector Appliance 管理ページでのネットワーク設定の構成」ページを参照してください。

次の手順: Connector Appliance を Citrix Cloud に登録する。

Google Cloud Platform

このセクションでは、Google Cloud Platform で Connector Appliance を展開する方法について説明します。Connector Appliance は、Google Cloud Marketplace からインストールできます。または、Google Cloud

Platform コンソールを使用するか、組み込みの PowerShell スクリプトを使用して、ダウンロードしたディスクイメージを展開できます。

`connector-appliance-gcp.zip`ファイルには、以下が含まれています:

- `connector-appliance.tar.gz`: Connector Appliance のディスクイメージ。
- `connector-appliance-upload-gcp.ps1`: Connector Appliance を自動的に展開するために使用できる PowerShell スクリプト。

Google Cloud Marketplace から **Connector Appliance** を展開する

1. Google アカウントにログインします。
2. Citrix Cloud に表示される Marketplace リンクに従います（Google Cloud Marketplace)。

   または、Marketplace 検索で「Connector Appliance for Cloud Services」を検索して移動することもできます。
3. ［起動］をクリックします。
4. クラウドサービス用の新しい **Citrix Connector Appliance** 展開のページで、次の情報を入力します:

   - 展開ジョブの ［展開名］を指定します。
   - Connector Appliance を配置する ［ゾーン］を選択します。
   - 使用する ［マシンファミリ］、［シリーズ］、［マシンの種類］を選択します。
   - ［起動ディスクの種類］と ［起動ディスクのサイズ（**GB**)］を選択します。
   - ［ネットワーク］セクションで、Connector Appliance で使用するネットワークインターフェイスを指定します。パブリックネットワークから管理ページに接続できるようにするには、［外部 **IP**］を指定します。

   ［展開］をクリックします。［**Deployment Manager**］ページが開きます。

   > 注:
   >
   > Connector Appliance が展開され、正常に起動すると、Connector Appliance が Google Cloud Platform に展開されていることを確認するメールが届きます。

5. ［**Deployment Manager**］ページで、インスタンス名をクリックします。または、**Compute Engine** で作成した Connector Appliance インスタンスを検索することもできます。
6. Connector Appliance のネットワークインターフェイス設定時に ［外部 **IP**］を指定したことがある場合は、［詳細］タブの ［ネットワークインターフェイス］セクションの ［外部 **IP** アドレス］をコピーします。この IP アドレスを使用して Connector Appliance 管理ページに接続し、登録プロセスを完了します。または、［プライマリ内部 **IP** アドレス］を使用して、Connector Appliance と同じサブネット内の別のマシンから Connector Appliance 管理ページにアクセスすることもできます。

次の手順: Connector Appliance を Citrix Cloud に登録する。

Google Cloud Platform コンソールを使用した **Connector Appliance** の展開

1. ローカルシステムで、`connector-appliance-gcp.zip`のコンテンツを抽出します。
2. Google Cloud Platform プロジェクトで、ストレージバケットを作成します（既存のストレージバケットを使用することもできます）。

   a) メインメニューから、[**Cloud Storage**] を選択します。
   b) メインペインで、[**Create bucket**] を選択します。
   c) バケットの名前を指定します。
   d) 必要なデータストレージとアクセス設定を構成します。これらの設定はデフォルトのままにしておいても構いません。
   e) [作成] をクリックします。

3. ストレージバケット内で、[**Upload files**] を選択し、`connector-appliance.tar.gz`ファイルを選択します。ファイルがアップロードされるまで待ちます。
4. アップロードされたファイルを選択して、その詳細を表示します。クリップボードに [**gsutil URI**] の値をコピーします。
5. ヘッダーバーの [**Activate Cloud Shell**] アイコンをクリックして、Cloud Shell を開きます。
6. Cloud Shell で、次のコマンドを実行してイメージを作成します:

```
gcloud compute images create "Image name" --guest-os-features=
    MULTI_IP_SUBNET --source-uri="gsutil URI of uploaded connector-
    appliance.tar.gz file"
```

7. メインメニューから、[**Compute Engine**] > [**VM Instances**] を選択します。
8. [**Create Instance**] を選択します。開いたペインで、次の情報を指定します:

   a) [**Name**] フィールドに、Connector Appliance インスタンスの名前を入力します。
   b) Connector Appliance を配置するリージョンを選択します。
   c) マシン構成を選択します。
   d) [**Boot disk**] セクションで、[**Change**] をクリックします。
   e) 開いたセクションで、[**Custom images**] タブに移動します。
   f) [**Image**] 一覧から、作成したイメージを選択します。
   g) [**Select**] をクリックします。
   h) [**Firewall**] セクションで、HTTPS トラフィックを有効にして、Connector Appliance 管理ページへのアクセスを許可します。
   i) 必要な追加の構成を指定します。たとえば、デフォルトのネットワーク構成を使用したくない場合などです。

   [作成] をクリックします。

9. [**VM Instances**] セクションで、新しく作成した VM を選択して、その詳細を表示します。

Connector Appliance が展開され、正常に起動すると、[**VM Instances**] セクションに Connector Appliance の IP アドレスが表示されます。

Connector Appliance に外部 IP アドレスがある場合は、この IP アドレスを使用して、Web ブラウザーから Connector Appliance 管理ページに移動し、登録プロセスを完了できます。

Connector Appliance に内部 IP アドレスしかない場合は、踏み台ホストを使用して、Web ブラウザーから Connector Appliance 管理ページに移動し、登録プロセスを完了します。詳しくは、https://cloud.google.com/compute/docs/connect/ssh-using-bastion-hostを参照してください。

次の手順：Connector Appliance を Citrix Cloud に登録する。

PowerShell スクリプトを使用した **Connector Appliance** の展開　提供されている PowerShell スクリプトを使用して Connector Appliance を展開するには、システムに Google Cloud SDK がインストールされている必要があります。

1. ローカルシステムで、`connector-appliance-gcp.zip`のコンテンツをフォルダーに抽出します。
2. PowerShell で、抽出したファイルが配置されているこのフォルダーにディレクトリを変更します。
3. コマンド`.\connector-appliance-upload-GCP.ps1`を実行します。
4. 開いた Web ブラウザーのウィンドウで、Connector Appliance の展開先であるプロジェクトへのアクセス権限があるアカウントを使用して、Google Cloud SDK で認証します。
5. Google Cloud Tools for PowerShell で、PowerShell スクリプトのプロンプトが表示されたら、使用するプロジェクトを選択します。Enter キーを押します。
6. スクリプトのプロンプトに従って、ディスクをアップロードし、イメージを作成して、仮想マシンを作成します。
7. 最初の VM を作成した後、アップロードされたイメージから別の VM を作成するかどうかを尋ねられます。
   - 「y」と入力して、別の VM を作成します。
   - 「n」と入力して、スクリプトを終了します。

Connector Appliance が展開され、正常に起動すると、スクリプトにより Connector Appliance の内部 IP アドレスが表示されます。または、Google Cloud Platform コンソールで、Connector Appliance の内部 IP アドレスを見つけることもできます。[**Compute Engine**] > [**VM Instances**] セクションには、Connector Appliance の IP アドレスが表示されます。

踏み台ホストを使用して、Web ブラウザーから内部 IP アドレスにある Connector Appliance 管理ページに移動し、登録プロセスを完了します。詳しくは、https://cloud.google.com/compute/docs/connect/ssh-using-bastion-hostを参照してください。

次の手順：Connector Appliance を Citrix Cloud に登録する。

Connector Appliance を **Citrix Cloud** に登録する

Citrix Cloud とリソースの場所の間の通信チャネルを提供するため、Connector Appliance を Citrix Cloud に登録します。

Connector Appliance をハイパーバイザーにインストールして起動すると、コンソールに Connector Appliance の IP アドレスが表示されます。コンソールには、Connector Appliance UI への接続を検証するために使用できる SSL フィンガープリントも表示されます。

1. Connector Appliance の IP アドレスを次の形式です入力してください: `https://xx.xx.xx.xx/?deployment=productionjp`
   Connector Appliance UI は、5 年間有効な自己署名証明書を使用します。その結果、接続が安全でないというメッセージが表示される場合があります。Connector Appliance への接続を確認するには、コンソールの SSL フィンガープリントを、ブラウザーが Web ページから受信したフィンガープリントと比較します。

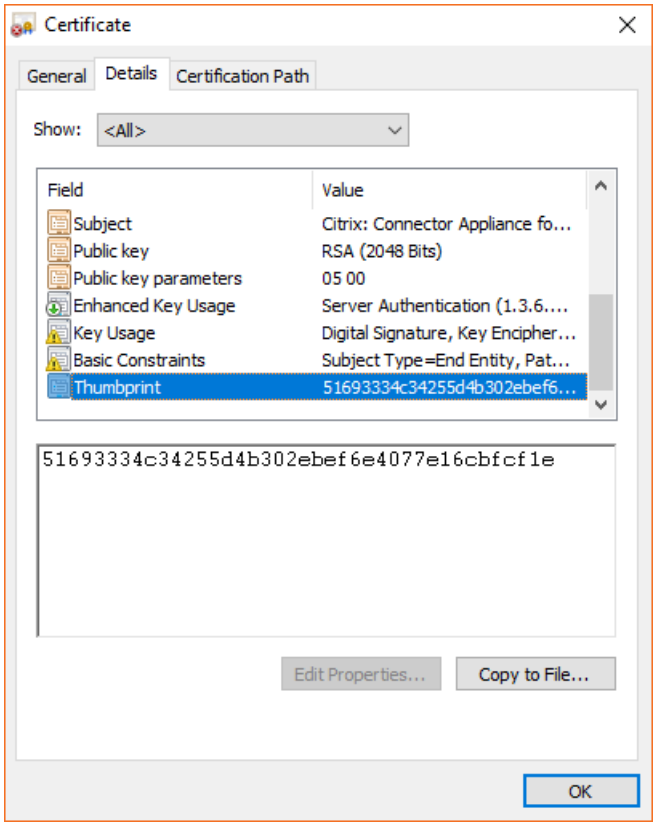
   たとえば、Google Chrome ブラウザーで、以下の手順を実行します:

   a) アドレスバーの横にある保護されていない通信マーカーをクリックします。

   b) ［証明書］を選択します。［証明書］ウィンドウが開きます。

   c) ［詳細］タブに移動し、拇印フィールドを見つけます。

      拇印フィールドの値とコンソールで提供された SSL フィンガープリントが一致する場合、ブラウザーが Connector Appliance UI に直接接続していることを確認できます。

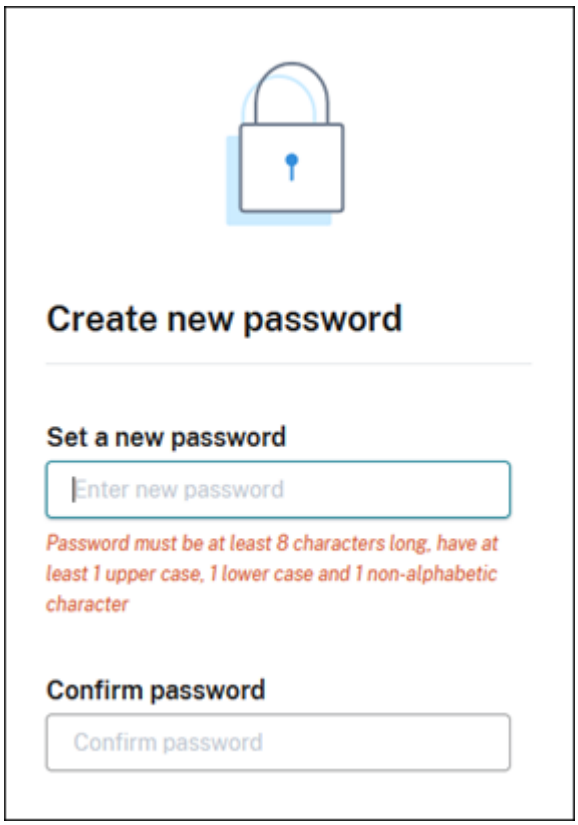


この自己署名証明書を組織によって署名された、または組織の信頼チェーンを使用して生成された独自の証明書に置き換えることができます。詳しくは、「証明書の管理」を参照してください。

2. ブラウザーがサイトへの移動を確認するために追加の手順を要求する場合は、この手順を完了してください。

   ［新しいパスワードの作成］ Web ページが開きます。

3. Connector Appliance UI のパスワードを作成し、［新しいパスワードの設定］をクリックします。

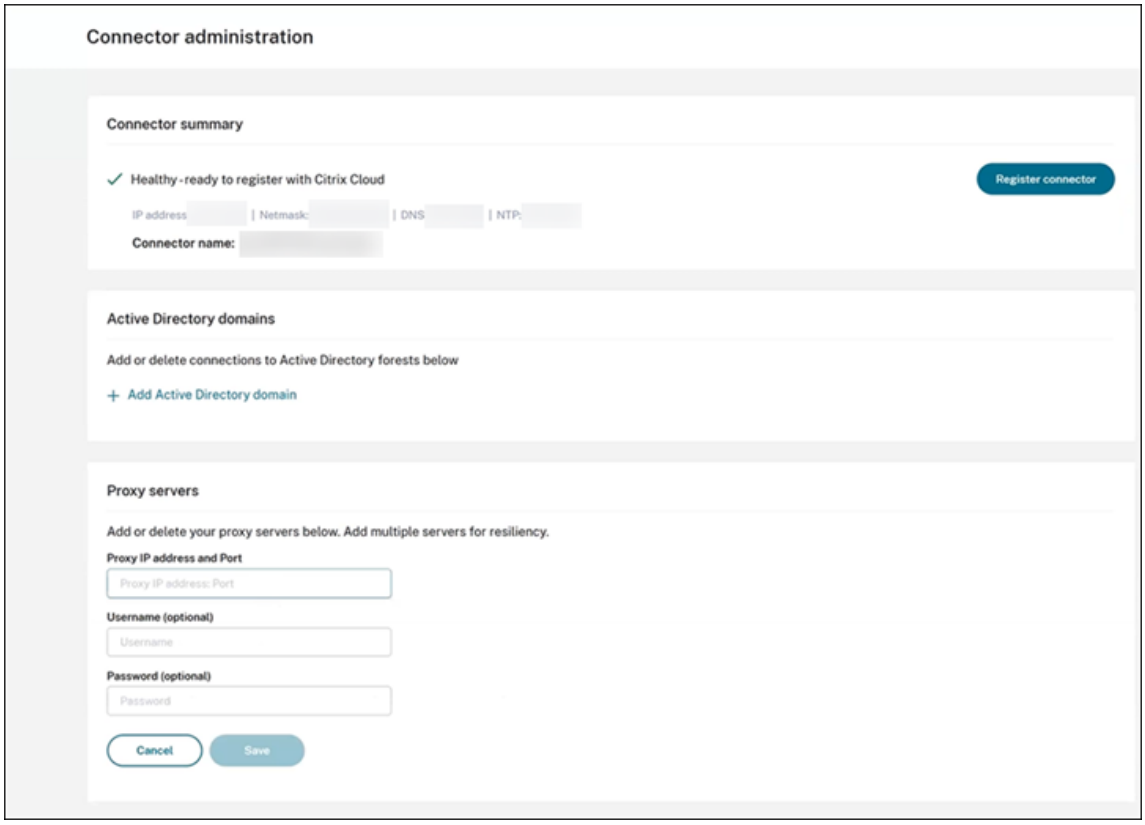


設定するパスワードは次の要件を満たしている必要があります:

- 8 文字以上
- 大文字と小文字の両方を含む
- アルファベット以外の文字を少なくとも 1 つ含む

このパスワードは、将来の使用に備えて安全な場所に保管してください。

4. 設定したパスワードでサインインします。［コネクタの管理］ページが開きます。



5. （オプション）1 つ以上の Web プロキシを使用する場合、［プロキシサーバー］セクションにプロキシアドレスを追加できます。認証されていないプロキシと認証されたプロキシの両方がサポートされています。認証されていないプロキシを追加するには、有効なプロキシ **IP** アドレスとポートを入力します。認証されたプロキシを追加するには、有効なユーザー名とパスワードも指定します。

   > 注:
   >
   > 基本的なプロキシ認証のみがサポートされています。他の形式の認証はサポートされていません。

   外部システムへのトラフィックのみが Web プロキシ経由でルーティングされます。詳しくは、「Connector Appliance の通信」を参照してください。

6. （オプション）ネットワークがインターネットにアクセスするために TLS インターセプト Web プロキシを使用している場合、クラウドと正常に通信するためにコネクタがそのルート証明機関を信頼する必要がある場合があります。

   a) ［ルート証明機関］で、［証明書を追加］を選択します。

   b) 証明書の内容を PEM 形式としてコピーします。

   ```
   -----BEGIN CERTIFICATE-----
   <certificate-base64-bytes>
   -----END CERTIFICATE-----
   <!--NeedCopy-->
   ```


c)［証明書の完全な詳細］に証明書の内容を貼り付けます。

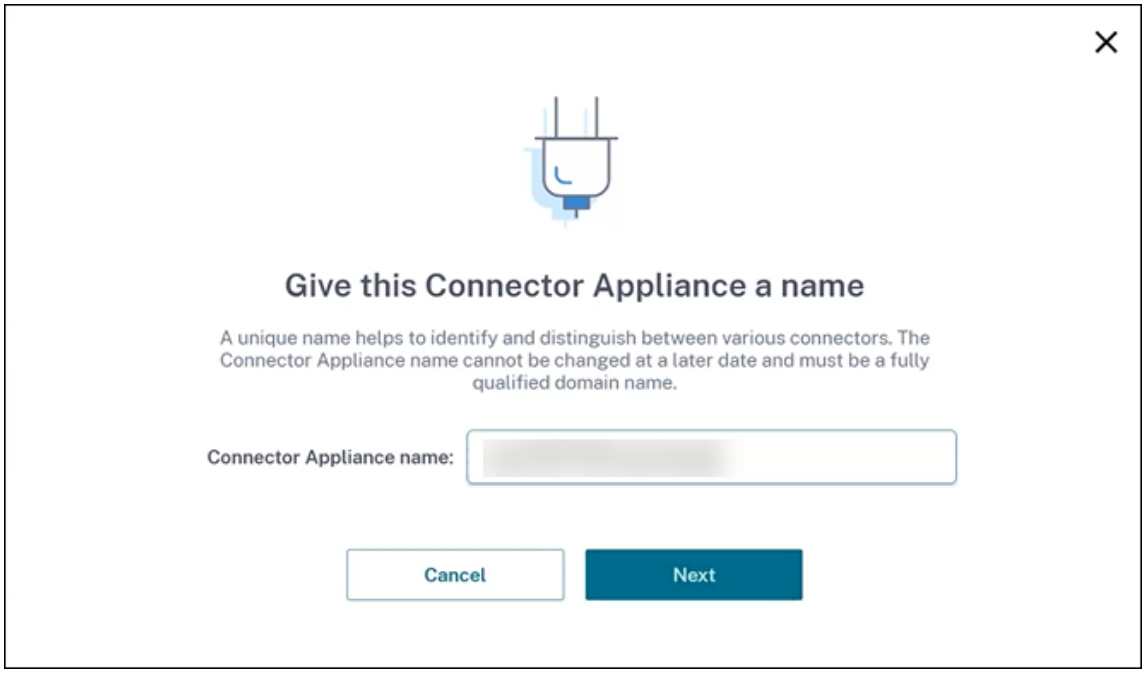
d)［証明書の追加］を選択します。

Connector Appliance API を使用してルート証明機関（RootCA）を追加するには、Citrix 開発者向けドキュメントの「Managing root certificate authorities」を参照してください。

> 注:
>
> 有効期限が切れた証明書、または今後 30 日以内に期限切れになる証明書には警告が表示されます。

7. ［コネクタの登録］をクリックして、登録タスクを開きます。
8. Connector Appliance の名前を選択します。この名前は、リソースの場所に存在するさまざまな Connector Appliance を区別するのに役立ちます。Connector Appliance を登録した後は、名前を変更することはできません。

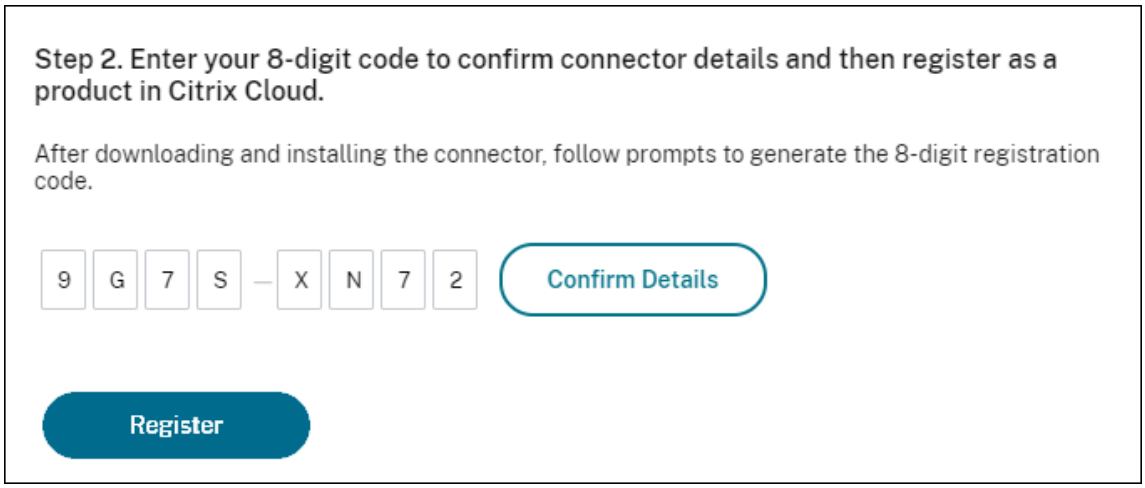
   ［**Connector Appliance** 名］フィールドに名前を入力し、［次へ］をクリックします。



   Web ページで、Citrix Cloud での登録に使用するコードが提供されます。このコードは 15 分で期限切れになります。

9. ［コピー］ボタンを使用し、コードをクリップボードにコピーします。
10. ［リソースの場所］ Web ページに戻ります。
11. ［**Connector Appliance** のインストール］タスクの ［手順 **2**］にコードを貼り付けます。［詳細を確認］をクリックします。

    Citrix Cloud で、Connector Appliance が存在し、接続できることを確認します。登録コードの有効期限が切れている場合、新しいコードを生成するよう指示されます。



12. ［登録］をクリックします。

    このページに、登録が成功したかどうかが表示されます。登録が失敗した場合、再試行するよう指示されます。

13. ［閉じる］をクリックします。

Connector Appliance 管理ページでは、Connector Appliance の診断レポートをダウンロードすることもできます。詳しくは、「診断レポートの生成」を参照してください。

Connector Appliance の登録後

各リソースの場所で、2 つ以上の Connector Appliance をインストールして登録することをお勧めします。この構成により、継続的な可用性が確保され、コネクタ間で負荷を分散できます。

Connector Appliance を直接管理することはできません。

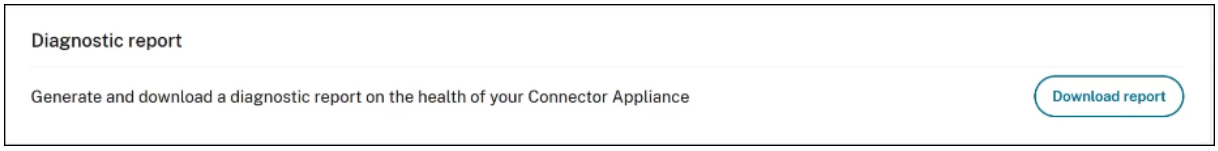
Connector Appliance は自動的に更新されます。コネクタを更新するためにアクションを実行する必要はありません。Connector Appliance の更新をリソースの場所に適用する日時を指定できます。

Connector Appliance VM のスナップショットを複製、一時停止、作成しないでください。これらの操作はサポートされていません。

Connector Appliance UI に初めて接続したときにのみ、［新しいパスワードの作成］ページが表示されます。このパスワードは、将来の使用に備えて安全な場所に保管してください。このパスワードはリセットできません。パスワードを忘れた場合は、Connector Appliance を再インストールする必要があります。その後の UI への接続では、Connector Appliance の登録時に設定したパスワードを入力するように求められます。

診断レポートの生成

Connector Appliance 管理ページから診断レポートを生成してダウンロードできます。



1. ハイパーバイザーの Connector Appliance コンソールから、IP アドレスを Web ブラウザーのアドレスバーにコピーします。
2. Connector Appliance の登録時に設定したパスワードを入力します。
3. ページの ［診断レポート］セクションで、［レポートのダウンロード］をクリックします。

診断レポートは、`.zip`ファイルで提供されます。

ネットワーク接続の確認

［**TCP** キャプチャ］診断チェックを使用して、**Connector Appliance** 管理ページからネットワーク接続を確認できます。

1. **Connector Appliance** の管理ページで、ヘッダーバーのアカウント名をクリックし、［ネットワーク診断］を選択します。
2. （オプション）［**TCP** キャプチャ］セクションに、ターゲット IP アドレス、ホスト名、またはポートを入力して、TCP キャプチャを制限します。
3. ［トレース期間］メニューから、トレースを実行する期間を選択します。
4. （オプション）［パケットトレース］を有効にして、パケットの内容をキャプチャします。

   パケットトレースが無効になっている場合、TCP キャプチャ機能はベストエフォートアプローチをとり、診断用にヘッダーをキャプチャします。このベストエフォートアプローチは、各パケットの最初の 94 バイトをキャプチャします。ただし、ヘッダーは固定サイズではないため、このアプローチではすべてのヘッダーをキャプチャできないことがあります。
5. ［トレースの開始］をクリックします。
6. トレースが完了するまで待ちます。トレースが完了したら、トレースレポートをダウンロードするか、新しいトレースを開始することができます。

   - ［ダウンロード］をクリックして、トレースレポートをダウンロードします。トレースレポートは`.pcap`ファイルで提供されます。
   - ［新しいトレースの開始］をクリックして、別のトレースを開始します。

Active Directory を **Citrix Cloud** に接続する

Connector Appliance を使用して、Citrix Virtual Apps and Desktops リソースを含まないフォレストにリソースの場所を接続できます。たとえば、一部のフォレストがユーザー認証にのみ使用される Citrix Virtual Apps and Desktops の顧客の場合です。

詳しくは、「Connector Appliance を使用した Active Directory」を参照してください。

Connector Appliance のネットワーク設定

デフォルトでは、Connector Appliance の IP アドレスとネットワーク設定は、DHCP を使用して自動的に割り当てられます。

DHCP を使用して Connector Appliance を登録した後、**Connector Appliance** 管理ページでネットワーク設定を編集できます。

ただし、ご使用の環境で DHCP を使用できない場合、または **Connector Appliance** 管理ページにアクセスできない場合は、Connector Appliance コンソールで直接ネットワーク構成を設定できます。

Connector Appliance 管理ページでのネットワーク設定の構成

DHCP を使用して Connector Appliance を登録した後、**Connector Appliance** 管理ページでネットワーク設定を編集できます。

ネットワーク設定を手動で構成するには:

1. ［コネクタの概要］セクションで、［ネットワーク設定の編集］を選択します。
2. ［ネットワーク設定］ダイアログボックスで、［独自のネットワーク設定を構成する］を選択します。
3. **IP** アドレス、サブネットマスク、デフォルトゲートウェイを入力します。
4. 1 つまたは複数の **DNS** サーバーを追加します。
5. 1 つまたは複数の **NTP** サーバーを追加します。
6. ［保存］をクリックします。

ネットワーク設定への変更を保存すると、Connector Appliance が再起動します。再起動中、Connector Appliance は一時的に使用できなくなります。**Connector Appliance** 管理ページからログアウトされ、このページの URL が変更されます。新しい URL は、Connector Appliance コンソール内で、またはハイパーバイザーでネットワーク情報を確認することで、見つけることができます。

自動的に割り当てられた値を使用するよう、ネットワーク構成を変更するには:

1. ［コネクタの概要］セクションで、［ネットワーク設定の編集］を選択します。
2. ［ネットワーク設定］ダイアログボックスで、［**IP** アドレスを自動的に取得する］を選択します。
3. ［保存］をクリックします。

ネットワーク設定への変更を保存すると、Connector Appliance が再起動します。再起動中、Connector Appliance は一時的に使用できなくなります。**Connector Appliance** 管理ページからログアウトされ、このページの URL が変更されます。新しい URL は、Connector Appliance コンソール内で、またはハイパーバイザーでネットワーク情報を確認することで、見つけることができます。

Connector Appliance コンソールを使用したネットワーク構成の設定

デフォルトでは、Connector Appliance の IP アドレスとネットワーク設定は、DHCP を使用して自動的に割り当てられます。ただし、ご使用の環境で DHCP を使用できない場合、または **Connector Appliance** 管理ページにアクセスできない場合は、Connector Appliance コンソールで直接ネットワーク構成を設定できます。

ネットワーク構成を設定するには:

1. ハイパーバイザーで、Connector Appliance を再起動します。
2. Connector Appliance の起動中に、コンソールでメッセージ「`Welcome to GRUB!`」を確認します。
3. このメッセージが表示されたら、**Esc** キーを押して GRUB メニューに入ります。
4. 起動パラメーターを編集するには、**e** キーを押します。

   次の画像のようなビューが表示されます:

5. 「`linux`」で始まる行を編集して、必要なネットワーク構成を設定します。

   - DHCP ネットワークを指定するには、行末に「`network=dhcp`」を追加します。
   - 静的ネットワークを指定するには、行の最後に次のパラメーターを追加します:

     ```
     network=static:ip=<static_ip_address>:netmask=<netmask>:route
        =<default_gateway>:dns=<dns_server_1>,<dns_server_2>:ntp=<
        ntp_server_1>,<ntp_server_2>
     <!--NeedCopy-->
     ```

     プレースホルダーの値を構成の値に置き換えます。

6. **Ctrl+X** キーを押して、新しい構成で Connector Appliance を起動します。

Connector Appliance の管理者ユーザーパスワードの変更

1. コンソールの右上にあるユーザーメニューから、［パスワードの変更］を選択します。

   ［パスワードの変更］ページが表示されます。

2. 現在のパスワードを入力してから、新しいパスワードを入力して確認します。設定する新しいパスワードは次の要件を満たしている必要があります:

   - 8 文字以上
   - 大文字と小文字の両方を含む
   - アルファベット以外の文字を少なくとも 1 つ含む
   - 現在のパスワードと同じものにしない

3. ［パスワードの変更］を選択して変更を保存します。

Citrix Cloud から自動的にサインアウトされ、サインインページにリダイレクトされます。

Connector Appliance を使用した **Active Directory**

March 27, 2024

Connector Appliance を使用して、Citrix Virtual Apps and Desktops リソースを含まないフォレストにリソースの場所を接続できます。たとえば、一部のフォレストがユーザー認証にのみ使用される Citrix Virtual Apps and Desktops の顧客の場合です。

Connector Appliance を使用したマルチドメイン Active Directory の場合、次の制限が適用されます:

- VDA を含むフォレストでは、Cloud Connector の代わりに Connector Appliance を使用することはできません。

要件

Active Directory の要件

- ユーザー用のオファリングを作成するために使用するリソースとユーザーを含む Active Directory ドメインに参加済み。詳しくは、「Active Directory での Connector Appliance の展開シナリオ」を参照してください。
- Citrix Cloud で使用する予定の各 Active Directory フォレストには、常に 2 つの Connector Appliance がアクセスできるようにする必要があります。
- Connector Appliance は、フォレストルートドメインと Citrix Cloud で使用する予定のドメインの両方のドメインコントローラーにアクセスできる必要があります。詳しくは、次の Microsoft のサポート文書を参照してください:

  - ドメインと信頼を構成する方法
  - 「Windows のサービス概要およびネットワークポート要件」の「システムサービスポート」セクション

- グローバルセキュリティグループの代わりに、ユニバーサルセキュリティグループを使用します。この構成により、ユーザーグループのメンバーシップをフォレスト内の任意のドメインコントローラーから確実に取得できます。

ネットワークの要件

- リソースの場所で使用するリソースに接続できるネットワークに接続済み。
- インターネットに接続済み。詳しくは、「システムおよび接続要件」を参照してください。

「Connector Appliance の通信」に記載されているポートに加えて、Connector Appliance には、次のポートを介して Active Directory ドメインに送信接続する必要があります:

サービス	ポート	サポートされるドメインプロトコル
kerberos	88	TCP/UDP
エンドポイントマッパー (DCE/RPC ロケーターサービス)	135	TCP
NetBIOS ネームサービス	137	UDP
NetBIOS データグラム	138	UDP
NetBIOS セッション	139	TCP
LDAP	389	TCP/UDP
SMB over TCP	445	TCP
Kerberos kpasswd	464	TCP/UDP
グローバルカタログ	3268	TCP
動的 RPC ポート	49152～65535	TCP

Connector Appliance は、LDAP 署名を使用してドメインコントローラーへの接続をセキュリティで保護します。つまり、SSL 経由の LDAP（LDAPS）は必要ありません。LDAP 署名について詳しくは、「Windows Server で LDAP 署名を有効にする方法」および「LDAP チャネルバインディングと LDAP 署名を有効にするためのマイクロソフトガイダンス」を参照してください。

サポートされる **Active Directory** の機能レベル

Connector Appliance はテスト済みで、Active Directory のフォレストとドメインの以下の機能レベルでサポートされます。

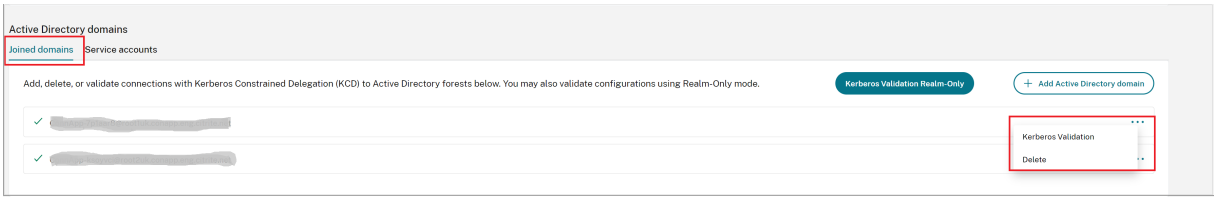
フォレスト機能レベル	ドメイン機能レベル	サポートされるドメインコントローラー
Windows Server 2016	Windows Server 2016	Windows Server 2019

ドメインコントローラ、フォレスト機能レベル、およびドメインの機能レベルの他の組み合わせは、Connector Appliance ではテストされていません。ただし、これらの組み合わせは正常に動作することが期待されており、サポートされています。

Connector Appliance を使用して **Active Directory** ドメインを **Citrix Cloud** に接続する

Connector Appliance 管理 Web ページに接続すると、Active Directory ドメインセクションに 2 つのタブが表示されます。

- **Joined Domains** –Connector Appliance を AD ドメインに参加させるために使用され、ドメイン内にアプライアンスのマシンアカウントを作成します。Kerberos を検証するには、参加したドメインの右側にある省略記号メニューをクリックします。ドメイン内にマシンアカウントが存在する必要があります。



Connector Appliance を介して Citrix Cloud に接続するように Active Directory を構成するには、次の手順を実行します。

1. Connector Appliance をリソースの場所にインストールします。

   Connector Appliance の製品ドキュメントの情報を参照できます。

2. Connector Appliance コンソールで提供される IP アドレスを使用して、Web ブラウザーで Connector Appliance の管理 Web ページに接続します。
3. [**Active Directory** ドメイン] セクションで、[**Joined domains**] タブに移動します。
4. [**+Active Directory** ドメインの追加] をクリックすると、ドメイン名を入力するための新しいポップアップウィンドウが表示されます。

   Connector Appliance はドメインをチェックします。チェックで問題がなければ、[**Active Directory** に参加] ダイアログボックスが開きます。この新しいウィンドウでは、ドメインに参加するためのユーザー名とパスワードを入力できます。

5. [追加] をクリックします。
6. ドメインへの参加権限を持つ Active Directory ユーザーのユーザー名とパスワードを入力します。

7. Connector Appliance からマシン名が提案されます。提案された名前を上書きして、独自のマシン名（最大 15 文字）を指定することもできます。

   このマシン名は、Connector Appliance が参加したときに Active Directory ドメインに作成されます。

8. ［参加］をクリックします。

   これで、Connector Appliance のユーザーインターフェイス ［**Active Directory** ドメイン］セクションにドメインが一覧表示されます。

9. **Active Directory** ドメインをさらに追加するには、［**+ Active Directory** ドメインの追加］を選択して、上記の手順を繰り返します。

10. **Citrix Cloud** コンソールのドメインページに移動し、ドメインにサービスを提供する ［**Connector Appliance**］を選択します。

11. Connector Appliance をまだ登録していない場合は、「Connector Appliance を Citrix Cloud に登録する」で説明されている手順を続行します。

> 注
>
> ドメインへの参加を試行しているときにエラーが発生した場合は、お使いの環境が Active Directory の要件とネットワークの要件を満たしていることを確認してください。

次の操作

- この Connector Appliance には、さらにドメインを追加できます。

  > 注:
  >
  > Connector Appliance は最大 10 個のフォレストでテストされています。

- 耐障害性を向上させるため、各ドメインを各リソースの場所にある複数の Connector Appliance に追加します。

Active Directory 構成を表示する

リソースの場所の Active Directory ドメインと Connector Appliance の構成は、次の場所で表示できます:

- Citrix Cloud の場合:

  1. メニューで、［**ID** およびアクセス管理］ページに移動します。
  2. ［ドメイン］タブに移動します。

     Active Directory ドメインは、そのドメインが属しているリソースの場所とともに一覧表示されます。

- Connector Appliance の Web ページの場合:

1. Connector Appliance コンソールで提供される IP アドレスを使用して、Connector Appliance の Web ページに接続します。
2. 初回登録時に作成したパスワードでログインします。
3. ページの ［**Active Directory** ドメイン］セクションには、この Connector Appliance が参加している Active Directory ドメインの一覧が表示されます。

Connector Appliance から **Active Directory** ドメインを削除する

Active Directory ドメインから離脱するには、次の手順を実行します:

1. Connector Appliance コンソールで提供される IP アドレスを使用して、Connector Appliance の Web ページに接続します。
2. 初回登録時に作成したパスワードでログインします。
3. ページの ［**Active Directory** ドメイン］セクションにある、参加している Active Directory ドメインの一覧で、離脱するドメインを探します。
4. Connector Appliance によって作成されたマシンアカウントの名前を記録します。
5. ドメインの横にある削除アイコン（ごみ箱）をクリックします。確認ダイアログボックスが開きます。
6. ［続行］をクリックして、その操作を確認します。
7. Active Directory コントローラに移動します。
8. Connector Appliance によって作成されたマシンアカウントをコントローラから削除します。

Active Directory で **Connector Appliance** を使用した展開シナリオ

Cloud Connector と Connector Appliance の両方を使用して、Active Directory コントローラに接続できます。使用するコネクタの種類は、展開によって異なります。

次の状況では、Connector Appliance を使用してリソースの場所を Active Directory フォレストに接続します:

- ユーザー認証にのみ使用されるフォレストが 1 つ以上ある
- 複数のフォレストのサポートに必要なコネクタ数の削減を希望している
- 他のユースケースに Connector Appliance を必要としている

1 つ以上のフォレストにユーザーのみが存在する場合に、すべてのフォレストに対して **1** セットの **Connector Appliance** を展開

このシナリオは、Workspace Standard の顧客、または Secure Private Access のために Connector Appliance を使用する顧客に適用されます。

このシナリオでは、ユーザーオブジェクト（`forest1.local`、`forest2.local`）のみを含むフォレストがいくつかあります。これらのフォレストにはリソースは含まれていません。単一の Connector Appliance セットがリソースの場所に展開され、各フォレストのドメインに参加します。

- 信頼関係：なし
- [**ID** およびアクセスの管理］に表示されるドメイン：forest1.local、forest2.local
- Citrix Workspace にログオンできるユーザー：すべてのユーザー
- オンプレミス StoreFront にログオンできるユーザー: すべてのユーザー

別々のフォレストにユーザーとリソースが存在する場合に（信頼関係あり）、すべてのフォレストに単一の **Connector Appliance** セットを展開

このシナリオは、複数のフォレストを持つ Citrix Virtual Apps and Desktops の顧客に適用されます。

このシナリオでは、一部のフォレスト（resourceforest1.local、resourceforest2.local）はリソース（VDA など）を含み、一部のフォレスト（userforest1.local、userforest2.local）ユーザーのみを含みます。これらのフォレスト間には、ユーザーがリソースにログオンできる信頼関係が存在します。

単一の Cloud Connector セットがresourceforest1.localフォレストに展開されます。別の Cloud Connector セットがresourceforest2.localフォレスト内に展開されます。

単一の Connector Appliance セットがuserforest1.localフォレストに展開され、その同じセットがuserforest2.localフォレスト内に展開されます。

- 信頼関係：双方向のフォレストの信頼、またはリソースフォレストからユーザーフォレストへの一方向の信頼
- [**ID** およびアクセスの管理]に表示されるドメイン:resourceforest1.local、resourceforest2.local、userforest1.local、userforest2.local
- Citrix Workspace にログオンできるユーザー：すべてのユーザー
- オンプレミス StoreFront にログオンできるユーザー: すべてのユーザー

ワークスペースのセットアップ

December 20, 2023

Citrix Workspace は、エンドユーザーがいつでもどこでも、どのデバイスでも作業を行うことができるようにする包括的なデジタルワークスペースソリューションです。ユーザーは、Web ブラウザーまたはデバイスにインストールされている Workspace アプリ経由で Citrix Workspace にサインインします。サインイン後、ユーザーは使用が許可されているアプリケーションとデスクトップにアクセスできます。

ワークスペースの機能

- Citrix フェデレーション認証サービスを使用したシングルサインオンを有効にします。
- 組織のリソースの適切な使用法を説明する、エンドユーザー用のサインインポリシーを作成します。

- ネットワークの場所を使用して、内部ユーザーがワークスペースリソースにすばやく接続できるようにし、Citrix Gateway によって内部ユーザーがワークスペースにルーティングされるようにします。
- エンドユーザーが Citrix Workspace を離れることなく、必要に応じてドメインパスワードを変更できるようにします。
- サイトアグリゲーションを使用して、StoreFront ではなく Citrix Workspace によってオンプレミスの Virtual Apps and Desktops 環境でリソースにアクセスできるようにします。
- サービス継続性を有効にして、クラウドサービスが停止した場合でも、エンドユーザーがワークスペースリソースにアクセスできるようにします。

追加情報

- Citrix Cloud Japan のワークスペースの違い：サービスの機能の可用性
- シングルサインオン：Citrix フェデレーション認証サービスを使用したワークスペースへのシングルサインオンの有効化
- ネットワークの場所：直接ワークロード接続でワークスペースへの接続を最適化
- サイトアグリゲーション：オンプレミスの Virtual Apps and Desktops をワークスペースに集約
- サービス継続性
- ドメインパスワードの変更：利用者がアカウントのパスワードを変更できるようにする
- サインインポリシー：サインインポリシーの構成

ワークスペースの構成

Citrix DaaS 環境をセットアップ後、次のタスクを実行してワークスペースを構成します：

1. Citrix Workspace でサービス統合を有効にします。Citrix DaaS のサービス統合では、以前の名称である Virtual Apps and Desktops が引き続き使用される場合があります。Citrix Workspace ドキュメントの「サービスをワークスペースに統合する」を参照してください。
2. ［ワークスペース構成］**>**［認証］で、エンドユーザーの優先ワークスペース認証方法として、先ほど構成した ID プロバイダーを選択します。
3. オンプレミスの Citrix Gateway または Citrix Gateway サービスで、リモートエンドユーザーのワークスペースへのセキュアなアクセスを構成します。
4. シングルサインオンやサービス継続性などのワークスペース機能を構成します。

ワークスペースをカスタマイズする

1. ワークスペースのデフォルトのテーマをカスタマイズします。
2. エンドユーザーがアクセス するワークスペース URLをカスタマイズします。
3. お気に入りのアプリやデスクトップ がワークスペースのエンドユーザーにどのように表示されるかをカスタマイズします。

4. Web ブラウザーまたは Workspace アプリ経由でワークスペースにアクセスするエンドユーザーの非アクティブタイムアウトを構成します。
5. Citrix DaaS 環境経由で提供するアプリとデスクトップをエンドユーザーが起動する方法をカスタマイズします。

ID およびアクセス管理

March 27, 2024

ID プロバイダーは、次の目的で使用されます:

- 管理者が Citrix Cloud Japan にサインインするときに認証する
- ライブラリオファリングをワークスペース利用者に割り当てるためのユーザー一覧へのアクセスを提供する
- Citrix Workspace アプリを介してサインインするときにワークスペース利用者を認証します。

Citrix Cloud Japan は、次の ID プロバイダーをサポートしています。これらの ID プロバイダーを使用して、Citrix Cloud 管理者、ワークスペース利用者、またはその両方を認証できます。

ID プロバイダー	管理者認証	利用者認証
Citrix ID プロバイダー（デフォルト）	はい	いいえ
オンプレミス Active Directory (AD)	いいえ	はい
Azure Active Directory	はい	はい
オンプレミスの Citrix Gateway	いいえ	はい
Okta	いいえ	はい
SAML 2.0	はい（AD グループのみ - プレビュー）	はい

管理者認証

Citrix Cloud Japan はデフォルトでは、組み込みの ID プロバイダーを使用して、管理者をサインイン時に認証します。または、Azure AD を ID プロバイダーとして接続して、Citrix Cloud Japan 管理者を認証することもできます。SAML 2.0 を使用して AD の管理者グループを認証することもできます。

管理者認証に Azure AD または SAML 2.0 を使用する場合、管理者は一意の URL を使用して Citrix Cloud Japan にサインインできます。サインインするには、管理者は Citrix Cloud Japan アカウントの識別子を入力します。

> 注:
>
> 管理者認証に Azure AD を使用する場合、Citrix ID プロバイダーに少なくとも 1 つのフルアクセスのアカウントを維持することをお勧めします:
>
> - 代替 ID プロバイダーをセットアップする前に Azure AD が切断された場合でも、Citrix Cloud Japan アカウントからロックアウトされることはありません。
> - Citrix Cloud Japan アカウントにアクセスすることで、Azure AD 経由で管理者としてサインインした場合に完了できない特定の操作を実行できます。たとえば、Citrix が Azure AD に接続している Azure AD アプリケーションを更新する場合は、Citrix Cloud Japan アカウントでも更新されていることを確認してください。この更新を実行できるのは、Citrix ID プロバイダーのフルアクセス管理者のみです。

Workspace の認証

サポートされているすべての ID プロバイダー（Citrix ID プロバイダーを除く）を使用して、ワークスペース利用者が Citrix Workspace アプリからサインインするときに認証できます。

ID プロバイダーの前提条件

Citrix Cloud Japan に接続する前に、次のサポートされている ID プロバイダーで Citrix Cloud Connector をオンプレミス環境にインストールする必要があります:

- Active Directory
- オンプレミスの Citrix Gateway
- Okta
- SAML 2.0

サポートされている各 ID プロバイダーの前提条件について は、この記事の「詳細情報」を参照してください。

ユーザーへのアプリケーションとデスクトップの配信

Citrix DaaS を使用する場合は、次のいずれかの方法を使用して、AD または Azure AD のユーザーとグループをリソースに割り当てます。

- Studio で、目的のアプリケーションとデスクトップで構成されるデリバリーグループを作成し、AD からアクセスが許可されたユーザーを指定します。
- Studio では、配信のために必要なアプリケーションとデスクトップを含むデリバリーグループを形成し、それをライブラリ内のオファリングとして表示します。次に、ライブラリを使用して、デリバリーグループ内のリソースへのアクセスを許可されている AD または Azure AD からユーザーを選択する。この方法では、AD または Azure AD を ID プロバイダーとして Citrix Cloud Japan に接続する必要があります。

追加情報

ID プロバイダーを Citrix Cloud Japan に接続する手順については、次の記事を参照してください:

- Active Directory を ID プロバイダーとして接続
- Azure Active Directory を ID プロバイダーとして接続
- オンプレミスの Citrix Gateway を ID プロバイダーとして接続
- Okta を ID プロバイダーとして接続
- SAML を ID プロバイダーとして接続

Active Directory を **Citrix Cloud Japan** に接続する

October 8, 2021

デフォルトでは、Citrix ID プロバイダーを使用して、Citrix Cloud Japan アカウントのすべてのユーザーの ID 情報を管理します。これを Active Directory（AD）の使用に変更できます。

オンプレミスの Active Directory を Citrix Cloud Japan に接続するには、ドメインに Cloud Connector をインストールする必要があります。可用性を高めるため、Cloud Connector を 2 つインストールすることを Citrix ではお勧めします。要件と手順については、「Citrix Cloud Connector の要件」を参照してください。

Active Directory を **Citrix Cloud Japan** に接続するには

1. Citrix Cloud メニューで、[**ID** およびアクセス管理] を選択します。
2. [認証] タブの [**Active Directory**] で、省略記号メニューをクリックし、[接続] を選択します。
3. [コネクタのインストール] をクリックして、Cloud Connector ソフトウェアをダウンロードします。
4. Cloud Connector インストーラーを起動し、インストールウィザードの指示に従って操作します。
5. [**Active Directory** に接続する] ページで、[検出] をクリックします。確認後、Citrix Cloud は Active Directory が接続されているというメッセージを表示します。
6. [認証に戻る] をクリックします。**Active Directory** エントリは、[認証] タブで [有効] とマークされます。

ワークスペースの **AD** 認証を有効にする

AD を Citrix Cloud Japan に接続すると、AD 経由で自分のワークスペースに認証する許可を利用者に付与できます。

1. Citrix Cloud Japan コンソールで左上隅のメニューボタンをクリックし、[ワークスペース構成] を選択します。
2. [認証] タブで、[**Active Directory**] を選択します。
3. [確認] をクリックして Azure AD 認証を有効にした場合のワークスペース環境の変更を承諾します。

Azure Active Directory を ID プロバイダーとして接続

November 21, 2023

デフォルトでは、Citrix ID プロバイダーを使用して、Citrix Cloud Japan アカウントのすべてのユーザーの ID 情報を管理します。これを変更し、Azure Active Directory (AD) を使用して Citrix Cloud Japan 管理者と Workspace 利用者を認証できます。

Citrix Cloud Japan で Azure AD を使用すると、次のことができるようになります:

- 独自の Active Directory を使用して、監査、パスワードポリシーを制御し、必要に応じて簡単にアカウントを無効にできます。
- 多要素認証を構成して高いレベルのセキュリティを実現し、盗まれたサインイン資格情報が使用される可能性を回避します。
- ブランド設定済みのログインページを使用するため、ユーザーは正しい場所にログインしていることを確認できます。
- ADFS、Okta、Ping などの任意の ID プロバイダーにフェデレーションを使用できます。

Azure AD アプリケーションと権限

Citrix Cloud Japan には Azure AD アプリが含まれているため、アクティブな Azure AD セッションにログインする必要なく Azure AD に接続できます。Citrix Cloud Japan が Azure AD との接続に使用する Azure AD アプリケーションと権限について詳しくは、「Citrix Cloud Japan 用の Azure Active Directory の権限」を参照してください。

Active Directory と Azure AD を準備する

Azure AD を使用する前に、次の要件を満たしていることを確認してください:

- Microsoft Azure アカウントを持っている。すべての Azure アカウントに無料の Azure AD が付属しています。Azure アカウントをお持ちでない場合は、https://azure.microsoft.com/en-us/free/?v=17.36に登録してください。
- Azure AD にはグローバル管理者の役割があります。この役割は、Citrix Cloud Japan が Azure AD と接続できるようにするために必要です。
- 管理者アカウントには、**Azure AD** で構成された「**mail**」プロパティがあります。Microsoft のAzure AD Connectツールを使用することで、オンプレミスの Active Directory アカウントを Azure AD と同期させることができます。または、Office 365 のメールで同期されていない Azure AD アカウントを構成することもできます。

Azure AD Connect でアカウントを同期する

1. Active Directory アカウントにメールのユーザープロパティが構成されていることを確認します:
    a) ［Active Directory ユーザーとコンピューター］を開きます。
    b) **Users** フォルダーで、確認するアカウントを見つけて右クリックし、［プロパティ］を選択します。［全般］タブで、［メール］フィールドに有効なエントリがあることを確認します。Citrix Cloud Japan では、Azure AD から追加された管理者には、Citrix がホストする ID を使用してサインインする管理者とは異なるメールアドレスが必要です。
2. Azure AD Connect をインストールおよび構成します。手順について詳しくは、Microsoft Azure Web サイトでオンプレミスのディレクトリと Azure Active Directory の統合を参照してください。

Citrix Cloud Japan を Azure AD に接続する

Citrix Cloud Japan アカウントを Azure AD に接続する場合、Azure AD のユーザーの基本プロファイルだけでなく、ユーザープロファイル（またはサインインしたユーザーのプロファイル）へのアクセス権限が必要です。Citrix はこの権限を要求し、（管理者の）名前とメールアドレスを取得して、管理者が後で他のユーザーを管理者として追加することができるようにします。

1. Citrix Cloud Japan にサインインします（https://citrix.citrixcloud.jp）。
2. ページの左上隅にあるメニューボタンをクリックし、［**ID** およびアクセス管理］を選択します。
3. **Azure Active Directory** を見つけ、省略記号ボタンをクリックして ［接続］を選択します。
4. 入力画面が表示されたら、URL に適した短い会社の識別子を入力し、［接続］をクリックします。この識別子は、Citrix Cloud Japan 内でグローバルに一意である必要があります。
5. 入力画面が表示されたら、接続する Azure アカウントにサインインします。Azure は、Citrix Cloud Japan がアカウントにアクセスして接続に必要な情報を取得するためのアクセス権限を表示します。
6. ［承諾］をクリックして権限の要求を承諾します。

Azure AD から Citrix Cloud Japan に管理者を追加する

1. Citrix Cloud Japan 管理コンソールの［**ID** およびアクセス管理］ページで［管理者］タブをクリックします。
2. ［管理者/グループを追加する］を選択します。
3. ［管理者の詳細］で、［**Azure AD**］を選択します。
4. 追加するユーザーの名前を入力し、［次へ］をクリックします。Azure AD ゲストユーザーの招待はサポートされていません。
5. ［アクセスの設定］で、管理者に適切な権限を設定します。
6. 管理者の詳細を確認します。変更するには、［戻る］を選択します。
7. ［招待を送信］を選択します。Citrix Cloud Japan は、指定されたメールアドレスに招待メールを送信し、管理者を一覧に追加します。

メールのリンクをクリックして、会社の Azure Active Directory にサインインします。これにより、ユーザーのメールアドレスが確認され、Azure AD ユーザーアカウントと Citrix Cloud Japan 間の接続が完了します。

Azure AD 管理者グループから **Citrix Cloud Japan** に管理者を追加する

Azure Active Directory（AD）グループを使用して、Citrix Cloud Japan アカウントに管理者を追加できます。その後、グループ内のすべての管理者のサービスアクセス許可を管理できます。

この機能は、**Citrix DaaS**（Virtual Apps and Desktops サービスの新名称）での使用のみがサポートされています。グループ内の管理者は、Citrix Cloud Japan アカウントのその他のサービスを管理するためのアクセス権を持っていません。

詳しくは、「管理者グループを管理する」を参照してください。

Azure AD を使用して **Citrix Cloud Japan** にサインインする

Azure AD ユーザーアカウントの接続後、管理者は次のいずれかの方法で Citrix Cloud Japan にサインインできます:

- 会社の Azure AD ID プロバイダーを最初に接続した時に構成した管理者のサインイン URL に移動します。例: `https://citrix.citrixcloud.jp/go/myorganization`
- Citrix Cloud Japan のサインインページで、［会社の資格情報でサインイン］をクリックし、最初に Azure AD を接続したときに作成した識別子を入力し、［続行］をクリックします。

ワークスペースの **Azure AD** 認証を有効にする

Azure AD を Citrix Cloud Japan に接続すると、Azure AD 経由で自分のワークスペースに認証する許可を利用者に付与できます。

> 重要:
>
> Azure AD ワークスペース認証を有効にする前に、Citrix Workspace で Azure AD を使用するための考慮事項について「Azure Active Directory」セクションで確認してください。

1. 左上隅の Citrix Cloud Japan メニューから、［ワークスペースの構成］を選択します。
2. ［認証］タブ、［**Azure Active Directory**］の順に選択します。
3. ［確認］をクリックして Azure AD 認証を有効にした場合のワークスペース環境の変更を承諾します。

高度な **Azure AD** 機能を有効にする

Azure AD は、高度な多要素認証、国際的レベルのセキュリティ機能、20 種類の ID プロバイダーとのフェデレーション、セルフサービスパスワードの変更とリセットなどの機能を提供します。Azure AD ユーザーでこれらの機能を有効にすると、Citrix Cloud Japan が自動的に使用できるようになります。

アプリのアップデートに対応するため **Azure AD** に再接続する

2022 年 4 月に、Citrix Cloud Japan で使用された Azure AD アプリが更新され、Group.Read.All 権限の代わりに GroupMember.Read.All 権限を使用するようになりました。

2022 年 4 月より前に Azure AD を Citrix Cloud Japan に接続しており、最新の更新済みアプリを使用する場合は、Azure AD を Citrix Cloud Japan から切断し、再接続する必要があります。最新のアプリの使用は任意です。アプリを更新しないことを選択した場合でも、既存の接続は正常に機能します。

要件

Azure AD を再接続する前に、次の要件を満たしていることを確認してください:

- Azure AD のグローバル管理者である必要があります。Azure AD を再接続するときは、Azure AD のグローバル管理者の役割を使用して、Citrix Cloud Japan にアプリケーションレベルの権限を付与します。これにより、Citrix Cloud Japan が Azure AD に再接続できるようになります。詳しくは、「Citrix Cloud Japan 用の Azure Active Directory の権限」を参照してください。
- デフォルトの Citrix ID プロバイダーのフルアクセス権限を持つ管理者である必要があります。Azure AD の資格情報を使用して Citrix Cloud Japan にサインインしている場合、再接続は失敗します。アカウントに Citrix ID プロバイダーを使用する管理者がいない場合は、一時的にアカウントを追加して、Azure AD に再接続した後にそのアカウントを削除できます。手順については、「個別の管理者を招待する」を参照してください。
- Azure AD を使用してワークスペース利用者を認証している場合は、一時的に別の ID プロバイダーを選択します。Azure AD が Citrix Workspace の認証方法としても使用されている場合、Citrix Cloud Japan では Azure AD を切断できません。詳しくは、Citrix Workspace ドキュメントの「認証方法の選択または変更」を参照してください。

Azure AD を再接続するには

1. Citrix ID プロバイダーのフルアクセス権を持つ管理者として、Citrix Cloud Japan にサインインします。
2. Citrix Cloud Japan メニューから、［**ID** およびアクセス管理］を選択し、次に ［認証］を選択します。
3. **Azure Active Directory** を見つけ、ページの右端にある省略記号（…）メニューから［切断］を選択します。
4. 省略記号メニューの ［接続］を選択します。
5. プロンプトが表示されたら、グローバル管理者の資格情報を使用して Azure アカウントにサインインします。Azure は、Citrix Cloud Japan がアカウントにアクセスして接続に必要な情報を取得するための権限を表示します。
6. ［承諾］を選択して権限の要求を承諾します。

Citrix Cloud Japan 用の Azure Active Directory の権限

December 20, 2023

この記事では、Azure Active Directory（AD）を接続して使用するときに Citrix Cloud Japan が要求する権限について説明します。Citrix Cloud Japan アカウントで Azure AD がどのように使用されるかによって、ターゲットの Azure AD テナントに 1 つまたは複数のエンタープライズアプリケーションが作成されることがあります。アカウントごとにアプリケーションのセットを作成しなくても、複数の Citrix Cloud Japan アカウントを 1 つの Azure AD テナントに接続し、同じエンタープライズアプリケーションを使用できます。

> 注:
>
> 2022 年 4 月、Citrix Cloud Japan が Azure AD の接続のために使用する Azure AD アプリは、Group.Read.All 権限の代わりに GroupMember.Read.All 権限を使用するように更新されました。既存の（2022 年 4 月より前の）Azure AD 接続により、アプリで新しい権限を使用する場合は、Azure AD を切断してから Citrix Cloud Japan に再接続する必要があります。この操作により、Citrix Cloud Japan で最新の Azure AD アプリが使用されるようになります。詳しくは、「アプリのアップデートに対応するため Azure AD に再接続する」を参照してください。
>
> アプリを更新しないことを選択した場合でも、既存の接続は正常に機能します。

エンタープライズアプリケーション

次の表では、Citrix Cloud Japan で Azure AD の接続時および使用時に使用される Azure AD エンタープライズアプリケーションと、各アプリケーションの使用目的を示します。

名前	アプリケーション ID	使用状況
Citrix Cloud ProductionJP	f751768a-a91d-4306-af65-448ab59e2c85	ワークスペース利用者ログイン
CC-Directory-ProductionJP	6550e1c7-8970-46bc-82b6-ebd920ff255d	Azure AD と Citrix Cloud Japan 間のデフォルト接続
Athena ProductionJP	6464247d-8d40-42b9-a75e-4660db847454	管理者の招待とログイン

アクセス権

Citrix Cloud Japan のエンタープライズアプリケーションの権限があれば、Citrix Cloud Japan は Azure AD テナント内の特定のデータにアクセスできます。Citrix Cloud Japan はこれらのデータを使用して、Azure AD テナントに接続する、専用のサインイン URL を使用した管理者による Citrix Cloud Japan へのサインインを可能にするなど、特定の機能を実行します。Citrix Cloud Japan がこれらのデータにアクセスするには、管理者の同意が必要で

す。これらのアクセス権限は、Citrix Cloud Japan が Azure AD と連携するための必要最低限の特権です。Azure AD の権限と同意について詳しくは、Microsoft Azure ドキュメント Web サイトの「Microsoft ID プラットフォームでのアクセス許可と同意」を参照してください。

本記事では、Azure AD アプリケーション権限の各セットについて次の情報を記載しています:

- **API** 名: Citrix Cloud Japan が権限を要求するリソースアプリケーション。Microsoft Graph と Windows Azure Active Directory のことです。Citrix Cloud Japan は、この 2 つのリソースアプリケーションに同じ権限を要求します。
- タイプ: Citrix Cloud Japan が特定の権限に対して要求するアクセスレベル。特定のエンタープライズアプリケーションの権限には、次のいずれかのアクセスレベルを設定できます:
  - 委任権限は、ユーザーのプロファイルを照会する場合など、サインインユーザーの代理として操作するために使用されます。
  - アプリケーション権限 は、特定のグループ内のユーザーを照会する場合など、ユーザー不在でアプリケーションが操作を実行するときに使用されます。この種類の権限を付与するには、Azure AD のグローバル管理者の同意が必要です。
- 要求値: Azure AD が特定の権限に割り当てる情報の文字列。特定のエンタープライズアプリケーションの権限には、次のいずれかの要求値を設定できます:
  - **User.Read**: Citrix Cloud Japan 管理者が、接続された Azure AD のユーザーを Citrix Cloud Japan アカウントの管理者として追加できるようにします。
  - **User.ReadBasic.All**: ユーザーのプロファイルから基本情報を収集します。これは`User.Read.All`のサブセットですが、下位互換性のために権限自体は残ります。
  - **User.Read.All**: Citrix Cloud Japan は、Microsoft Graph のList usersを呼び出して、顧客が接続した Azure AD からユーザーを参照および選択できるようにします。たとえば、Azure AD のユーザーに対し、ワークスペースを使用した Citrix DaaS リソースへのアクセス権限を付与できます。Citrix Cloud Japan は、`onPremisesSecurityIdentifier`などの基本プロファイル以外のプロパティにアクセスする必要があるため、`User.ReadBasic.All`を使用できません。
  - **GroupMember.Read.All**: Citrix Cloud Japan は、Microsoft Graph のList groupsを呼び出して、顧客が接続した Azure AD からグループを参照および選択できるようにします。たとえば、Azure AD のグループに対しては、Citrix DaaS アプリケーションへのアクセス権限を付与することもできます。

ワークスペース利用者ログイン

Citrix Cloud ProductionJP（ID: f751768a-a91d-4306-af65-448ab59e2c85）は、Microsoft Graph と Windows Azure Active Directory リソースアプリケーションの両方で、同じ権限を使用します。

API 名	要求値	権限名	種類
Microsoft Graph	User.Read	サインインとユーザープロファイルの読み取り	委任
Windows Azure Active Directory	User.Read	サインインとユーザープロファイルの読み取り	委任

Azure AD と **Citrix Cloud Japan** 間のデフォルト接続

CC-Directory-ProductionJP アプリケーション（ID：6550e1c7-8970-46bc-82b6-ebd920ff255d）は、次の権限を使用します：

API 名	要求値	権限	種類
Microsoft Graph	GroupMember.Read.All	すべてのグループの読み取り	委任
Microsoft Graph	User.ReadBasic.All	すべてのユーザーの基本プロファイルの読み取り	委任
Microsoft Graph	User.Read.All	すべてのユーザーの完全なプロファイルの読み取り	委任
Microsoft Graph	User.Read	サインインとユーザープロファイルの読み取り	委任
Microsoft Graph	GroupMember.Read.All	すべてのグループの読み取り	アプリケーション
Microsoft Graph	User.Read.All	すべてのユーザーの完全なプロファイルの読み取り	アプリケーション

管理者の招待とログイン

Athena ProductionJP アプリケーション（ID：6464247d-8d40-42b9-a75e-4660db847454）は、次の権限を使用します：

API 名	要求値	権限名	種類
Microsoft Graph	User.Read	サインインとユーザープロファイルの読み取り	委任
Microsoft Graph	User.ReadBasic.All	すべてのユーザーの基本プロファイルの読み取り	委任

オンプレミスの **Citrix Gateway** を **ID** プロバイダーとして接続

November 21, 2023

Citrix Cloud Japan では、オンプレミスの Citrix Gateway を ID プロバイダーとして使用して、ワークスペースにサインインする利用者が認証されるようにできます。

Citrix Gateway 認証を使用すると、以下のことを実行できます:

- 引き続き、既存の Citrix Gateway でユーザーを認証するため、Citrix Workspace 経由でオンプレミスの Virtual Apps and Desktops のリソースにアクセスできます。
- Citrix Workspace で Citrix Gateway の認証、承認、および監査（AAA: authentication, authorization, and auditing）機能を使用します。
- パススルー認証、スマートカード、セキュアトークン、条件付きアクセスポリシー、フェデレーション、その他多くの機能を使用しながら、ユーザーに必要なリソースへの Citrix Workspace 経由のアクセスを提供できます。

> ヒント:
>
> 「Citrix ID と認証の概要」教育コースで、サポートされている ID プロバイダーの詳細をご覧ください。「Citrix Identity and Access Management の計画」モジュールには、この ID プロバイダーを Citrix Cloud Japan に接続して Citrix Workspace の認証を有効にする方法を説明した短い動画があります。

サポートされるバージョン

Citrix Gateway 認証は、次のオンプレミス製品バージョンでの使用がサポートされています:

- Citrix Gateway 12.1 54.13 Advanced Edition 以降
- Citrix Gateway 13.0 41.20 Advanced Edition 以降

前提条件

Cloud Connector

Citrix Cloud Connector ソフトウェアのインストール先となるサーバーが少なくとも 2 台必要です。これらのサーバーは、次の要件を満たしている必要があります:

- 「Citrix Cloud Connector の要件」に記載されているシステム要件を満たしている。
- 他の Citrix コンポーネントはインストールされておらず、Active Directory ドメインコントローラーではなく、リソースの場所のインフラストラクチャに不可欠なマシンでもない。
- サイトが存在するドメインに参加している。ユーザーが複数のドメインにあるサイトのアプリケーションにアクセスする場合は、各ドメインに Cloud Connector を少なくとも 2 つインストールする必要があります。

- サイトに接続可能なネットワークに接続している。
- インターネットに接続済み。詳しくは、「サービス接続要件」を参照してください。
- Cloud Connector の可用性を高めるため、サーバーは 2 台用意することを Citrix ではお勧めします。インストール後、Citrix Cloud Japan は Cloud Connector によりサイトを検出して通信できるようになります。

Cloud Connector のインストールについて詳しくは、以下の記事を参照してください:

- Cloud Connector をインストールする
- コマンドラインから Cloud Connector をインストールする

Active Directory

Citrix Gateway 認証を有効にする前に、次のタスクを実行します:

- ワークスペース利用者に Active Directory（AD）のユーザーアカウントがあることを確認します。AD アカウントがない利用者は、ワークスペースにサインインできません。
- 利用者の AD アカウントのユーザープロパティが入力されていることを確認します。Citrix Cloud Japan では、利用者がサインインする際、ユーザーコンテキストを決定するためにこれらのプロパティが必要とされます。これらのプロパティが入力されていないと、利用者がワークスペースにサインインできません。これらのプロパティには以下が含まれます:
  - メールアドレス
  - 表示名
  - 共通名
  - SAM アカウント名
  - ユーザープリンシパル名
  - OID
  - SID
- Active Directory（AD）を Citrix Cloud Japan アカウントに接続します。このタスクでは、「Cloud Connector」セクションの説明に従い、準備したサーバーに Cloud Connector ソフトウェアをインストールします。Cloud Connector により、Citrix Cloud Japan がオンプレミス環境と通信できるようになります。手順については、「Azure Active Directory を Citrix Cloud Japan に接続する」を参照してください。
- Citrix Gateway 認証を使用してフェデレーションを実行している場合、AD ユーザーをフェデレーションプロバイダーと同期します。Citrix Cloud Japan では、サインインするワークスペース利用者の AD ユーザー属性が必要とされます。

要件

Citrix Gateway の拡張ポリシー

Citrix Gateway 認証では、クラシックポリシーが廃止されたため、オンプレミス Gateway の拡張ポリシーを使用する必要があります。拡張ポリシーでは、ID プロバイダーチェーンなどのオプションを含む Citrix Cloud Japan の多要素認証がサポートされています。現在クラシックポリシーを使用している場合、Citrix Cloud Japan で Citrix Gateway 認証を使用するには、新しい拡張ポリシーを作成する必要があります。拡張ポリシーを作成する際に、クラシックポリシーのアクション部分を再利用できます。

署名用証明書

Citrix Workspace の利用者を認証するために Gateway を構成する場合、Gateway は OpenID Connect プロバイダーとして機能します。Citrix Cloud Japan と Gateway 間のメッセージは OIDC プロトコルに準拠し、デジタル署名トークンが含まれます。したがって、これらのトークンに署名するための証明書を構成する必要があります。この証明書は、公的証明機関（CA）から発行される必要があります。私的 CA が発行した証明書は使用できません。Citrix Cloud Japan に私的な CA 証明書を提供する手段がないためです。そのため、信頼できる証明書チェーンを確立できません。署名用の証明書を複数構成する場合、各メッセージでこれらのキーがローテーションされます。

キーを **VPN** グローバルにバインドする必要がありますこれらのキーがないと、利用者はサインイン後にワークスペースに正常にアクセスできません。

クロック同期

OIDC のデジタル署名されたメッセージにはタイムスタンプが含まれているため、Gateway は NTP 時間に同期される必要があります。クロックが同期されていない場合、Citrix Cloud Japan でのトークンの有効性チェックでトークンが古いと判断されます。

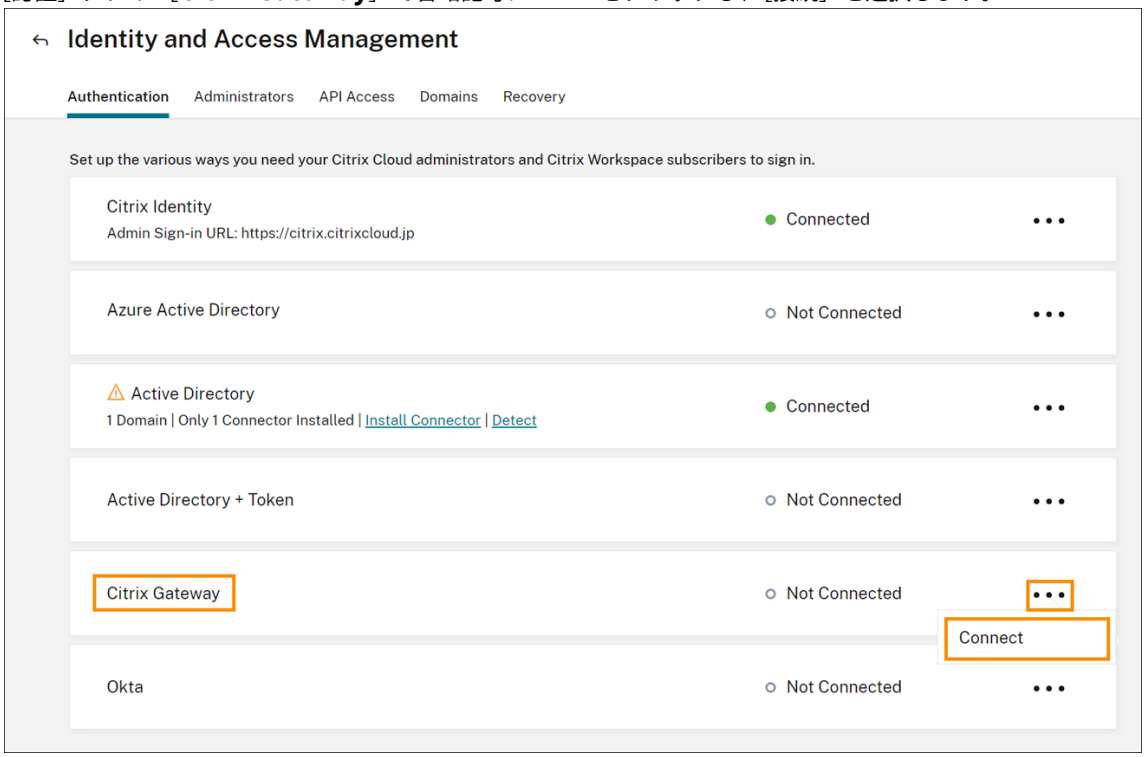
タスクの概要

Citrix Gateway 認証を設定するには、次のタスクを実行します:

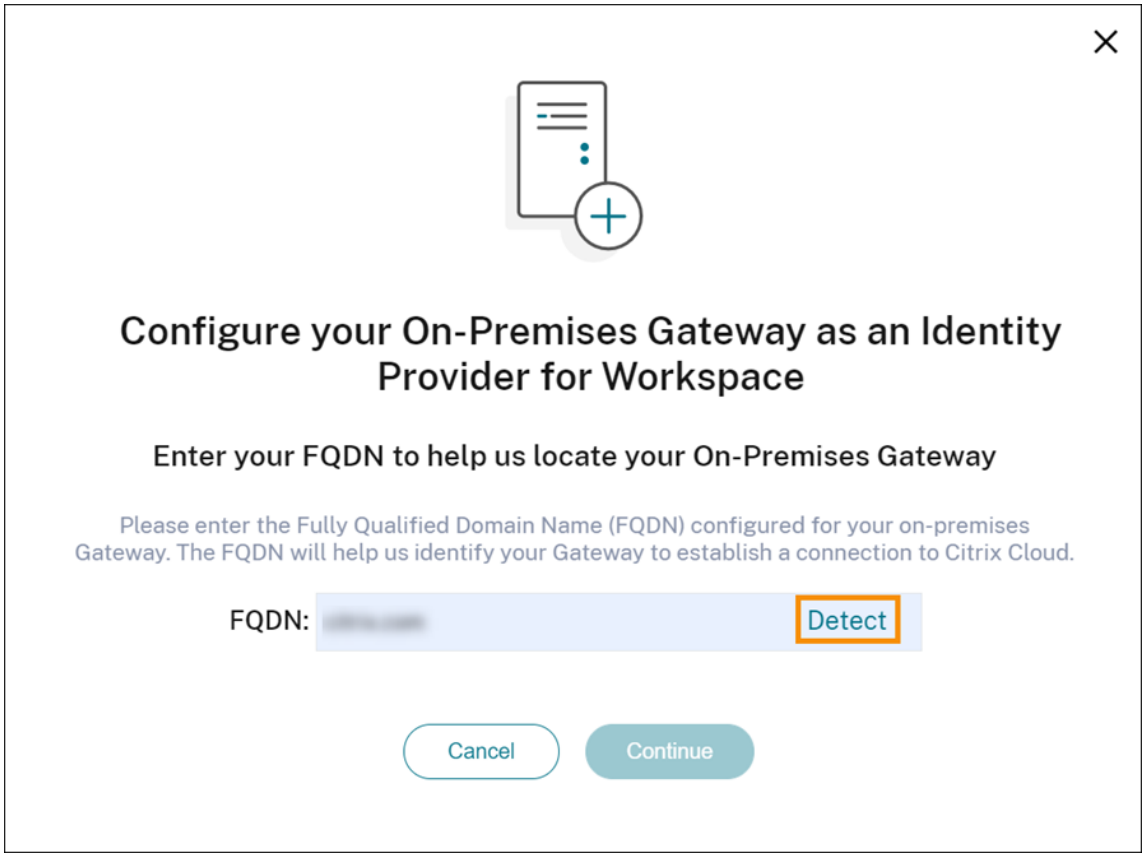
1. ［**ID** およびアクセス管理］で Gateway への接続を構成します。この手順では、Gateway のクライアント ID、シークレット、リダイレクト URL を生成します。
2. Gateway で、Citrix Cloud Japan から生成された情報を使用して OAuth ID プロバイダー拡張ポリシーを作成します。これにより Citrix Cloud Japan がオンプレミス Gateway に接続できるようになります。手順については、以下の記事を参照してください:
   - Citrix Gateway 12.1: オンプレミス Citrix Gateway を ID プロバイダーとして Citrix Cloud に使用
   - Citrix Gateway 13.0: オンプレミス Citrix Gateway を ID プロバイダーとして Citrix Cloud に使用
3. ［ワークスペース構成］で、利用者の Citrix Gateway 認証を有効にします。

Citrix Gateway 認証を構成する

1. Citrix Cloud Japan メニューで、［**ID** およびアクセス管理］を選択します。
2. ［認証］タブの ［**Citrix Gateway**］で省略記号メニューをクリックし、［接続］を選択します。



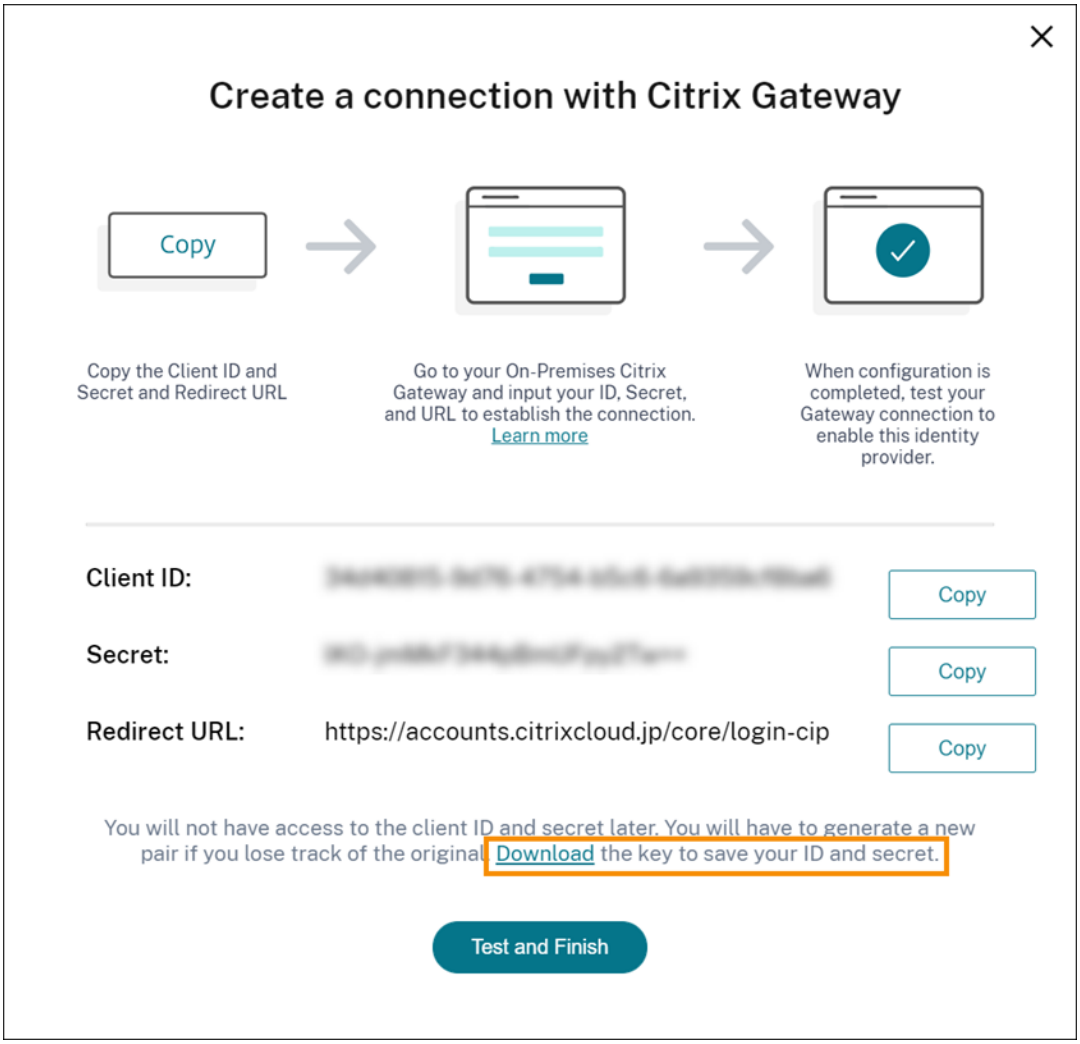
3. オンプレミス Gateway の完全修飾ドメイン名を入力して ［検出］をクリックします。



Citrix Cloud Japan が正常に FQDN を検出したら、［続行］をクリックします。

4. オンプレミス Gateway との接続を作成します:

   a) Citrix Cloud Japan で表示されるクライアント ID、シークレット、リダイレクト URL をコピーします。



また、この情報のコピーをダウンロードし、参照用としてオフラインで安全に保存します。この情報は生成後、Citrix Cloud Japan で表示することはできなくなります。

b) Gateway で、Citrix Cloud Japan のクライアント ID、シークレット、リダイレクト URL を使用して OAUth ID プロバイダー拡張ポリシーを作成します。手順については、以下の記事を参照してください:

- Citrix Gateway 12.1 の場合: オンプレミス Citrix Gateway を ID プロバイダーとして Citrix Cloud に使用
- Citrix Gateway 13.0 の場合: オンプレミス Citrix Gateway を ID プロバイダーとして Citrix Cloud に使用

c) [テストして終了] をクリックします。Citrix Cloud Japan は、Gateway が到達可能であり、正しく構成されていることを確認します。

ワークスペース利用者の **Citrix Gateway** 認証を有効にする

1. Citrix Cloud Japan メニューから、[ワークスペース構成] を選択します。
2. [認証] タブで [**Citrix Gateway**] を選択します。

3. ［利用者のエクスペリエンスに与える影響を了承しています］を選択して ［保存］をクリックします。

トラブルシューティング

最初の手順として、この記事の「前提条件」および「要件」セクションを確認します。オンプレミス環境に必要なコンポーネントがすべて揃っており、必要な構成をすべて行ったことを確認してください。これらのアイテムのいずれかが欠落しているか、正しく構成されていないと、Citrix Gateway でのワークスペース認証が機能しません。

Citrix Cloud Japan とオンプレミスの Gateway との間で接続の問題が発生した場合、以下の事項を確認してください:

- Gateway の完全修飾ドメイン名がインターネットで到達可能である。
- Citrix Cloud Japan で Gateway の完全修飾ドメイン名を正しく入力した。
- OAuth ID プロバイダーポリシーの`-issuer`パラメーターに Gateway の URL を正しく入力した（例: `-issuer https://GatewayFQDN.com`）。`issuer`パラメーターでは大文字と小文字は区別されません。
- Citrix Cloud Japan のクライアント ID、シークレット、リダイレクト URL の値が、OAuth ID プロバイダーポリシーの［クライアント ID］［クライアントシークレット］、［リダイレクト URL］、［オーディエンス］フィールドに正しく入力されている。ポリシーの［オーディエンス］フィールドに正しいクライアント ID が入力されていることを確認します。
- OAuth ID プロバイダー認証ポリシーが正しく構成されている。手順については、以下の記事を参照してください。
  - Citrix Gateway 12.1: オンプレミス Citrix Gateway を ID プロバイダーとして Citrix Cloud に使用
  - Citrix Gateway 13.0: オンプレミス Citrix Gateway を ID プロバイダーとして Citrix Cloud に使用
- ポリシーが「認証ポリシーのバインド」に記載されている手順で、AAA 認証サーバーに正しくバインドされていることを確認します。

グローバルカタログサーバー

Gateway は、ユーザーアカウントの詳細に加えて、ユーザーのドメイン名、Active Directory の NETBIOS 名、およびルート Active Directory ドメイン名を取得します。Active Directory の NETBIOS 名を取得するために、Gateway はユーザーアカウントが存在する Active Directory を検索します。NETBIOS 名はグローバルカタログサーバーに複製されません。

Active Directory 環境でグローバルカタログサーバーを使用する場合、これらのサーバーで構成された LDAP アクションは Citrix Cloud Japan で機能しません。代わりに、LDAP アクションで個別の Active Directory を構成する必要があります。複数のドメインまたはフォレストがある場合、複数の LDAP ポリシーを構成できます。

Kerberos または **ID** プロバイダーチェーンを使用したシングルサインオンの **Active Directory** 検索

Kerberos か、利用者のサインインに SAML または OIDC プロトコルを使用するまたは外部 ID プロバイダーを使用する場合、Active Directory 参照が構成されていることを確認します。Gateway では、利用者の Active Directory ユーザープロパティと Active Directory 構成プロパティを取得するために Active Directory 参照が必要です。

認証がサードパーティのサーバーによって処理される場合でも、LDAP ポリシーが構成されていることを確認してください。これらのポリシーを構成するには、以下のタスクを実行して既存のログインスキーマプロファイルに第 2 の認証要素を追加します:

1. Active Directory から属性およびグループの抽出のみを実行する LDAP 認証サーバーを作成します。
2. LDAP 拡張認証ポリシーを作成します。
3. 認証ポリシーラベルを作成します。
4. プライマリ ID プロバイダーのあとの次の要素として認証ポリシーラベルを定義します。

LDAP を第 **2** の認証要素として追加するには

1. LDAP 認証サーバーを作成します:
    a) [**System**] > [**Authentication**] > [**Basic Policies**] > [**LDAP**] > [**Servers**] > [**Add**] を選択します。
    b) [**Create Authentication LDAP Server**] ページで次の情報を入力します:
        - [**Choose Server Type**] で [**LDAP**] を選択します。
        - [**Name**] でサーバーのフレンドリ名を入力します。
        - [**Server IP**] を選択してから LDAP サーバーの IP アドレスを入力します。
        - [**Security Type**] で必要な LDAP セキュリティの種類を選択します。
        - [**Server Type**] で [**AD**] を選択します。
        - [**Authentication**] ではチェックボックスをオンにしないでください。この認証サーバーは、Active Directory からユーザー属性とグループを抽出するだけで認証用ではないので、チェックボックスはオフにする必要があります。
    c) [**Other Settings**] で、次の情報を入力します:
        - [**Server Logon Name Attribute**] で、**UserPrincipalName** を選択します。
        - [**Group Attribute**] で **memberOf** を選択します。
        - [**Sub Attribute Name**] で **cn** を選択します。
2. LDAP 拡張認証ポリシーを作成します。
    a) [**Security**] > [**AAA - Application Traffic**] > [**Policies**] > [**Authentication**] > [**Advanced Policies**] > [**Policy**] > [**Add**] を選択します。
    b) [**Create Authentication Policy**] ページで次の情報を入力します:
        - [**Name**] でポリシーのフレンドリ名を入力します。
        - [**Action Type**] で [**LDAP**] を選択します。

- ［**Action**］で作成済みの LDAP 認証サーバーを選択します。
- ［**Expression**］で **TRUE** と入力します。

c) ［作成］をクリックしてこの構成を保存します。

3. 認証ポリシーラベルを作成します:

a) ［**Security**］**>** ［**AAA - Application Traffic**］**>** ［**Policies**］**>** ［**Authentication**］**>** ［**Advanced Policies**］**>** ［**Policy Label**］**>** ［**Add**］を選択します。
b) ［**Name**］で認証ポリシーラベルのフレンドリ名を入力します。
c) ログインスキーマで **LSCHEMA_INT** を選択します。
d) ［**Policy Binding**］の ［**Select Policy**］で、作成済みの LDAP 拡張認証ポリシーを選択します。
e) ［**GoTo Expression**］で **END** を選択します。
f) ［**Bind**］をクリックして、構成を完了します。

4. LDAP 認証ポリシーラベルをプライマリ ID プロバイダーの次の要素として定義します:

a) ［**System**］**>** ［**Security**］**>** ［**AAA - Application Traffic**］**>** ［**Virtual Servers**］を選択します。
b) プライマリ ID プロバイダーのバインディングを含む仮想サーバーを選択して、［**Edit**］を選択します。
c) ［**Advanced Authentication Policies**］で既存の ［**Authentication Policy**］バインディングを選択します。
d) プライマリ ID プロバイダーのバインディングを選択して、［**Edit Binding**］を選択します。
e) ［**Policy Binding**］ページの ［**Select Next Factor**］で、作成済みの LDAP 拡張認証ポリシーを選択します。
f) ［**Bind**］をクリックして、構成を保存します。

多要素認証のデフォルトパスワード

ワークスペース利用者に多要素認証を使用する場合、Gateway ではシングルサインオンのデフォルトパスワードとして最後の要素のパスワードが使用されます。このパスワードは、利用者がワークスペースにサインインする際に Citrix Cloud Japan に送信されます。環境内で LDAP 認証の後に別の要素が続く場合、Citrix Cloud Japan に送信されるデフォルトパスワードとして LDAP パスワードを構成する必要があります。LDAP 要素に対応するログインスキーマで、**SSOCredentials** を有効にします。

Okta を **ID** プロバイダーとして接続

February 8, 2023

Citrix Cloud Japan では、ワークスペースにサインインする利用者を認証するための ID プロバイダーとして使用して、Okta を使用できます。Okta 組織を Citrix Cloud Japan に接続することにより、Citrix Workspace のリソースにアクセスする利用者に共通のサインイン操作を提供できます。

ワークスペース構成で Okta 認証を有効にした後、利用者のサインイン操作は変化します。Okta 認証を選択すると、シングルサインオンではなく、フェデレーション ID によるサインイン環境となります。利用者は、Okta サインインページからワークスペースにサインインしますが、Citrix DaaS（Citrix Virtual Apps and Desktops サービスの新名称）からアプリまたはデスクトップを起動するときにもう一度認証する必要があります。シングルサインオンを有効にし、2 つ目のログオンプロンプトが表示されないようにするには、Citrix Cloud Japan で Citrix フェデレーション認証サービスを使用する必要があります。詳しくは、「Citrix フェデレーション認証サービスを使用したワークスペースに対するシングルサインオンの有効化」を参照してください。

前提条件

Cloud Connector

Active Directory ドメインで、Citrix Cloud Connector ソフトウェアのインストール先となるサーバーが少なくとも 2 台必要です。Cloud Connector は、Citrix Cloud Japan とリソースの間で通信するために必要です。Cloud Connector の可用性を高めるため、サーバーは 2 台用意することを Citrix ではお勧めします。これらのサーバーは、次の要件を満たしている必要があります:

- 「Citrix Cloud Connector の要件」に記載されている要件を満たしている。
- 他の Citrix コンポーネントはインストールされておらず、Active Directory ドメインコントローラーではなく、リソースの場所のインフラストラクチャに不可欠なマシンでもない。
- Active Directory（AD）ドメインに参加している。ワークスペースリソースとユーザーが複数のドメインに存在する場合は、各ドメインに Cloud Connector を少なくとも 2 つインストールする必要があります。詳しくは、「Active Directory での Cloud Connector 展開シナリオ」を参照してください。
- ユーザーが Citrix Workspace を介してアクセスするリソースにアクセスできるネットワークに接続済み。
- インターネットに接続済み。詳しくは、「サービス接続要件」を参照してください。

Cloud Connector のインストールについて詳しくは、以下の記事を参照してください:

- Cloud Connector をインストールする
- コマンドラインから Cloud Connector をインストールする

Okta ドメイン

Okta を Citrix Cloud Japan に接続する場合、組織の Okta ドメインを指定する必要があります。Citrix は、次の Okta ドメインをサポートしています:

- okta.com
- okta-eu.com
- oktapreview.com

Citrix Cloud Japan で Okta カスタムドメインを使用することもできます。Okta Web サイトの「Okta URL ドメインのカスタマイズ」で、カスタムドメインの使用に関する重要な考慮事項をレビューします。

組織のカスタムドメインを見つける方法について詳しくは、Okta Web サイトで「自身の Okta ドメインの検索」を参照してください。

Okta OIDC Web アプリケーション

Okta を ID プロバイダーとして使用するには、まず Citrix Cloud Japan で使用できるクライアント資格情報を使用して Okta OIDC Web アプリケーションを作成する必要があります。アプリケーションを作成して構成したら、クライアント ID とクライアントシークレットをメモします。Okta 組織の接続時に、これらの値を Citrix Cloud Japan に入力します。

このアプリケーションを作成および構成するには、この記事の次のセクションを参照してください:

- Okta OIDC Web アプリケーション統合の作成
- Okta OIDC Web アプリケーションの構成

ワークスペース URL

Okta アプリケーションの作成時には、Citrix Cloud Japan からのワークスペース URL を入力する必要があります。ワークスペース URL を見つけるには、Citrix Cloud Japan メニューから［ワークスペース構成］を選択します。ワークスペース URL は、［アクセス］タブに表示されます。

> 重要:
>
> 後でワークスペース URL を変更する場合、Okta アプリケーションの構成を新しい URL によって更新する必要があります。そうしないと、ワークスペースからのサインアウト時に問題が発生する可能性があります。

Okta API トークン

Citrix Cloud Japan で Okta を ID プロバイダーとして使用するには、Okta 組織の API トークンが必要です。Okta 組織で読み取り専用の管理者アカウントを使用し、このトークンを作成します。このトークンは、Okta 組織内のユーザーとグループを読み取れる必要があります。

API トークンを作成するには、この記事の「Okta API トークンの作成」を参照してください。API トークンについて詳しくは、Okta ウェブサイトで「API トークンの作成」を参照してください。

> 重要:
>
> API トークンを作成する際には、トークンの値をメモしてください（たとえば、値を一時的にプレーンテキストドキュメントにコピーしてください）。Okta ではこの値が一度だけ表示され、「Citrix Cloud Japan を Okta 組織に接続する」の手順を実行する直前にトークンを作成する場合があります。

Okta AD エージェントでアカウントを同期

Okta を ID プロバイダーとして使用するには、まず、オンプレミス Active Directory と Okta を統合する必要があります。そのためには、ドメイン内に Okta AD エージェントをインストールし、Okta 組織に Active Directory を追加します。Okta Active Directory エージェントを展開するためのガイダンスについては、Okta Web サイトで「Get started with Active Directory integration（Active Directory の統合を開始する）」を参照してください。

その後、Active Directory ユーザーおよびグループを Okta にインポートします。インポート時には、Active Directory アカウントに関連付けられている以下の値を含めます：

- メール
- SID
- UPN
- OID

> 注：
>
> ワークスペースで Citrix Gateway サービスを使用している場合、Active Directory アカウントを Okta 組織と同期する必要はありません。

Active Directory ユーザーおよびグループを Okta 組織と同期するには：

1. Okta Active Directory エージェントをインストールして構成します。詳しい手順については、Okta Web サイトの次の記事を参照してください：
   - Install the Okta Active Directory agent（Okta Active Directory エージェントのインストール）
   - Configure Active Directory import and account settings（Active Directory のインポートとアカウント設定の構成）
   - Configure Active Directory provisioning settings（Active Directory プロビジョニング設定の構成）
2. 手動インポートまたは自動インポートを実行して、Active Directory ユーザーおよびグループを Okta に追加します。Okta のインポート方法と手順ついて詳しくは、Okta Web サイトで「Manage Active Directory users and groups（Active Directory ユーザーとグループの管理）」を参照してください。

Okta OIDC Web アプリケーション統合の作成

1. Okta 管理コンソールの［**Applications**］から［**Applications**］を選択します。
2. ［**Create App Integration**］を選択します。
3. ［**Sign in method**］で［**OIDC - OpenID Connect**］を選択します。
4. ［**Application Type**］で［**Web Application**］を選択します。［**Next**］を選択します。
5. ［**App Integration Name**］にアプリ統合のフレンドリ名を入力します。
6. ［**Grant type**］で、以下のオプションを選択します：

- Authorization Code（デフォルトで選択済み）
- Implicit（Hybrid）

7. [**Sign-in redirect URIs**]に「`https://accounts.citrixcloud.jp/core/login-okta`」を入力します。
8. [**Sign-out redirect URIs**］に、Citrix Cloud Japan からのワークスペース URL を入力します。
9. [**Assignments**］の ［**Controlled access**］で、アプリ統合を組織の全員に割り当てるか、指定したグループのみに割り当てるかか、または後からアクセスを割り当てるかを選択します。
10. [**Save**］を選択します。アプリ統合を保存すると、コンソールにアプリケーション構成ページが表示されます。
11. [**Client Credentials**] セクションで、[**Client ID**］と［**Client Secret**］の値をコピーします。Citrix Cloud Japan を Okta 組織に接続するときに、これらの値を使用します。

Okta OIDC Web アプリケーションの構成

この手順では、Citrix Cloud Japan に必要な設定で Okta OIDC Web アプリケーションを構成します。Citrix Cloud Japan では、ワークスペースへのサインイン時に Okta を介して利用者を認証するため、これらの設定が必要です。

1. （オプション）暗黙的な許可タイプのクライアント権限を更新します。この付与タイプに最小限の権限を許可する場合に、この手順の実行を選択できます。

   a) Okta アプリケーション構成ページの ［**General Settings**］で、[**Edit**］をクリックします。
   b) [**Application**］セクションの ［**Client acting on behalf of user**］で ［**Allow Access Token with implicit grant type**］をオフにします。
   c) [**Save**］を選択します。

2. アプリケーション属性を追加します。これらの属性では大文字と小文字が区別されます。

   a) Okta コンソールメニューから、[**Directory**］**>** ［**Profile Editor**］の順に選択します。
   b) Okta ［**User**］（デフォルト）プロファイルを選択します。Okta が ［**User**］プロファイルページを表示します。
   c) [**Attributes**］で、[**Add attribute**］を選択します。
   d) 次の情報を入力します:

      - Display Name：cip_email
      - Variable Name：cip_email
      - Description：Active Directory ユーザーセキュリティ識別子
      - Attribute Length：1 より大きい値
      - Attribute Required：Yes

   e) [**Save and Add Another**］を選択します。
   f) 次の情報を入力します:

      - Display Name：cip_sid
      - Variable Name：cip_sid

- Description：Active Directory ユーザーセキュリティ識別子
- Attribute Length：1 より大きい値
- Attribute Required：Yes

g) ［**Save and Add Another**］を選択します。

h) 次の情報を入力します：

- Display Name：cip_upn
- Variable Name：cip_upn
- Description：AD ユーザープリンシパル名
- Attribute Length：1 より大きい値
- Attribute Required：Yes

i) ［**Save and Add Another**］を選択します。

j) 次の情報を入力します：

- Display Name：cip_oid
- Variable Name：cip_oid
- Description：AD ユーザー GUID
- Attribute Length：1 より大きい値
- Attribute Required：Yes

k) ［**Save**］を選択します。

3. アプリケーションの属性マッピングの編集：

a) Okta コンソールから、［**Directory**］**>** ［**Profile Editor**］の順に選択します。

b) Active Directory の **active_directory** プロファイルを見つけます。このプロファイルは、「`myDomain User`」形式で表示される場合があります。ここで、<`myDomain`> は統合された Active Directory ドメインの名前です。

c) ［**Mappings**］を選択します。Active Directory ドメインのユーザープロファイルマッピングページが表示され、Active Directory を Okta ユーザーにマップするためのタブが選択されています。

d) ［**Okta User Profile**］列で、手順 2 で作成された属性を見つけて以下のようにマップします：

- `cip_email`の場合、ドメインの［User Profile］列から`email`を選択します。選択すると、マッピングには`appuser.email`が表示されます。
- `cip_sid`の場合、ドメインの［User Profile］列から`objectSid`を選択します。選択すると、マッピングには`appuser.objectSid`が表示されます。
- `cip_upn`の場合、ドメインの［User Profile］列から`userName`を選択します。選択すると、マッピングには`appuser.userName`が表示されます。
- `cip_oid`の場合、ドメインの［User Profile］列から`externalId`を選択します。選択すると、マッピングには`appuser.externalId`が表示されます。

e) ［**Save Mappings**］を選択します。

f) ［**Apply updates now**］を選択します。Okta は、マッピングを適用するジョブを開始します。

g) Okta を Active Directory と同期します。

i. Okta コンソールから ［**Directory**］**>** ［**Directory Integrations**］の順に選択します。

ii. 統合された Active Directory を選択します。
iii. ［**Provisioning**］タブを選択します。
iv. ［**Settings**］で ［**To Okta**］を選択します。
v. ［**Okta Attribute Mappings**］セクションまでスクロールして、［**Force Sync**］を選択します。

Okta API トークンの作成

1. 読み取り専用管理者アカウントを使用して、Okta コンソールにサインインします。
2. Okta コンソールメニューから、［**Security**］**>** ［**API**］の順に選択します。
3. ［**Tokens**］タブを選択してから、［**Create Token**］を選択します。
4. トークンの名前を入力します。
5. ［**Create Token**］を選択します。
6. トークン値をコピーします。Okta 組織の Citrix Cloud Japan への接続時に、この値を入力します。

Citrix Cloud Japan を **Okta** 組織に接続

1. Citrix Cloud Japan にサインインします（https://citrix.citrixcloud.jp）。
2. 管理コンソールの左上隅にある Citrix Cloud Japan メニューで、［**ID** およびアクセス管理］を選択します。
3. 「**Okta**」を見つけ、省略記号（…）メニューから ［接続］を選択します。
4. ［**Okta URL**］に Okta ドメインを入力します。
5. ［**Okta API** トークン］に、Okta 組織の API トークンを入力します。
6. ［クライアント **ID**］と ［クライアントシークレット］に、先ほど作成した OIDC Web アプリ統合からクライアント ID とシークレットを入力します。Okta コンソールからこれらの値をコピーするには、［アプリケーション］を選択し、Okta アプリケーションを見つけます。［クライアント資格情報］で、［クリップボードにコピー］ボタンを各値に対して使用します。
7. ［テストして終了］をクリックします。Citrix Cloud Japan で Okta の詳細が確認され、接続がテストされます。

ワークスペースの **Okta** 認証を有効にする

1. Citrix Cloud Japan メニューから ［ワークスペース構成］**>** ［認証］の順に選択します。
2. ［**Okta**］を選択します。プロンプトが表示されたら、［利用者のエクスペリエンスに与える影響を了承しています。］を選択します。
3. ［承諾］をクリックして権限の要求を承諾します。

SAML を ID プロバイダーとして Citrix Cloud Japan に接続する

March 1, 2024

Citrix Cloud Japan では、ワークスペースにサインインする管理者（プレビュー）および利用者を認証するための ID プロバイダーとして、SAML（セキュリティアサーションマークアップランゲージ）を使用できます。オンプレミスの Active Directory（AD）で、選択した SAML 2.0 プロバイダーを使用できます。

ほとんどの SAML プロバイダーの場合、この記事の情報を使用して SAML 認証を設定します。Azure AD で SAML 認証を使用する場合は、Azure AD アプリギャラリーから Citrix Cloud Japan SAML SSO アプリを使用することを許可できます。Citrix Cloud Japan SAML SSO アプリを使用した Citrix Cloud Japan での SAML 認証の設定方法について詳しくは、Azure AD アプリドキュメント Web サイトの「チュートリアル：Azure Active Directory シングルサインオン（SSO）と Citrix Cloud SAML SSO の統合」を参照してください。

前提条件

Citrix Cloud Japan で SAML 認証を使用する場合、次の要件があります：

- SAML 2.0 をサポートする SAML プロバイダー
- オンプレミスの AD ドメイン
- リソースの場所に展開され、オンプレミスの AD ドメインに参加している 2 つの Cloud Connector。Cloud Connector は、Citrix Cloud Japan がリソースの場所と通信するために使用されます。
- SAML プロバイダーとの AD 統合。

Cloud Connector

Citrix Cloud Connector ソフトウェアのインストール先となるサーバーが少なくとも 2 台必要です。Cloud Connector の可用性を高めるため、サーバーは 2 台以上用意することを Citrix ではお勧めします。これらのサーバーは、次の要件を満たしている必要があります：

- 「Citrix Cloud Connector の要件」に記載されているシステム要件を満たしている。
- 他の Citrix コンポーネントはインストールされておらず、AD ドメインコントローラーではなく、リソースの場所のインフラストラクチャに不可欠なマシンでもない。
- リソースが存在するドメインに参加している。ユーザーが複数のドメインにあるリソースにアクセスする場合は、各ドメインに Citrix Cloud を少なくとも 2 つインストールする必要がある。
- 利用者が Citrix Workspace を介してアクセスするリソースにアクセスできるネットワークに接続済み。
- インターネットに接続済み。詳しくは、「接続要件」を参照してください。

Cloud Connector のインストール手順について詳しくは、「タスク 3：Cloud Connector のインストール」を参照してください。

Active Directory

SAML 認証を構成する前に、次のタスクを実行します:

- ワークスペース利用者に Active Directory（AD）のユーザーアカウントがあることを確認します。SAML 認証が構成されている場合、AD アカウントがない利用者はワークスペースにサインインできません。
- 利用者の AD アカウントのユーザープロパティが入力されていることを確認します。Citrix Cloud Japan では、利用者が Citrix Workspace にサインインする際、ユーザーコンテキストを決定するためにこれらのプロパティが必要とされます。これらのプロパティが入力されていないと、利用者がサインインできません。これらのプロパティには以下が含まれます:
  - メールアドレス
  - 表示名（オプション）
  - 共通名
  - SAM アカウント名
  - ユーザープリンシパル名
  - オブジェクト GUID
  - SID
- Cloud Connector を展開して、オンプレミスの Active Directory（AD）と Citrix Cloud Japan アカウントの間で接続を確立します。
- AD ユーザーを SAML プロバイダーに同期します。Citrix Cloud Japan では、サインインするワークスペース利用者の AD ユーザー属性が必要とされます。

Active Directory との **SAML** 統合

SAML 認証を有効にする前に、オンプレミスの AD を SAML プロバイダーと統合する必要があります。この統合により、SAML プロバイダーは SAML アサーションで次の必要な AD ユーザー属性を Citrix Cloud Japan に渡すことができます:

- SecurityIDentifier（SID）
- objectGUID（OID）
- userPrincipalName（UPN）
- メール（email）

正確な統合手順は SAML プロバイダーによって異なりますが、通常統合プロセスには、次のタスクが含まれます:

1. AD ドメインに同期エージェントをインストールして、ドメインと SAML プロバイダー間の接続を確立します。
2. 前述の AD ユーザー属性に対応するカスタム属性が使用できない場合は、カスタム属性を生成し、Active Directory（AD）に関連付けます。このタスクの一般的な手順は、この記事の「カスタム SAML 属性の作成およびマッピング」で説明されています。
3. AD ユーザーを SAML プロバイダーに同期します。

> 注:
>
> 表示された AD ユーザー属性にマッピングするカスタム属性を既に作成している場合は、それ以上の作成やマッピングは必要ありません。代わりに、Citrix Cloud Japan で SAML プロバイダーからメタデータを構成するときに、既存のカスタム属性を使用してください。

AD と SAML プロバイダーの統合について詳しくは、SAML プロバイダーの製品ドキュメントを参照してください。

SAML 2.0 による管理者認証

> 注:
>
> Citrix Cloud Japan 管理者向けの SAML 認証は、Technical Preview 段階です。プレビュー機能を非実稼働環境でのみ使用することを Citrix ではお勧めします。

AD グループ

AD グループのみを使用して Citrix Cloud Japan に管理者を追加できます。SAML 認証を使用して個別の管理者を追加することはできません。

サインイン **URL**

SAML 認証を構成するときは、管理者が Citrix Cloud Japan へのサインインに使用できるサインイン URL を構成します。この URL には`https://citrix.citrixcloud.jp/go/myorganization`形式を使用します。ここで、「myorganization」は組織用に選択する一意の識別子です。

AD グループを追加すると、そのグループの管理者は、指定したサインイン URL を使用してすぐに Citrix Cloud Japan にサインインできます。Citrix は、Citrix Cloud Japan にアクセスできることを管理者に通知で知らせることはありません。

サポートされている権限

カスタムアクセス権限のみがサポートされています。AD グループを追加するときは、グループ内の管理者に付与する権限を選択する必要があります。フルアクセス権限はサポートされていません。

タスクの概要

SAML 認証を設定するには、次のタスクを実行します:

1. [**ID** およびアクセス管理] で、「Active Directory を Citrix Cloud Japan に接続する」の説明に従って、オンプレミスの AD を Citrix Cloud Japan に接続します。
2. 本記事の「Active Directory との SAML 統合」で説明されているように、SAML プロバイダーをオンプレミスの AD と統合します。
3. [**ID** およびアクセス管理] で、Citrix Cloud Japan での SAML 認証を構成します。Citrix Cloud Japan のメタデータを使用して SAML プロバイダーを構成してから、SAML プロバイダーからのメタデータを使用して Citrix Cloud Japan を構成して SAML 接続を確立します。
4. SAML を使用して管理者を認証する場合:

   a) 管理者が Citrix Cloud Japan へのサインインに使用できるサインイン URL を構成します。
   b) 所属する AD グループを指定して、Citrix Cloud Japan に管理者を追加します。

5. SAML を使用してワークスペース利用者を認証する場合は、[ワークスペース構成] で **SAML** 認証方法を有効にします。SAML を Citrix Cloud 管理者の認証にのみ使用している場合、このタスクを実行する必要はありません。

カスタム **SAML** 属性の作成およびマッピング

SAML プロバイダーで SID、UPN、OID、およびメール属性のカスタム属性を既に構成している場合は、このタスクを実行する必要はありません。「SAML コネクタアプリケーションの作成」に進み、手順 8 の既存のカスタム SAML 属性を使用します。

> 注:
>
> このセクションの手順では、SAML プロバイダーの管理コンソールで実行するアクションについて説明します。これらのアクションを実行するために使用する特定のコマンドは、選択した SAML プロバイダーによっては、このセクションで説明するコマンドとは異なる場合があります。このセクションの SAML プロバイダーコマンドは、例としてのみ提供されています。SAML プロバイダーに固有の関連コマンドの詳細については、SAML プロバイダーのドキュメントを参照してください。

1. SAML プロバイダーの管理コンソールにサインインし、カスタムユーザー属性を作成するためのオプションを選択します。たとえば、SAML プロバイダーのコンソールによっては、[**Users**] **>** [**Custom User Fields**] **>** [**New User Field**] を選択します。
2. 次の属性を追加します:

   - cip_sid
   - cip_upn
   - cip_oid
   - cip_email

3. Citrix Cloud Japan に接続した AD を選択します。たとえば、SAML プロバイダーのコンソールによっては、[**Users**] **>** [**Directories**] を選択します。

4. ディレクトリ属性を追加するためのオプションを選択します。たとえば、SAML プロバイダーのコンソールによっては、[**Directory Attributes**] を選択します。
5. 属性を追加するためのオプションを選択し、次の AD 属性を手順 2 で作成したカスタムユーザー属性にマップします:

   - `objectSid`を選択し、`cip_sid`属性にマップします。
   - `userPrincipalName`を選択し、`cip_upn`属性にマップします。
   - `ObjectGUID`を選択し、`cip_oid`属性にマップします。
   - `mail`を選択し、`cip_email`属性にマップします。

管理者のサインイン **URL** の構成

1. Citrix Cloud にサインインします（https://citrix.citrixcloud.jp）。
2. Citrix Cloud メニューで、[**ID** およびアクセス管理] を選択します。
3. [**SAML 2.0**] を見つけ、省略記号メニューから [接続] を選択します。
4. 入力画面が表示されたら、URL に適した短い会社の識別子を入力し、[保存して続行] を選択します。[**SAML** の構成] ページが表示されます。
5. 次のセクションに進み、Citrix Cloud への SAML 接続を構成します。

SAML プロバイダーのメタデータの構成

このタスクでは、Citrix Cloud Japan の SAML メタデータを使用してコネクタアプリケーションを作成します。SAML アプリケーションを構成した後、SAML メタデータを使用して、コネクタアプリケーションから Citrix Cloud Japan への SAML 接続を構成します。

> 注:
>
> このセクションのいくつかの手順では、SAML プロバイダーの管理コンソールで実行するアクションについて説明します。これらのアクションを実行するために使用する特定のコマンドは、選択した SAML プロバイダーによっては、このセクションで説明するコマンドとは異なる場合があります。このセクションの SAML プロバイダーコマンドは、例としてのみ提供されています。SAML プロバイダーに固有の関連コマンドの詳細については、SAML プロバイダーのドキュメントを参照してください。

SAML コネクタアプリケーションの作成

1. SAML プロバイダーの管理コンソールから、属性付き、署名応答付き ID プロバイダーのアプリケーションを追加します。たとえば、プロバイダーのコンソールによっては、[**Applications**] > [**Applications**] > [**Add App**] を選択して [**SAML Test Connector (IdP w/ attr w/ sign response)**] を選択します。
2. 必要に応じて、表示名を入力してアプリを保存します。

3. Citrix Cloud Japan の ［**SAML** の構成］画面の ［**SAML** メタデータ］で ［ダウンロード］を選択します。メタデータ XML ファイルが別のブラウザータブに表示されます。

   > 注:
   >
   > 必要に応じて、`https://saml.citrixcloud.jp/saml/metadata.xml`からこのファイルをダウンロードすることもできます。このエンドポイントは、一部の ID プロバイダーにとって、SAML プロバイダーのメタデータをインポートおよび監視するときにより適している場合があります。

4. コネクタアプリケーションについて、次の詳細を入力します:

   - **Audience** フィールドに、`https://saml.citrixcloud.jp`と入力します。
   - **Recipient** フィールドに、`https://saml.citrixcloud.jp/saml/acs`を入力します。
   - ACS URL 検証のフィールドに、`https://saml.citrixcloud.jp/saml/acs`を入力します。
   - ACS URL のフィールドに、`https://saml.citrixcloud.jp/saml/acs`を入力します。

5. カスタム SAML 属性をアプリケーションのパラメーター値として追加します。

このフィールドを作成	このカスタム属性を割り当て
cip_sid	cip_sid または既存の SID 属性
cip_upn	cip_upn または既存の UPN 属性
cip_oid	cip_oid または既存の OID 属性
cip_email	cip_email または既存のメール属性

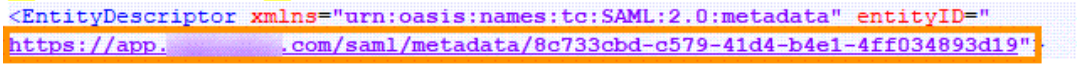
6. ワークスペース利用者をユーザーとして追加して、アプリケーションへのアクセスを許可します。

SAML プロバイダーのメタデータを **Citrix Cloud Japan** に追加

1. SAML プロバイダーから SAML メタデータを取得します。次の画像は、このファイルがどのように見えるかの例です:

2. Citrix Cloud Japan の［**SAML** の構成］画面で、SAML プロバイダーのメタデータファイルから次の値を入力します:

   - ［エンティティ **ID**］で、メタデータの **EntityDescriptor** 要素から **entityID** の値を入力します。

   - ［認証要求に署名する］で ［はい］を選択して Citrix Cloud Japan が認証要求に署名できるようにして、Citrix Cloud Japan によるものであり、悪意のあるアクターによるものではないことを保証します。安全な SAML 応答のために SAML プロバイダーが使用する許可リストに Citrix ACS URL を追加する場合は、［いいえ］を選択します。

   - ［**SSO** サービス **URL**］で、使用するバインドメカニズムの URL を入力します。HTTP-POST または HTTP-Redirect バインドのいずれかを使用できます。メタデータファイルで、**HTTP-POST** または **HTTP-Redirect** のいずれかのバインド値を持つ **SingleSignOnService** 要素を見つけます。

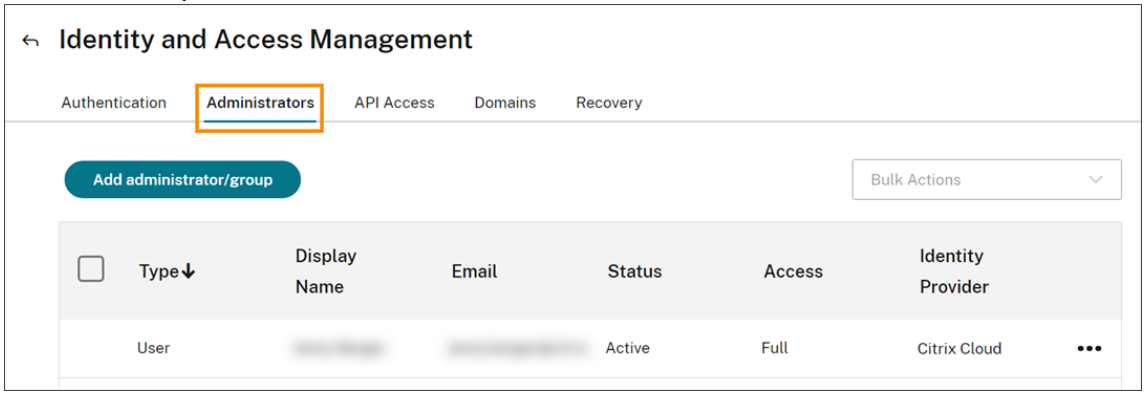
   - ［バインドメカニズム］で、メタデータファイルから選択した SSO サービス URL のバインドに一致するメカニズムを選択します。

- ［**SAML** 応答］で、SAML プロバイダーが SAML 応答と SAML アサーションに使用する署名方法を選択します。デフォルトでは、Citrix Cloud Japan はこのフィールドで指定されたとおりに署名されていない応答を拒否します。

3. SAML プロバイダーの管理コンソールで、次のアクションを実行します:
   - SAML 署名アルゴリズムに **SHA-256** を選択します。
   - X.509 証明書を PEM ファイルとしてダウンロードします。
4. Citrix Cloud Japan の ［**SAML** の構成］画面で、［ファイルのアップロード］を選択し、前の手順でダウンロードした PEM ファイルを選択します。
5. ［続行］を選択してアップロードを完了します。
6. ［認証コンテキスト］で、使用するコンテキストと Citrix Cloud Japan がコンテキストを適用する厳格さのレベルを選択します。選択したコンテキストで認証を強制せずに、そのコンテキストで認証を要求するには、［最小］を選択します。選択したコンテキストで認証を要求し、そのコンテキストでのみ認証を強制するには、［完全一致］を選択します。SAML プロバイダーが認証コンテキストをサポートしていない場合、または認証コンテキストを使用しないことを選択した場合は、［未指定］および ［最小］を選択します。
7. ［ログアウト **URL**］で、SAML プロバイダーのメタデータファイルから HTTP-Redirect バインディングを使用した **SingleSignOnService** 要素を見つけ、URL を入力します。ログアウト URL を省略することを選択した場合、Citrix Cloud Japan は ID プロバイダーにログオフ要求を送信しません。代わりに、Citrix Cloud Japan はワークスペース URL にリダイレクトします。Citrix Cloud Japan は、シングルログアウト（SLO）または署名されたログアウト要求の送信をサポートしていません。
8. Citrix Cloud Japan の次のデフォルトの名前属性値が、SAML プロバイダーの管理コンソールの対応する属性値と一致することを確認します。SAML プロバイダーの値が異なる場合は、Citrix Cloud Japan でこれらの値を変更して、SAML プロバイダーと一致させることができます。
   - ユーザーの表示名の属性名: `displayName`
   - ユーザーの名の属性名: `givenName`
   - ユーザーの姓の属性名: `familyName`
9. Citrix Cloud Japan で、SAML プロバイダーからのカスタム SAML 属性を入力します。
   - ［セキュリティ識別子（**SID**）の属性名］に、カスタム SID 属性名を入力します。デフォルトの値は`cip_sid`です。
   - ［ユーザープリンシパル名（**UPN**）の属性名］に、カスタム UPN 属性名を入力します。デフォルトの値は`cip_upn`です。
   - ［メールの属性名］では、カスタムメール属性名を入力します。デフォルトの値は`cip_email`です。
   - ［**AD** オブジェクト識別子（**OID**）の属性名］に、カスタム OID 属性名を入力します。デフォルトの値は`cip_oid`です。
10. ［テストして終了］を選択して、正常に接続を構成したことを確認します。

AD から Citrix Cloud Japan に管理者を追加する

1. Citrix Cloud Japan の ［**ID** およびアクセス管理］ページで ［管理者］を選択します。



2. ［管理者の詳細］で、［**Active Directory**］を選択し、使用するドメインを選択します。
3. ［追加するグループを検索する］で、検索ボックスに追加するグループの名前を入力し始めます。表示されたら、プラス記号（+）をクリックしてグループを選択します。
4. ［次へ］を選択します。
5. グループに割り当てるカスタムアクセス権限または役割を選択します。［次へ］を選択します。
6. 管理者の詳細を確認します。変更するには、［戻る］を選択します。
7. 完了したら、［保存］を選択します。

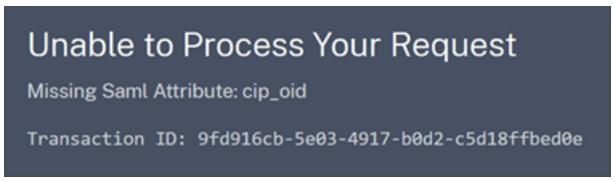
ワークスペースの SAML 認証を有効にする

1. Citrix Cloud Japan メニューから、［ワークスペース構成］を選択します。
2. ［認証］タブを選択します。
3. ［**SAML 2.0**］を選択します。

トラブルシューティング

属性エラー

SAML 構成で必要な属性が正しくエンコードされていない場合、属性エラーが発生することがあります。属性エラーが発生すると、Citrix Cloud Japan は問題のある属性について説明したエラーメッセージを表示します。



この種類のエラーを解決するには、これらの属性が以下の表の説明に従ってエンコードされていることを確認してください。

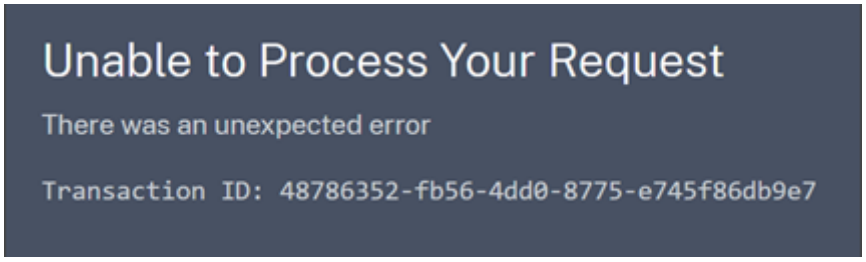
属性	エンコーディング
cip_email	文字列形式である必要があります（user@domain）
cip_oid	Base64 または文字列形式である必要があります
cip_sid	Base64 または文字列形式である必要があります
cip_upn	文字列形式である必要があります（user@domain）

予期しないエラー

次の場合、Citrix Cloud Japan で予期しないエラーが発生することがあります:

- ユーザーが、IDP 開始のフローを使用して、SAML 要求を開始する。たとえば、ワークスペース URL に直接アクセスするのではなく、ID プロバイダーのアプリポータル（customer.citrixcloud.jp）からタイルを選択することによって、要求が開始される場合。
- SAML 証明書が無効であるか、有効期限が切れている。
- 認証コンテキストが無効である。
- SAML アサーションと応答署名が一致していない。

このエラーが発生すると、Citrix Cloud Japan は一般的なエラーメッセージを表示します。



ID プロバイダーのアプリポータルを介して Citrix Cloud Japan に移動した結果としてこのエラーが発生した場合は、次の回避策が考えられます:

1. ワークスペース URL（https://customer.citrixcloud.jpなど）を参照するブックマークアプリを、ID プロバイダーのアプリポータルに作成します。
2. SAML アプリとブックマークアプリの両方にユーザーを割り当てます。
3. アプリポータルの表示設定を変更して、SAML アプリを非表示にし、ブックマークアプリを表示します。
4. Prompt=Login パラメーターを無効にして、余分なパスワードプロンプトを削除します。

Citrix Cloud Japan 用のライセンス

November 21, 2023

Citrix Cloud Japan では、特定のクラウドサービスのライセンスと使用状況を監視できます。Citrix ライセンスサーバーが Citrix Cloud Japan に登録されているオンプレミス環境でも、ライセンスと使用状況を監視できます。

Citrix Cloud Japan のライセンスと使用状況の監視およびライセンスサーバー登録に関するすべての機能は、Citrix Cloud と同じように機能します。

クラウドサービスのライセンス

法人顧客は、Citrix Cloud Japan メニューの ［ライセンス］を選択することで、サポートされているクラウドサービスのライセンス割り当てと使用状況を監視できます。

現在、ライセンスと使用状況の監視は **Citrix DaaS** でのみ利用できます。詳しくは、Citrix Cloud ドキュメントの次の記事を参照してください。

- Citrix DaaS のライセンスおよびアクティブな使用状況の監視（ユーザー/デバイス）
- Citrix DaaS のライセンスとピーク時の使用状況の監視（同時使用）

オンプレミス環境用のライセンス

オンプレミス環境で Citrix Virtual Apps and Desktops を使用している法人顧客は、Citrix Cloud Japan を使用して、ユーザー/デバイスモデルと同時使用ライセンスモデルの両方のライセンスと使用状況を常に監視できます。Citrix ライセンスサーバーを Citrix Cloud Japan に登録することにより、顧客は［ライセンス割り当て済みの展開］ページで次のタスクを実行できます:

- 登録済みライセンスサーバーのレポートステータスを監視する
- ユーザー/デバイスライセンスモデルを使用する環境のライセンス割り当てと使用状況を表示する
- 同時使用ライセンスモデルを使用する環境のピーク時のライセンス使用状況を表示する

オンプレミス Virtual Apps and Desktops 環境のライセンスおよび使用状況の監視について詳しくは、Citrix Cloud ドキュメントの「オンプレミス展開のライセンスと使用状況の監視」を参照してください。

Citrix Service Provider 用のライセンス

Citrix Service Provider（CSP）では、次のツールを使用することで、製品ライセンスと使用状況を把握し、レポートを作成することができます:

- License Usage Insights は、シングルテナントおよびマルチテナントの顧客間で製品の使用状況情報を収集および集約する Citrix Cloud の無料サービスです。詳しくは、Citrix Cloud ドキュメントの「Citrix Service Provider 用のライセンス」を参照してください。
- Citrix Cloud のライセンス機能により、CSP の顧客は、Citrix DaaS（旧称 Citrix Virtual Apps and Desktops サービス）のライセンスと使用状況を監視できます。CSP は、顧客の Citrix Cloud アカウントでサインインして、この情報を表示およびエクスポートすることもできます。詳しくは、Citrix Cloud ドキュメントの「Citrix DaaS の顧客のライセンスと使用状況の監視」を参照してください。

Citrix Cloud Japan の管理

November 21, 2023

Citrix Cloud Japan には、次の管理機能が含まれています:

- 管理者を招待し、クラウドサービスへのアクセスを委任する
- ライブラリのサービスオファリングにユーザーを割り当てる
- サービス通知を監視する
- Citrix Cloud Japan で発生したイベントのシステムログを表示する

管理者

管理者は、ID を使用して Citrix Cloud Japan にアクセスし、管理アクティビティを実行し、Citrix Cloud Connector をインストールします。

Citrix の ID メカニズムは、メールとパスワードを使用して管理者を認証します。My Citrix 資格情報を使用して Citrix Cloud Japan にサインインすることもできます。

新しい管理者を追加する

アカウントの登録処理で、最初の管理者が作成されます。この管理者が、Citrix Cloud Japan に参加する他の管理者を招待できます。これらの新しい管理者は、既存の Citrix Cloud Japan アカウント資格情報を使用するか、必要に応じて新しいアカウントをセットアップすることができます。招待する管理者のアクセス権限を微調整することもできます。これにより、組織内の管理者の役割に合わせたアクセスを定義できます。

他の管理者を招待して Citrix Cloud Japan へのアクセスを微調整する方法については、「Citrix Cloud Japan アカウントに管理者を追加する」を参照してください。

パスワードを変更する

Citrix Cloud Japan 内からパスワードを変更する場合は、［アカウント設定］に移動して ［マイプロファイル］を選択します。［パスワードの変更］をクリックして現在のパスワードを入力し、新しいパスワードを確認します。

管理者を削除する

［管理者］タブで Citrix Cloud Japan アカウントから管理者を削除できます。管理者を削除すると、Citrix Cloud Japan にサインインできなくなります。アカウントが削除された時に管理者がログインしている場合、最大 1 分間、管理者はアクティブな状態のままでいられます。その後、Citrix Cloud Japan へのアクセスは拒否されます。

> 注:
>
> - アカウントに管理者が 1 人しかいない場合、その管理者を削除することはできません。Citrix Cloud Japan には、顧客アカウントごとに少なくとも 1 人の管理者が必要です。
> - Cloud Connector は管理者アカウントに関連付けられていません。Connector をインストールした管理者が顧客アカウントから削除されても、Connector は動作を続けます。

利用者

利用者の ID は、どの利用者が Citrix Cloud Japan 経由でサービスにアクセスできるかを定義します。この ID は、リソースの場所内のドメインから指定された Active Directory ドメインアカウントによって提供されます。ライブラリのオファリングに利用者を割り当てると、利用者はそのオファリングにアクセスできます。

> 重要:
>
> Citrix DaaS（旧称 Virtual Apps and Desktops サービス）でオンプレミスの StoreFront を使用している場合は、デリバリーグループを作成するときにライブラリを使用してリソースを割り当てないでください。代わりに、Studio を使用してリソースをユーザーに割り当てます。このシナリオでライブラリを使用する場合、リソースがユーザーに表示されない可能性があります。
>
> Studio でデリバリーグループを作成する場合、［ユーザー］ページで、［ユーザー管理を **Citrix Cloud** に任せます］を選択しないでください。代わりに、別のオプションを選択します（[任意の認証ユーザーによるこのデリバリーグループの使用を許可します］または ［次のユーザーに対するこのデリバリーグループの使用を制限します］を選択します）。

管理者は、これらの ID を提供するために使用するドメインを［ドメイン］タブで制御できます。複数のフォレストでドメインを使用する場合、各フォレストに最低 2 つの Cloud Connector をインストールします。高可用性環境を維持するために少なくとも 2 つの Cloud Connector のインストールを Citrix ではお勧めします。

ユーザーをライブラリオファリングに割り当てるプロセスは、Citrix Cloud Japan でも Citrix Cloud（citrix.cloud.com）でも同じです。手順については、「ライブラリを使用してサービスオファリングにユーザーとグループを割り当てる」を参照してください。

> 注:
>
> - ドメインを無効にすると、新しい ID のみが選択されなくなります。利用者は既に割り当てられている ID を使用することはできます。
> - 注：各 Cloud Connector がインストールされた単一のフォレストからすべてのドメインを表示し、使用できます。

利用者の使用状況を管理する

個別のアカウントまたは Active Directory グループを使用して、オファリングに利用者を追加します。グループをオファリングに割り当てた後、Active Directory グループを使用すると Citrix Cloud Japan 経由で管理する必要

はありません。

管理者がオファリングから利用者または利用者グループを削除すると、利用者はサービスにアクセスできなくなります。特定のサービスから利用者を削除する方法について詳しくは、Citrix 製品ドキュメントWeb サイトで該当サービスのドキュメントを参照してください。

プライマリのリソースの場所

プライマリのリソースの場所は、ドメインと Citrix Cloud Japan 間の通信に「最も優先される」と指定するリソースの場所です。「プライマリ」として選択したリソースの場所には、ドメインに対するパフォーマンスや接続性が最も優れた Cloud Connector が必要です。これにより、ユーザーは Citrix Cloud Japan にすばやくログオンできます。

プライマリのリソースの場所を選択するプロセスは、Citrix Cloud Japan でも Citrix Cloud（citrix.cloud.com）でも同じです。詳しくは、「プライマリのリソースの場所の選択」を参照してください。

通知

通知は、Citrix Cloud Japan の新機能やリソースの場所内のマシンに関する問題など、管理者が関心がある問題またはイベントに関する情報を提供します。通知は Citrix Cloud Japan のすべてのサービスで使用できます。

通知の管理は、Citrix Cloud Japan と Citrix Cloud（citrix.cloud.com）で同じプロセスを使用します。通知について詳しくは、「通知」を参照してください。

システムログ

システムログには、Citrix Cloud Japan で発生したイベントがタイムスタンプ付きで一覧表示されます。これらの変更を CSV ファイルとしてエクスポートして、組織の規制遵守要件を満たしたり、セキュリティ分析をサポートしたりすることができます。

Citrix Cloud Japan のシステムログ機能は、Citrix Cloud（citrix.cloud.com）と同じですが、いくつかの重要な制限があります。詳しくは、「システムログ」を参照してください。

Citrix Cloud Japan 管理者を管理する

December 20, 2023

Citrix Cloud Japan コンソールで管理者を管理します。管理者の認証に使用する ID プロバイダーに応じて、管理者を個別に追加することも、グループを使用して追加することもできます。

デフォルトでは、新しい管理者には Citrix Cloud Japan アカウント内のすべての機能へのフルアクセス権限があります。アカウント管理を委任する方法については、このページの「管理者権限を構成する」を参照してください。

新しい管理者を追加する

Citrix Cloud Japan は、管理者の認証で次の ID プロバイダーをサポートしています:

- Citrix ID プロバイダー: Citrix Cloud のデフォルトの ID プロバイダー。個別の管理者の追加のみをサポートします。
- Azure AD: 個別の、または Azure AD グループを使用しての管理者の追加をサポートします。Azure AD グループの管理者のアクセスは、Citrix DaaS のみに限定されています。詳しくは、「管理者グループを管理する」を参照してください。
- SAML 2.0: AD グループによる管理者の追加のみをサポートします。AD グループの管理者のアクセスは、Citrix DaaS の管理のみに限定されています。詳しくは、「SAML を ID プロバイダーとして Citrix Cloud Japan に接続する」を参照してください。

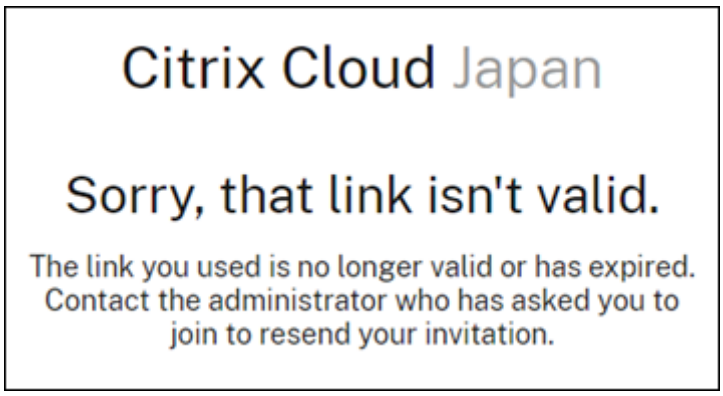
新しい管理者を追加するには、次のワークフローを使用します:

1. 管理者の認証に使用する ID プロバイダーを選択します。
2. ID プロバイダーに応じて、個別の管理者を招待するか、管理者が属するグループを選択します。
3. 組織内の管理者の役割に応じたアクセス権限を指定します。詳しくは、この記事の「管理者権限を構成する」を参照してください。

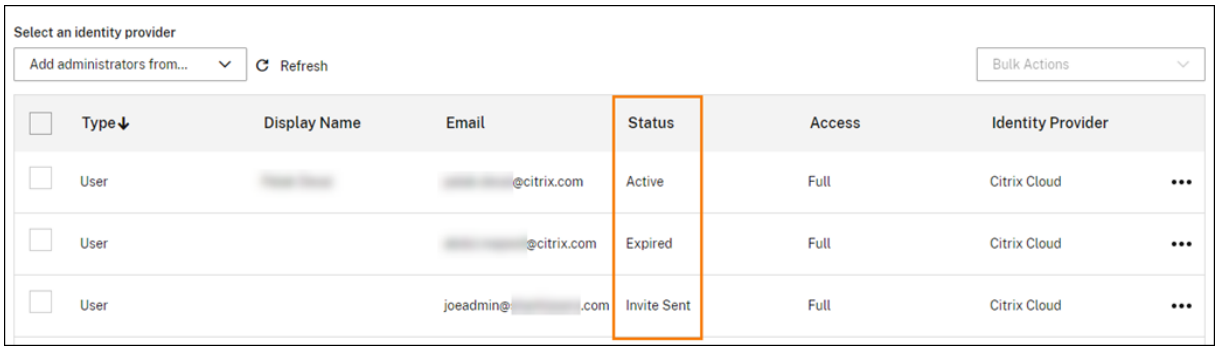
個別の管理者を招待する

個別の管理者を追加するには、Citrix Cloud Japan アカウントに参加するよう招待します。管理者を追加すると、Citrix から相手に招待メールが送信されます。管理者は、サインインする前に招待を承諾する必要があります。グループを通じて追加した管理者には招待は送信されず、追加後すぐにサインインできます。

`cloud@citrix.com`から送信された招待メールには、アカウントへのアクセス方法が記載されています。メールは送信日から 5 日間有効です。5 日が経過すると、招待リンクの有効期限が切れます。招待された管理者が期限切れのリンクを使用した場合、リンクが無効であることを知らせるメッセージが Citrix Cloud Japan で表示されます。



Citrix Cloud Japan には招待メールのステータスも表示されるため、管理者が招待メールを受け入れて Citrix Cloud にサインインしたかどうかを確認できます。

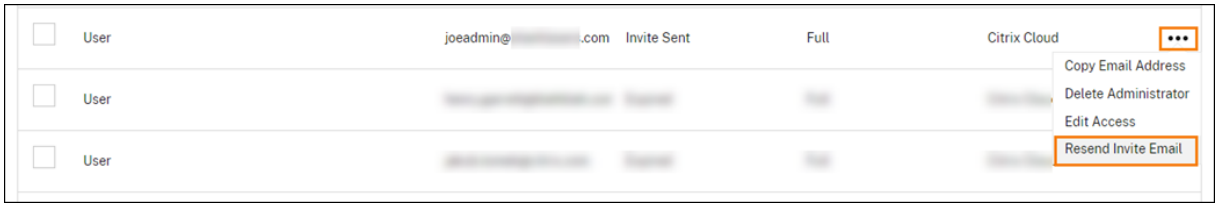


管理者を招待するには

1. Citrix Cloud Japanにサインイン後、メニューで ［**ID** およびアクセス管理］を選択します。
2. ［**ID** およびアクセス管理］ページで ［管理者］を選択します。コンソールに、アカウント内の現在の管理者全員が表示されます。
3. ［管理者/グループを追加する］を選択します。
4. ［管理者の詳細］で、使用する ID プロバイダーを選択します。Azure AD を使用している場合、最初にサインインするように求めるメッセージが Citrix Cloud Japan に表示されることがあります。
5. **Citrix ID** を選択した場合は、ユーザーのメールアドレスを入力して ［次へ］をクリックします。
6. **Azure AD** を選択した場合は、追加するユーザーの名前を入力して ［次へ］をクリックします。Azure AD ゲストユーザーの招待はサポートされていません。
7. ［アクセスの設定］で、管理者に適切な権限を設定します。フルアクセス（デフォルトで選択）では、すべての Citrix Cloud Japan 機能とサブスクライブ済みサービスを制御できます。カスタムアクセスでは、選択した機能とサービスを制御できます。
8. 管理者の詳細を確認します。変更するには、［戻る］を選択します。
9. ［招待を送信］を選択します。Citrix Cloud Japan は、指定されたメールアドレスに招待メールを送信し、管理者を一覧に追加します。

招待メールを再送信する

招待メールを再送信するには、コンソールの右端にある省略記号（…）メニューから ［招待メールの再送信］を選択します。招待メールを再送信しても、招待メールの有効期限が切れるまでの 5 日間の制限に変更はありません。



新しいサインインリンクを含む招待メールを再送信する

元の招待メールの有効期限が切れており、新しいメールを管理者に送信する場合は、Citrix Cloud Japan から管理者を削除してから、再度招待してください。

管理者の招待を受け入れる

Citrix Cloud Japan アカウントに招待された場合、Citrix Cloud Japan からアカウントの組織 ID と顧客名が記載されたメールが送信されます。

招待を受け入れるには、［サインイン］をクリックします。その後、ブラウザーウィンドウが開きます。Citrix アカウントをまだお持ちでない場合は、ブラウザーにパスワード作成ページが表示されます。既にアカウントをお持ちの場合は、Citrix Cloud Japan は既存のパスワードを使用してサインインするように要求します。

管理者グループを追加する

AD グループ（SAML 認証用）または Azure AD グループ（Azure AD 認証用）を使用して管理者を追加できます。詳しくは、次の記事を参照してください:

- 管理者グループを管理する
- SAML を ID プロバイダーとして Citrix Cloud Japan に接続する

管理者権限を構成する

管理者を Citrix Cloud Japan アカウントに追加するときは、次のような異なるレベルのアクセス権を割り当てる必要があります:

- Citrix DaaS に関するヘルプデスクへのアクセス
- 1 つまたは複数の特定のクラウドサービスを管理するためのアクセス
- ライブラリやリソースの場所など、特定の Citrix Cloud Japan 機能を管理するためのアクセス

委任管理により、組織内の役割に応じて管理者に必要となる、すべてのアクセス権限を構成できます。

コンソールの権限

Citrix Cloud Japan 管理コンソールへのカスタムアクセスを構成するには、次の権限を使用します:

- 顧客ダッシュボード（表示のみ）: Citrix Service Provider（CSP）のみ。顧客ダッシュボードへの表示アクセスを許可します。
- ドメイン:［**ID** およびアクセス管理］**>**［ドメイン］タブへのアクセスが許可されます。管理者は、このタブから Citrix Cloud Connector ソフトウェアをダウンロードし、ドメイン内のサーバーにインストールすることで、Active Directory ドメインを追加できます。
- ライブラリ:［ライブラリ］コンソールページへのアクセスが許可されます。
- ライセンス:［ライセンス］コンソールページの ［クラウドサービス］タブおよび ［ライセンス割り当て済みの展開］タブへのアクセスが許可されます。
- 通知:［通知］コンソールページへのアクセスが許可されます。管理者は Citrix Cloud の通知を表示したり閉じたりできます。
- リソースの場所:［リソースの場所］コンソールページへのアクセスが許可されます。管理者は、新しいリソースの場所を追加したり、Citrix Workspace のシングルサインオン用の FAS サーバーを追加したりできます。また、コネクタを追加したり、コネクタの更新を管理したりすることもできます。
- セキュアクライアント:［**ID** およびアクセス管理］**>**［**API** アクセス］**>**［セキュアクライアント］タブへのアクセスが許可されます。管理者は、Citrix Cloud APIで使用する独自のセキュアクライアントを作成および管理できます。この権限には、［**ID** およびアクセス管理］**>**［**API** アクセス］**>**［製品の登録］タブへのアクセスは含まれません。［製品の登録］タブにアクセスできるのはフルアクセス管理者のみです。詳しくは、Citrix Cloud 製品ドキュメントの「オンプレミス展開のライセンスと使用状況の監視」を参照してください。
- システムログ:［システムログ］コンソールページへのアクセスが許可されます。管理者は、システムログイベントを表示したり、イベントを CSV ファイルにエクスポートしたりできます。
- ワークスペース構成:［ワークスペース構成］コンソールページへのアクセスが許可されます。管理者は、認証方法の変更、ワークスペースの外観と動作のカスタマイズ、サービスの有効化と無効化、サイトアグリゲーションの構成を行うことができます。詳しくは、Citrix Workspaceの製品ドキュメントを参照してください。

既存の権限を変更するには

他の管理者のアクセス権限を定義できるのは、フルアクセス権限を持つ Citrix 管理者だけです。

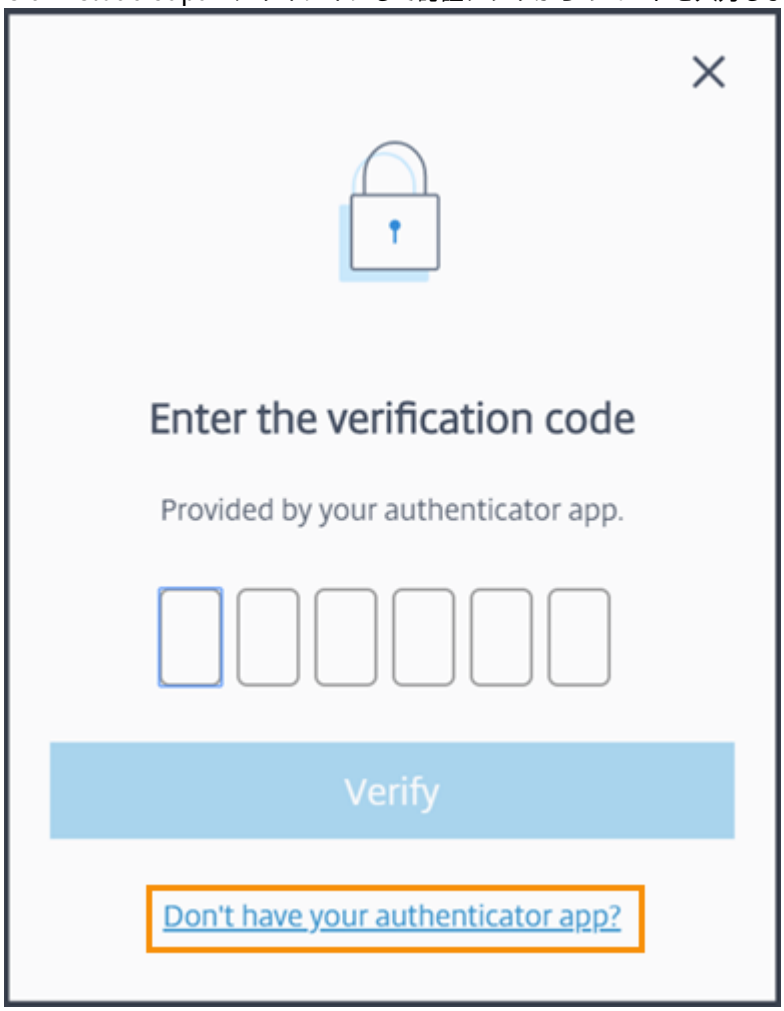
1. Citrix Cloud Japan にサインインします（https://citrix.citrixcloud.jp）。
2. ページの左上隅にあるメニューボタンをクリックし、［**ID** およびアクセス管理］を選択します。
3. ［管理者］タブをクリックします。
4. 管理する管理者を見つけ、省略記号ボタンをクリックし、［アクセスの編集］を選択します。
5. ［カスタムアクセス］を選択します。
6. 必要に応じて各権限を選択またはクリアします。
7. ［保存］をクリックします。

多要素認証用のデバイスを変更する

登録済みのデバイスを紛失した場合や、Citrix Cloud Japan で別のデバイスを使用したい場合、認証アプリをリセットした場合は、Citrix Cloud Japan の多要素認証に再登録できます。

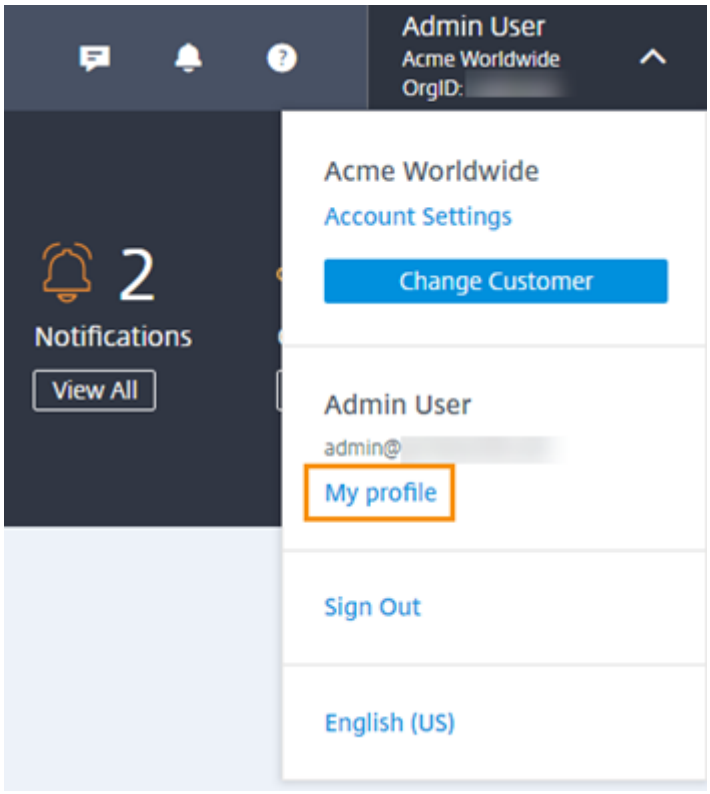
> 注
>
> - デバイスを変更すると、現在のデバイス登録が削除され、新しい認証アプリキーが生成されます。
> - 元の登録から同じ認証アプリで再登録する場合は、再登録する前に、認証アプリから Citrix Cloud Japan エントリを削除します。このエントリに表示されるコードは、再登録が完了すると機能しなくなるためです。再登録の前または後にこのエントリを削除しない場合、認証アプリには、異なるコードの 2 つの Citrix Cloud Japan エントリが表示され、Citrix Cloud Japan へのサインイン時に混乱を引き起こす可能性があります。
> - 新しいデバイスを再登録中で、認証アプリがない場合は、デバイスのアプリストアから認証アプリをダウンロードしてインストールします。操作をスムーズにするためには、デバイスを再登録する前に認証アプリをインストールすることを Citrix ではお勧めします。

1. Citrix Cloud Japan にサインインして認証アプリからのコードを入力します。

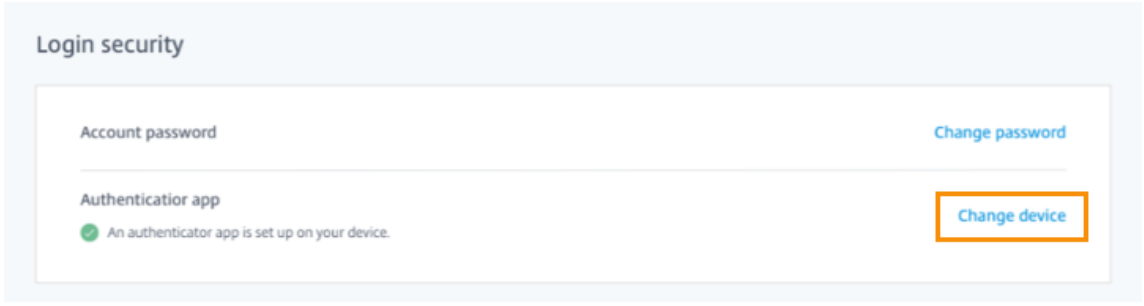


認証アプリがない場合は、［認証アプリがありませんか?］をクリックしてサインインに役立つ復旧方法を選択します。選択した復旧方法に応じて、受信した復旧コード、または未使用のバックアップコードを入力して［確認］を選択します。

2. 複数の顧客組織の管理者である場合は、任意の組織を選択します。
3. 右上のメニューから ［マイプロファイル］を選択します。



4. ［認証アプリ］で ［デバイスの変更］を選択します。

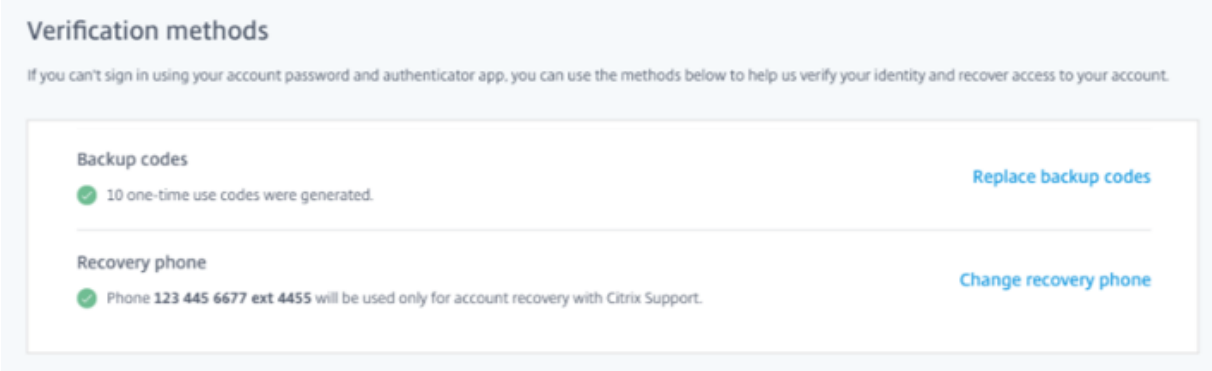


5. デバイスの変更を確認するメッセージが表示されたら、［はい、デバイスを変更します］を選択します。
6. 認証アプリから確認コードを入力して、本人確認を行います。認証アプリがない場合は、［認証アプリがありませんか?］、復旧方法の順に選択します。選択した復旧方法に応じて、受信した確認コードか復旧コード、または未使用のバックアップコードを入力します。［確認］を選択します。
7. 最初に登録したデバイスと元の認証アプリを使用している場合は、認証アプリから既存の Citrix Cloud Japan エントリを削除します。

8. 新しいデバイスを登録中で、認証アプリがない場合は、デバイスのアプリストアからダウンロードします。
9. 認証アプリから、デバイスで QR コードをスキャンするか、キーを手動で入力します。
10. 認証アプリで 6 桁の確認コードを入力して、［コードを確認する］を選択します。

確認方法を管理する

> 重要:
>
> Citrix Cloud Japan アカウントの安全を確保するには、確認方法を最新の状態に保ち、正確な情報を使用してください。認証アプリにアクセスできなくなった場合、これらの確認方法がアカウントへのアクセスを復旧する唯一の方法です。



新しいバックアップコードを生成する

1 回のみ使用できるバックアップコードを紛失したり、さらに生成する必要がある場合、いつでも新しいバックアップコードのセットを生成できます。新しいバックアップコードを生成したら、必ず安全な場所に保管してください。

1. Citrix Cloud Japan にサインインして認証アプリからのコードを入力します。
2. 複数の顧客組織の管理者である場合は、任意の組織を選択します。
3. 右上のメニューから ［マイプロファイル］を選択します。
4. ［確認方法］の ［バックアップコード］で ［バックアップコードを置き換える］を選択します。
5. 認証アプリからの確認コードを入力して、本人確認を行います。
6. バックアップコードを置き換えるように求められたら、［はい、置き換えます］を選択します。Citrix Cloud Japan により新しいバックアップコードのセットが生成され、表示されます。
7. ［コードをダウンロードする］を選択して、新しいコードをテキストファイルとしてダウンロードします。次に、［バックアップコードを保存しました。］、［閉じる］を選択します。

復旧用の電話番号を変更する

1. Citrix Cloud Japan にサインインして認証アプリからのコードを入力します。

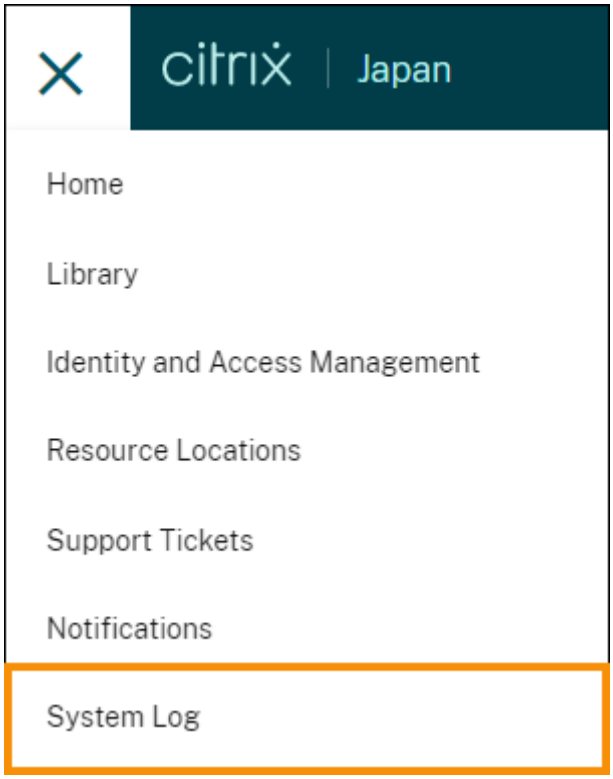
2. 複数の顧客組織の管理者である場合は、多要素認証で最初に登録した組織を選択します。
3. 右上のメニューから ［マイプロファイル］を選択します。
4. ［確認方法］の ［復旧用の電話番号］で ［復旧用の電話番号を変更する］を選択します。
5. 使用する新しい電話番号を入力し、［保存］を選択します。

システムログ

November 21, 2023

システムログには、Citrix Cloud Japan で発生したイベントがタイムスタンプ付きで一覧表示されます。これらの変更を CSV ファイルとしてエクスポートして、組織の規制遵守要件を満たしたり、セキュリティ分析をサポートしたりすることができます。

システムログを表示するには、Citrix Cloud Japan メニューで ［システムログ］を選択します。



システムログのデータの保持について詳しくは、この記事の「データ保持」を参照してください。

制限事項

このシステムログ機能は、Citrix Cloud Japan でも Citrix Cloud（citrix.cloud.com）と同様に機能しますが、以下の項目は Citrix Cloud Japan では使用できません。

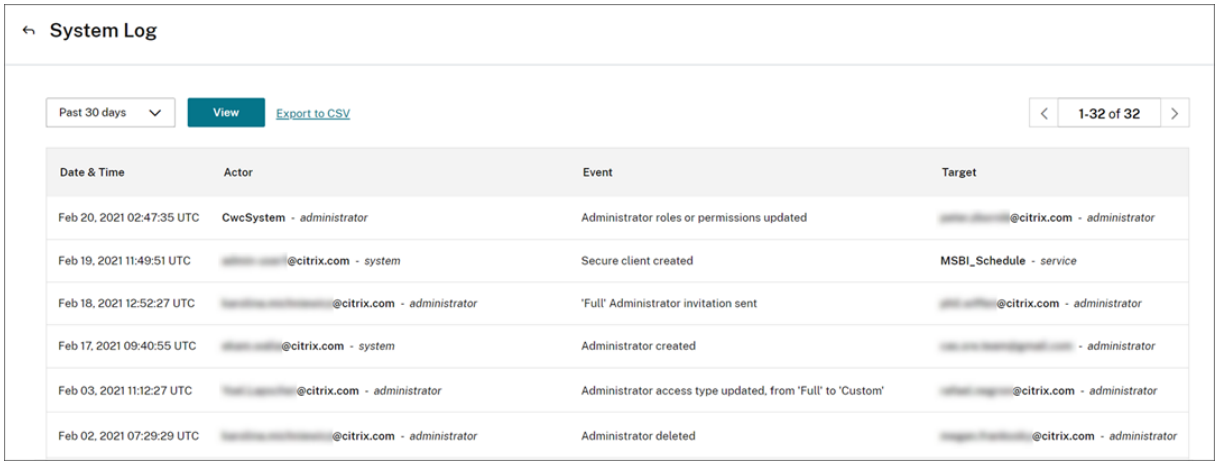
- SystemLog API
- システムログ用の Splunk アドオン

ログに記録されたイベント

システムログは、特定の Citrix Cloud Japan プラットフォームおよびクラウドサービス操作のイベントをキャプチャします。これらのイベントの完全な一覧とキャプチャされたデータの説明については、「システムログイベントのリファレンス」を参照してください。

> 注:
>
> システムログイベントのリファレンスには、Citrix Cloud で発生するプラットフォームおよびサービス関連のイベントが含まれています。Citrix Cloud Japan で生成されるイベントは、リファレンスの記事に記載されているイベントのサブセットです。Citrix Cloud Japan でサポートされている新しいイベントに関する通知については、「Citrix Cloud Japan の新機能」を参照してください。

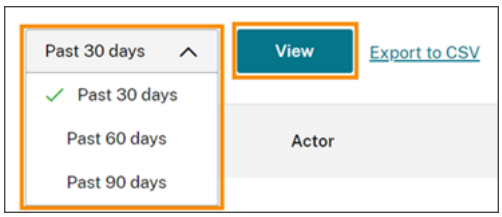
システムログには、過去 30 日間に発生したイベントがデフォルトで最大 90 日間表示されます。最新のイベントが一番上に表示されます。



表示される一覧には、次の情報が含まれます:

- イベントが発生した日時（UTC）。
- 管理者やセキュアクライアントなど、イベントを開始したアクター。アクター **CwcSystem** のエントリは、Citrix Cloud Japan がその操作を行ったことを示します。
- 管理者の編集や新しいセキュアクライアントの作成など、イベントの簡単な説明。
- イベントの対象。対象は、イベントの結果として影響を受けた、または変更されたシステムオブジェクトです。たとえば、管理者として追加されたユーザーなどです。

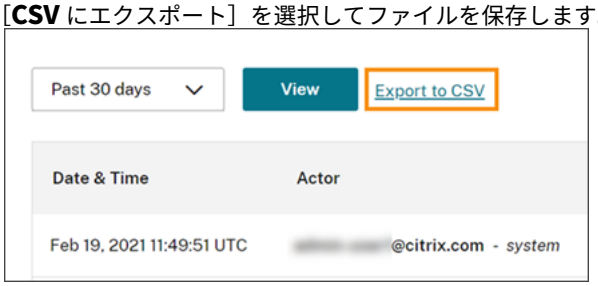
過去 90 日間に発生したイベントを表示するには、表示する期間でフィルタリングして ［表示］を選択します。



イベントのエクスポート

過去 90 日間に発生したシステムログイベントの CSV ファイルをエクスポートできます。ダウンロードしたファイルの名前は、次の形式です。`SystemLog-CustomerName-OrgID-DateTimeStamp.csv`

1. Citrix Cloud Japan メニューの ［システムログ］を選択します。
2. 必要に応じて一覧をフィルターして、イベントをエクスポートする期間を表示します。
3. ［**CSV** にエクスポート］を選択してファイルを保存します。



CSV ファイルには、次の情報が含まれています:

- 各イベントの UTC タイムスタンプ
- 名前やアクター ID など、イベントを開始したアクターの詳細。
- イベントの種類やイベントのテキストなど、イベントの詳細
- ターゲット ID、管理者またはセキュアクライアントの名前など、イベントの対象の詳細。

データ保持

シトリックスとお客様は、Citrix Cloud Japan がキャプチャしたシステムログデータを保持する共同責任があります。

Citrix は、イベントの記録後 90 日間、システムログレコードを保持します。

お客様には、組織のコンプライアンス要件に合わせて保持するシステムログレコードをダウンロードし、これらのレコードを長期ストレージソリューションに格納する責任があります。

パートナー向けの **Citrix Cloud Japan**

November 21, 2023

Citrix Cloud Japan には、顧客とパートナーの両方用に設計されたサービス、機能、エクスペリエンスが含まれています。Citrix Cloud Japan のパートナーエクスペリエンスは、Citrix Cloud の場合と同じです。

パートナーは、次の機能を利用できます:

- Citrix Cloud Japan で接続する顧客を招待します。
- トライアルを含む、顧客のサービス使用権を表示します。
- 管理者コンソールから顧客ダッシュボードへのアクセスを有効または無効にします。
- 顧客ダッシュボードからライセンスの傾向を表示します。
- ライセンスコンソールを使用して、Citrix DaaS の利用特典のカスタマーライセンスと使用状況を表示します。
- Citrix Cloud Japan 管理コンソールから顧客の通知を表示します。

パートナーエクスペリエンスについて詳しくは、「パートナー向けの Citrix Cloud」を参照してください。

SDK

November 21, 2023

Citrix DaaS Remote PowerShell SDK では、繰り返し行う複雑なタスクを自動化できます。この SDK のメカニズムにより、Studio のユーザーインターフェイスを使用することなく、Citrix DaaS（Citrix Virtual Apps and Desktops の新名称）環境を設定し管理できるようになります。

要件

マシン上で PowerShell 3.0 以降が使用できる必要があります。

Remote PowerShell SDK をインストールまたは削除する

Citrix Cloud Japan で使用する Remote PowerShell SDK をインストールするには:

1. インストーラーをダウンロードします: https://download.apps.cloud.com/CitrixPoshSdk.exe。
2. コマンド`CitrixPoshSdk.exe EnvironmentName=Japan`を実行します。このコマンドを使用すると、デフォルトで SDK を Citrix Cloud Japan のコンテキストで実行できます。

> 注:
>
> または、SDK インストーラーを実行し、ダイアログに従ってインストールを完了することもできます。ただし、Get-XdAuthentication コマンドレットを使用して認証する場合は、Citrix Cloud Japan 環境を指定する必要があります。この記事の「Remote PowerShell SDK を実行するには」を参照してください。

%TEMP%\CitrixLogs\CitrixPoshSdk にインストールログが作成されます。このログは、インストールの問題の解決に役立ちます。

Remote PowerShell SDK をアンインストールするには:

1. プログラムの削除または変更を行う Windows 機能で、[**Citrix DaaS Remote PowerShell SDK**] を選択します。
2. 右クリックして [アンインストール] を選択します。
3. ダイアログの手順を実行します。

Remote PowerShell SDK を実行するには

Remote PowerShell SDK は、そのリソースの場所内にあるドメイン参加済みコンピューターで実行します:

1. PowerShell コマンドプロンプトを開きます。管理者として実行する必要はありません。
2. Citrix スナップインを追加します: `asnp citrix.*`
3. コマンド`Get-XdAuthentication`を実行して、認証を明示的に行うことができます。また、最初の Remote PowerShell SDK コマンドを実行すると、Get-XdAuthentication と同じ認証が求められます。ただし、このページの前半の「Remote PowerShell SDK をインストールまたは削除する」で説明されているように SDK をインストールしなかった場合は、コマンド`Get-XdAuthentication -EnvironmentName Japan`を使用して Citrix Cloud Japan への認証を行う必要があります。
4. 引き続き PS SDK コマンドレットまたは PS SDK 自動化スクリプトを実行します。スクリプトの例については、Citrix DaaS のドキュメントの「アクティビティの例」を 参照してください。

> 注:
>
> - 一度認証を行うと、リモートアクセスは 24 時間にわたり現在の PowerShell セッションで有効なままになります。この期限後は、資格情報の入力が必要になります。
> - この SDK のコマンドレットは、Cloud Connector では実行しないことを Citrix ではお勧めします。これは、SDK の操作に Cloud Connector は関係しないためです。

サポート対象のスナップインおよび無効化されたスナップインの完全な一覧については、Citrix DaaS のドキュメントの「サポートと制限事項」を参照してください。

Citrix Cloud Japan での Citrix Gateway サービス

December 20, 2023

Citrix Gateway サービスは、Citrix Cloud Japan で一般提供されています。すべての顧客のトラフィックは、専用の Citrix Cloud Japan PoP のみを経由します。詳しくは、「CTX340508: Citrix Gateway Service Points of Presence (PoPs) - Citrix Cloud Japan」を参照してください。Citrix DaaS（Citrix Virtual Apps and Desktops サービスの新名称）を使用している場合、Citrix Cloud Japan 内で HDX プロキシ用 Gateway サービスを使用できるようになりました。Citrix Gateway サービスは東京と大阪の 2 つリージョン（PoP）で利用可能です。

サポートされている Citrix Gateway サービス機能

以下は、Citrix Cloud Japan 上の Citrix Gateway サービスでサポートされている機能の一部です。

HDX プロキシ

Citrix Gateway サービス内の HDX プロキシ機能は、Citrix Virtual Apps and Desktops へのセキュアで信頼性の高いアクセスを提供します

高可用性

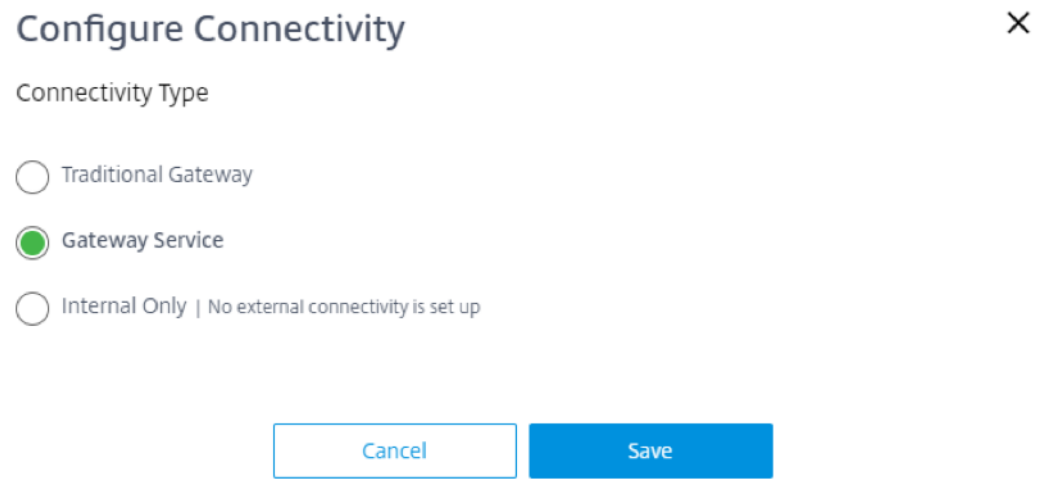
Citrix Gateway サービスによる複数段階の耐障害性アプローチは、あらゆるレベルで耐障害性を提供します。特定の Citrix Gateway サービス POP 内で、サービスを形成するマイクロサービスとテナントは高可用性形式で展開されます。コンポーネントは、N+1 モデルで展開されます。このモデルでは、すべてのコンポーネントが負荷分散されており、スタンバイ状態であるため何らかの障害が発生した場合に迅速なフェールオーバーを実行できます。まれに、POP 内の特定のコンポーネントのすべてのサービスがダウンしている場合、Citrix Gateway サービスはサービス自体をダウンとしてマークします。これにより、DNS サーバーはユーザーを次に近い POP にリダイレクトできるため、POP レベルの高可用性を提供できます。

最適なゲートウェイルーティング

Citrix Gateway サービスは、日本全国の複数の地域に展開されているため、最高のパフォーマンスを得るために最適な POP を選択するメカニズムが必要です。最適なゲートウェイルーティングまたは近接ルーティングの DNS ベースのサービスは、エンドユーザーが Citrix Gateway サービスに接続しようとするときに、最も近い POP ロケーションに戻るために使用されます。この DNS サービスは、クエリのソース IP アドレスをメタデータの 1 つとして使用して、最も近い Citrix Gateway サービスの POP IP アドレスを返します。

Citrix Gateway サービスを有効にする方法

1. ［リソースの場所］ページで構成するリソースの場所を見つけて、［**Gateway**］をクリックします。［接続の構成］ダイアログが開きます。



2. ［**Citrix Gateway** サービス］をクリックして、外部ユーザーにアプリケーションとデスクトップへのセキュアなアクセスを提供します。
3. ［保存］をクリックします。

Citrix Cloud Connector の接続要件

Citrix Cloud Connector は、Microsoft Windows サーバーで実行されるサービスセットを展開するソフトウェアパッケージです。Cloud Connector をホストするマシンは、Citrix Cloud Japan で使用するリソースが存在するネットワーク内にあります。Cloud Connector は Citrix Cloud Japan に接続し、必要に応じてリソースを操作および管理することができます。Citrix リソースの場所/Cloud Connector について詳しくは、Cloud Connector の一般的なサービス接続要件を参照してください。

Gateway サービスを使用するには、次の URL にアクセスできる必要があります: `https://*.*.nssvc.jp`。

すべてのサブドメインを有効にできない顧客は、代わりに次のアドレスを使用できます:

- `https://*.g.nssvc.jp`
- `https://*.c.nssvc.jp`

オンプレミスの **Citrix Gateway** からクラウドベースの **Citrix Gateway** サービスに移行

オンプレミスの Citrix Gateway からクラウドベースの Citrix Gateway サービスに移行できます。詳しくは、「Citrix Gateway を HDX プロキシ用の Citrix Gateway サービスに移行する」を参照してください。