Citrix Cloud

Contents

Citrix Cloud

September 17, 2021

Citrix Cloud は、シトリックスのクラウドサービスをホストし管理するプラットフォームです。どのクラウドやインフラストラクチャ（オンプレミス、パブリッククラウド、プライベートクラウド、またはハイブリッドクラウド）を使用する場合でも、コネクタ経由でローカルのリソースに接続します。単一のコンソールからエンドユーザーに対してアプリおよびデータとともにワークスペースを作成、管理、展開できます。

Citrix Cloud のトライアル

上記の 1 つまたは複数の Citrix Cloud サービスを、概念実証済みの製品版環境でお試しください。Citrix Cloud に登録後、コンソールからサービスごとのトライアルをリクエストできます。トライアルの終了後もすべての構成を保持できるように、製品版環境に移行することができます。詳しくは、「Citrix Cloud サービスのトライアル」を参照してください。

Citrix Cloud サービスドキュメント

Citrix Cloud サービスのセットアップまたは管理に関する情報をお探しですか? このページの左側にある目次の「**Citrix Cloud** サービス」セクションに移動します。サービスを選択して、そのサービスの製品ドキュメントに直接アクセスします。

アーキテクチャのリソースと展開のリソース

Citrix Tech Zoneには、Citrix Cloud およびそのほかのシトリックス製品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、技術資料を参照することができます。

Citrix Cloud の主要なサービスコンポーネントについて詳しくは、次のリソースを参照してください:

- Citrix Workspace の概念図: ID、ワークスペースインテリジェンス、シングルサインオンなどの主要分野の概要を提供します。
- リファレンスアーキテクチャ: ユースケース、推奨事項、関連リソースなど、Citrix Workspace の実装を計画するための包括的なガイドを提供します。
- Virtual Apps and Desktops サービスのリファレンスアーキテクチャ: Virtual Apps and Desktops サービスを関連するサービスとともに展開するための詳細なガイダンスを提供します。

教育リソース

Citrix Cloud Learning シリーズポータルでは、Citrix Cloud とそのサービスを導入して実行するための教育モジュールを提供しています。概要から、計画と構築のサービスまで、すべてのモジュールを順番に確認できます。次の

コースでクラウドの旅を始めましょう：

- Citrix Cloud の基礎
- Citrix ID と認証の概要
- StoreFront から Workspace への移行

Citrix Education ビデオライブラリでは、主要な展開タスクと、Citrix Cloud サービスで使用するコンポーネントのトラブルシューティングについて説明したオンライン動画レッスンを提供しています。Cloud Connector のインストールや VDA の登録、およびこれらのコンポーネントのトラブルシューティングなどのタスクに関する詳細をご覧ください。

サービスレベルアグリーメント

July 28, 2021

発効日：2020 年 10 月 30 日

Citrix Cloud は、業界のベストプラクティスを使用して、高度なサービス可用性を実現するように設計されています。

このサービスレベルアグリーメント（SLA）では、Citrix Cloud サービスの可用性に関するシトリックスの目標について説明します。この SLA は、対象サービス（「サービス」）に関するシトリックスのエンドユーザーサービス契約（EUSA）の一部です。

シトリックスのサービス目標（「サービス目標」）は、サービスの月間稼働時間（「月間稼働時間」）を 99.9%以上に維持することです。月間稼働時間は、当該サービスのインスタンスが 1 か月間に「使用不可」の状態にあった時間（分）のパーセント値を 100%から引いて計算します。サービスの種類およびサービス別の可用性の評価基準については、以下の表で定めるものとします。月間稼働時間（%）には次のような原因で生じたダウンタイムを含みません：

- 定期的にスケジュール設定された保守時間。
- 当該サービスの構成要件（https://docs.citrix.com）にお客様が従わなかった場合、不正なアクティビティがあった場合、または入力に問題があった場合。
- シトリックスがお客様に当該サービスの使用について変更するよう勧めた後に、お客様がサービスを変更せずに使用した場合。
- シトリックスが管理していないコンポーネント（次を含むがこれに限定されない）が原因である場合：お客様が管理している物理および仮想マシン、お客様がインストールし保守しているオペレーティングシステム、お客様がインストールし管理しているネットワーク機器またはその他のハードウェア、お客様が定義し管理しているセキュリティ設定、グループポリシーおよびその他の構成ポリシー。パブリッククラウドプロバイダーの障害、インターネットサービスプロバイダーの障害。シトリックスの制御の及ばない他のカスタマーサポート要因。
- お客様の従業員、代理店、契約社員、もしくはベンダー、もしくは第三者がお客様のパスワードや機器を使用してアクセスした場合、またはお客様が適切なセキュリティ上の推奨事項に従わなかったその他の場合。
- お客様がサービス使用権を越える処理を実行しようとした場合。

- 不可抗力によるサービスの中断（自然災害、戦争もしくはテロ行為、または政府の方針を含むがこれに限定されない）。

シトリックスのトライアル、テクニカルプレビュー、Labs もしくはベータ版のサービスについては、サービス目標は提供されません。

シトリックスは、次のお客様にサービス目標を提供します：

- 期間ベースのサブスクリプション（最低 1 年間のサブスクリプション期間）を使用して当該サービスを購入している。
- 請求期間中に当該サービスに適用できるライセンスモデルあたり少なくとも 100 ユニットのサブスクリプション（Citrix Service Provider で最小 1,000）がある。

Citrix Service Provider（CSP）は 2018 年 10 月 1 日に対象となりました。

サービス別の可用性の評価基準

サービス	月間稼働時間の評価基準
Citrix Analytics for Performance	ユーザーがアプリやデスクトップのパフォーマンスにアクセスして改善できる時間。
Citrix Analytics for Security	ユーザーがユーザーアクセスとユーザーアクティビティのリスクを検出して軽減できる時間。
Citrix Application Delivery Management サービス	すべての POP でサービスを利用できる平均時間。
Citrix Content Collaboration	ユーザーが自分のアカウントに関連付けられたファイルやフォルダーを表示したり、シトリックス管理のストレージゾーンでホストされているファイルをダウンロードしたりできる時間。
Citrix Endpoint Management	ユーザーがサービスを使用して、シトリックスが配信したモバイルアプリおよび登録済みデバイスにアクセスできる時間。
HDX プロキシ用の Citrix Gateway サービス	ユーザーがサービスを使用して、自分のアプリまたはデスクトップセッションにアクセスできる時間。
Citrix Intelligent Traffic Management	ユーザーが DNS クエリまたは HTTP API コールを使用してトラフィック管理機能にアクセスできる時間。
SD-WAN Orchestrator	ユーザーがサービスを使用して、SD-WAN Orchestrator アカウントにアクセスし、SD-WAN ネットワークを管理できる時間。
Citrix Secure Workspace Access	ユーザーがサービスを使用して、SaaS または内部 Web アプリにアクセスできる時間。

サービス	月間稼働時間の評価基準
Citrix Virtual Apps サービス	ユーザーがサービスを使用して、自分のアプリまたはデスクトップセッションにアクセスできる時間。
Citrix Virtual Desktops サービス	ユーザーがサービスを使用して、自分のアプリまたはデスクトップセッションにアクセスできる時間。
Citrix Virtual Apps and Desktops サービス	ユーザーがサービスを使用して、自分のアプリまたはデスクトップセッションにアクセスできる時間。
Citrix Workspace	上記コンポーネントサービスの場合と同じですが、可用性は個別に評価します。一部のコンポーネントに関するクレームの場合、クレジットはその割合で配分されることがあります。
Citrix Wrike	ユーザーがサービスにアクセスして使用できる時間。

サービス目標と救済措置

シトリックスが本 SLA 発効日から起算して連続 5 か月間に 3 回以上サービス目標を達成しなかった場合には、排他的な救済措置として、10%のサービスクレジットが、月単位で、シトリックスがサービス目標を達成しなかった月数分、お客様が直近の更新期間に翌年度のサービスを延長されるときに、影響を受けたものと同じサービスおよびユニット数に関して計上されるものとします。

- 月間稼働時間（%）：< 99.9%
- サービスクレジット：該当する月数分の 10%（お客様にバウチャーとして提供）

上記の救済を受けるためには、お客様は EUSA に従い、サービスクレジットを請求する連続 5 か月間の最終月末から三十（30）日以内に目標未達成について報告する必要があります。この SLA に違反している可能性を報告する手順については、CTX237141を参照してください。

請求の際は、サービスを特定し、使用不可の状態にあった日時および期間と合わせて証拠となるログまたはレコードを明確にし、影響を受けたユーザーとその場所、およびテクニカルサポートの要求または修復アクションの実施についてもすべて明示する必要があります。1 サービスあたり 1 回のみ、該当する月数分のサービスクレジットが発行されます。延長期間全体に対して、10% のサービスクレジットが最大 1 回、発行されます。お客様は、延長購入時にバウチャーを提示する必要があります。

販売代理店経由で延長を購入する場合は、販売代理店経由でクレジットを受け取ります。直接購入に適用されるか間接購入で販売代理店経由で提示されるクレジットは、同じユニット数を延長する場合の混合レートでの希望小売価格を配分した額に基づきます。シトリックスが再販価格および再販クレジットを制御することはありません。クレジットにはシトリックスまたは再販代理店への支払いを相殺する権利はありません。シトリックスは、これらの規定を適宜変更することができるものとします。変更時に、シトリックスは本サービスレベルアグリーメントの冒頭にある発行日を併せて変更します。変更はすべて、最新発行日以降のサービス新規購入あるいはサービス延長にのみ適用されます。

セキュリティで保護された **Citrix Cloud** プラットフォームの展開ガイド

July 29, 2021

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

以下の記事は、Citrix Cloud の他のサービスに関する同様の情報を提供しています:

- 分析技術セキュリティの概要
- Endpoint Management のセキュリティの技術概要
- Secure Browser のセキュリティの技術概要
- ShareFile のセキュリティの技術概要
- Virtual Apps and Desktops のセキュリティの技術概要
- Virtual Apps and Desktops Standard for Azure のセキュリティの技術概要

コントロールプレーン

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 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 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。
- デフォルトでは、Citrix Cloud は 60 分間何も操作しないと管理者セッションを自動的に終了します。この 60 分のタイムアウトは変更できません。_ 非アクティブ _ とは、セッションが完全にアイドル状態であり、管理者が Citrix Cloud コンソールを操作していないことを意味します。_ アクティビティ _ とは、グラフィックインターフェイスのナビゲート、構成オプションの選択、構成変更の保存、変更が有効になるまでの待機などのアクションを指します。

パスワードコンプライアンス

現在のパスワードが設定から 60 日以上経過している場合、Citrix Cloud で管理者にパスワードの変更が要求されます。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:

- 長さが 12 文字以上
- 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:

- 現在のパスワード内の文字を少なくとも 1 つ変更する必要があります。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 24 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、設定から 1 日間は変更できません。

暗号化とキー管理

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 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（管理者に明示的にプロンプトを表示します）。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 はシトリックス所有の cloud.com 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 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。

- Cloud Connector が Windows Server 2016 または Windows Server 2019 にインストールされている場合は、次の強力な暗号の組み合わせをお勧めします: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384、TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- Cloud Connector が Windows Server 2012 R2 にインストールされている場合、強力な暗号の組み合わせは使用できないため、次の暗号の組み合わせを使用する必要があります: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384、TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

各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。

データ主権

Citrix Cloud コントロールプレーンは、米国および欧州連合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 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。

Content Collaboration でデータの格納場所を管理する方法については、次のドキュメントを参照してください:

- Content Collaborationサービスのドキュメント
- ShareFile のセキュリティに関するよくある質問（英語）
- Citrix ShareFile のセキュリティとコンプライアンス（英語）
- オンプレミスストレージのストレージゾーンを実装する方法

他のサービスでは、異なるリージョンにデータを格納するオプションがあります。各サービスについては、「地理的な考慮事項」のトピックまたはこの記事の冒頭にも記載されているセキュリティの技術概要を参照してください。

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

Cloud Connector のインストール

セキュリティとパフォーマンス上の理由から、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でください。

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、「Citrix Cloud Connector」を参照してください。

Cloud Connector の構成

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ことを強くお勧めします。これは Active Directory のデフォルトの構成です。また、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 Virtual Apps and Desktops 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（保守操作のためなどに）ログオンできるようにすることを強くお勧めします。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 マシンへの他の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。これらのマシンには、それ以外のソフトウェアをインストールしないでください。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 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可能な受信ポートを設定しないことを強くお勧めします。

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 暗号化通信をサポート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。

内部ネットワーク内では、Citrix Connector 用に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	636/TCP	LDAP SSL
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 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、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）
- Citrix Cloud サービスの「インターネット接続の要件」
- Application Delivery Management サービスポートの要件
- Endpoint Management ポートの要件

外部通信の監視

Cloud Connector は、ポート 443 上で Citrix Cloud 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 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 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 がシトリックス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シトリックス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）
- Citrix Cloud サービスの「インターネット接続の要件」

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 の基本構成では、特に SSL/TLS 構成は必要ありません。

Cloud Connector は、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。シトリックスと 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 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。

セキュリティコンプライアンス

Cloud Connector は、自己管理機能によって確実なセキュリティコンプライアンスを実現します。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、重要な更新がある時に Cloud Connector が更新されなくなります。

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。セキュリティ上の修正プログラムは自動的に適用されます。

クラウドサービス用の **Citrix** コネクタアプライアンス

コネクタアプライアンスのインストール

コネクタアプライアンスはハイパーバイザーでホストされます。このハイパーバイザーは、DMZ ではなく、プライベートネットワーク内にある必要があります。

コネクタアプライアンスが、デフォルトでアクセスをブロックするファイアウォール内にあることを確認してください。許可リストを使用して、コネクタアプライアンスからの想定されるトラフィックのみを許可します。

コネクタアプライアンスをホストするハイパーバイザーが、最新のセキュリティアップデートが適用された状態でインストールされていることを確認してください。

ネットワークとシステムの要件、およびコネクタアプライアンスのインストール手順については、「クラウドサービス用のコネクタアプライアンス」を参照してください。

コネクタアプライアンスをホストするハイパーバイザーへのログオン

コネクタアプライアンスには、Citrix Cloud と通信するためのサービスキーが含まれています。最も権限のある管理者だけが、コネクタアプライアンスをホストしているハイパーバイザーに（保守操作のためなどに）ログオンできるようにします。通常、シトリックス製品を管理するために、管理者がこれらのハイパーバイザーにログオンする必要はありません。コネクタアプライアンスには、自己管理機能があります。

送受信ポートの構成

コネクタアプライアンスでは、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。コネクタアプライアンスにインターネットからアクセス可能な受信ポートを設定しないことを強くお勧めします。

送信インターネット通信を監視するために、Web プロキシの背後にコネクタアプライアンスを配置できます。ただし、Web プロキシは SSL/TLS 暗号化通信をサポートする必要があります。

コネクタアプライアンスには、インターネットにアクセスできる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、コネクタアプライアンスは幅広いポートにわたってネゴシエートします。

内部ネットワーク内では、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。

接続方向	コネクタアプライアンスポート	外部ポート	サービス
受信	443/TCP	任意	ローカル Web UI
送信	49152-65535/UDP	123/UDP	NTP
送信	53、49152-65535/TCP/UDP	53/TCP/UDP	DNS
送信	67/UDP	68/UDP	DHCP とブロードキャスト

Citrix Cloud 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、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）
- Citrix Cloud サービスの「システムおよび接続要件」

外部通信の監視

コネクタアプライアンスは、ポート 443 において Citrix Cloud サーバーでインターネットと通信します。

Citrix Cloud 内のサービスごとに、コネクタアプライアンス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、コネクタアプライアンスがシトリックス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シトリックス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）
- Citrix Cloud サービスの「システムおよび接続要件」

コネクタアプライアンスログの表示

さまざまなログファイルを含むコネクタアプライアンスの診断レポートをダウンロードできます。このレポートの取得について詳しくは、「クラウドサービス用のコネクタアプライアンス」を参照してください。

SSL/TLS 構成

コネクタアプライアンスでは、特に SSL/TLS 構成は必要ありません。

コネクタアプライアンスは、Citrix Cloud SSL/TLS 証明書で使用される証明機関（CA）を信頼します。シトリックスは将来的に証明書と CA を変更する可能性がありますが、必ずコネクタアプライアンスが信頼する CA を使用します。

Citrix Cloud 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。

セキュリティコンプライアンス

セキュリティコンプライアンスを確保するため、コネクタコンプライアンスは自己管理機能を備えており、コンソールからはログインできません。

コネクタの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。セキュリティ上の修正プログラムは自動的に適用されます。

コネクタアプライアンスをホストするハイパーバイザーが、最新のセキュリティアップデートが適用された状態でインストールされていることを確認してください。

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 の管理者リストを監査し、信頼されていないユーザー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。
- シトリックスに連絡して、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：シトリックスは、長期にわたり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：シトリックス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。

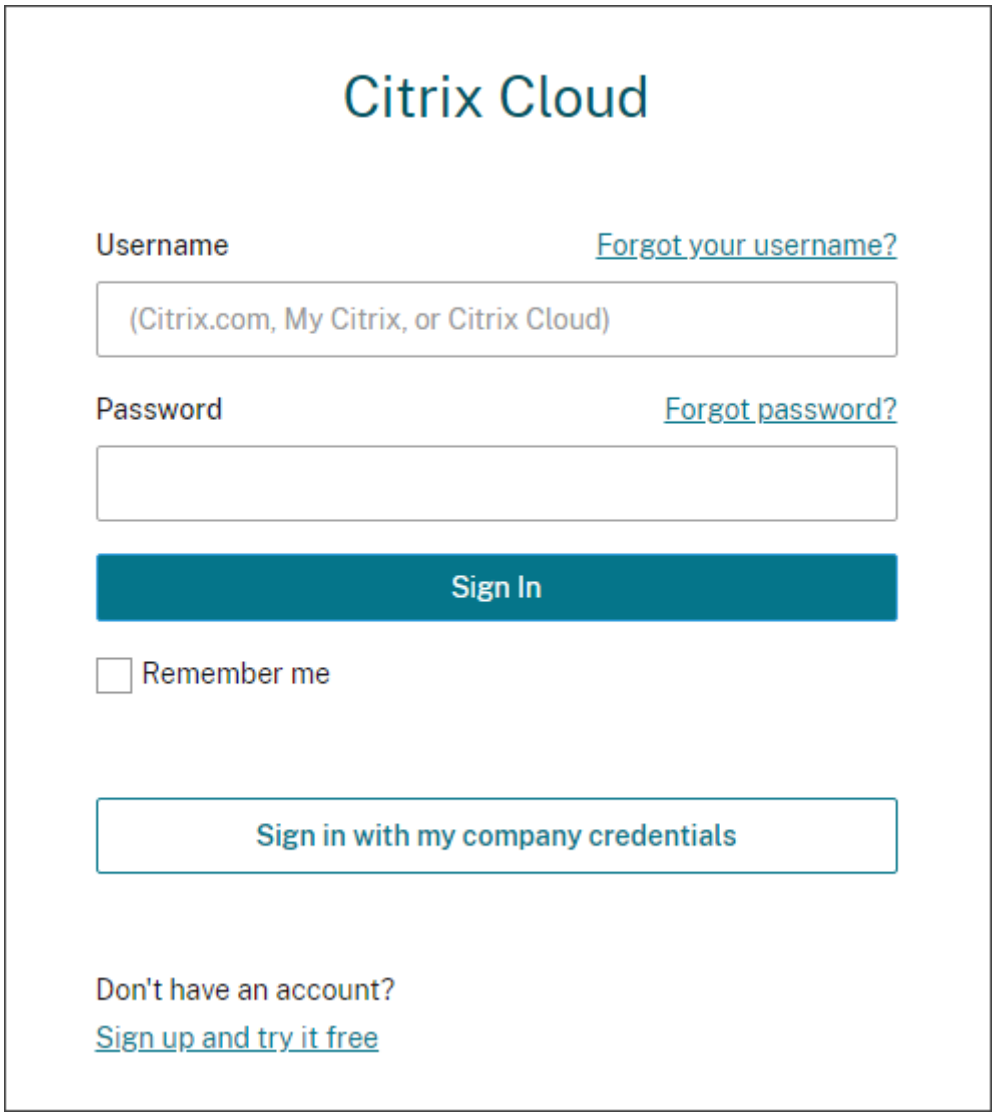
ヘルプとサポートの利用

July 29, 2021

Citrix Cloud アカウントを作成する

Citrix Cloud アカウントへの登録でエラーが発生した場合、シトリックステクニカルサポートにお問い合わせください。

アカウントにログインする



Citrix Cloud アカウントへのログインに問題がある場合は、次の手順を実行します:

- アカウントに登録したときに指定したメールアドレスおよびパスワードでログインしているかを確認してください。
- Citrix Cloud にしばらくサインインしていない場合、またはパスワードが要件を満たしていない場合、サインインする前にパスワードをリセットするよう求められます。詳しくは、この記事の「パスワードを変更する」を参照してください。
- ユーザーが Citrix アカウントではなく会社の資格情報を使用してサインインする場合は、［会社の資格情報でサインイン］を選択し、会社のサインイン URL を入力します。次に、会社の資格情報を入力すると、会社の Citrix Cloud アカウントにアクセスできます。会社のログイン URL がわからない場合、会社の管理者に問い合わせてください。

パスワードを変更する

Citrix Cloud アカウントのパスワードを忘れた場合は、[ユーザー名またはパスワードを忘れた場合] を選択して、アカウントのメールアドレスを入力し、パスワードリセットのメールを受け取ります。パスワードリセットメールが送られてこない場合、またはさらにサポートが必要な場合、シトリックスカスタマーサービスにお問い合わせください。

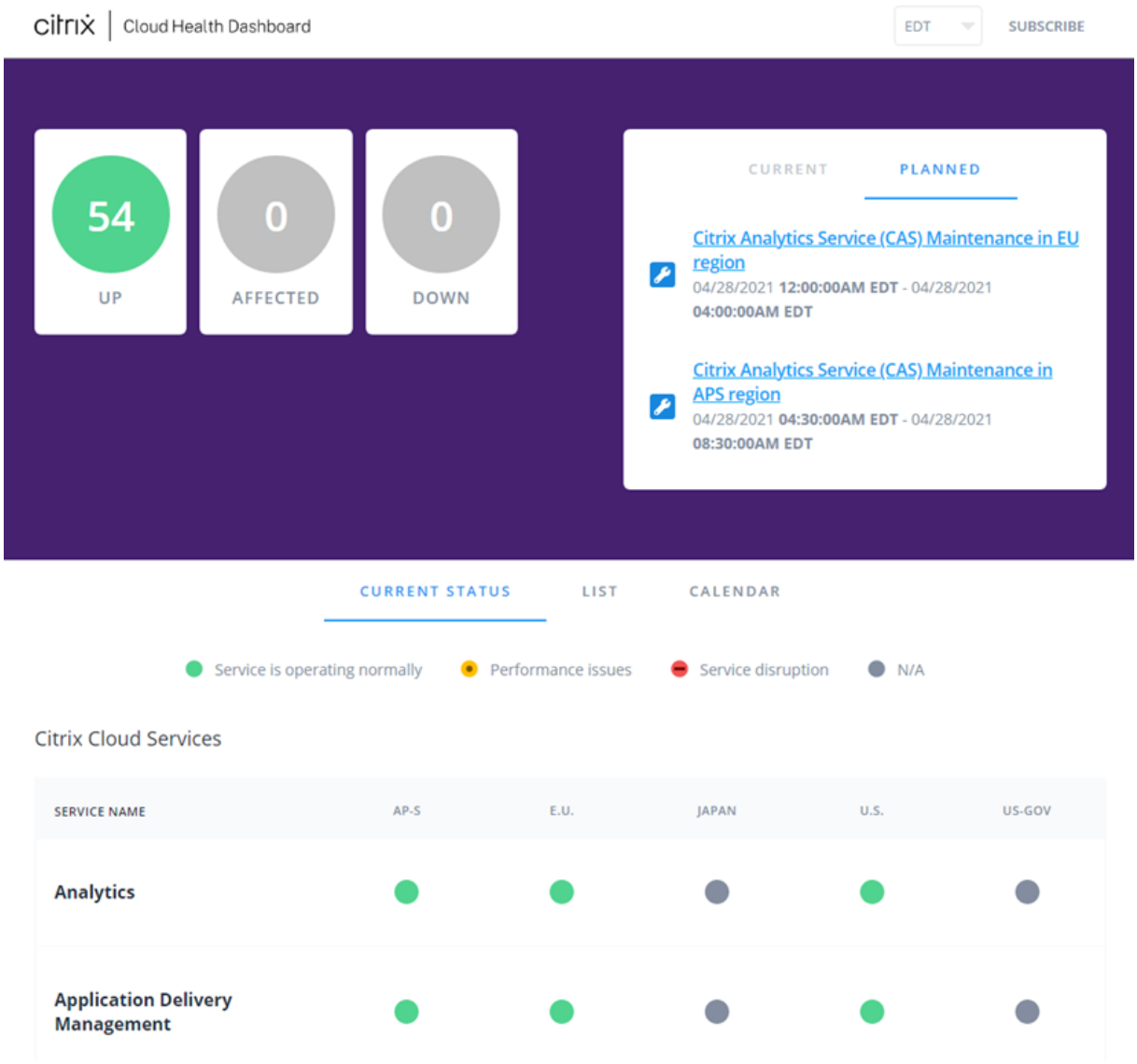
アカウントのパスワードを常に保護するために、サインイン時に Citrix Cloud からパスワードのリセットを求められる場合があります。このプロンプトは次の場合に表示されます:

- パスワードが Citrix Cloud の複雑さの要件を満たしていません。パスワードは 8 文字以上で、次の要素が含まれている必要があります:
  - 1 つ以上の数字
  - 1 つ以上の大文字
  - 1 つ以上の次の記号: ! @ # $ % ^ * ? + = -
- パスワードに辞書の単語が含まれています。
- 既知の侵害されたパスワードのデータベースに含まれるパスワードです。
- 過去 6 か月間 Citrix Cloud にサインインしていません。

プロンプトが表示されたら、[パスワードのリセット] を選択してアカウント用の強力なパスワードを作成します。

Cloud Health Dashboard

Citrix Cloud Health Dashboard（https://status.cloud.com）は、各地理的リージョンにおける Citrix Cloud プラットフォームとサービスの可用性についてリアルタイムで概要を提供します。Citrix Cloud で問題が発生した場合は、Cloud Health Dashboard をチェックして、Citrix Cloud または特定のサービスが正常に動作していることを確認してください。

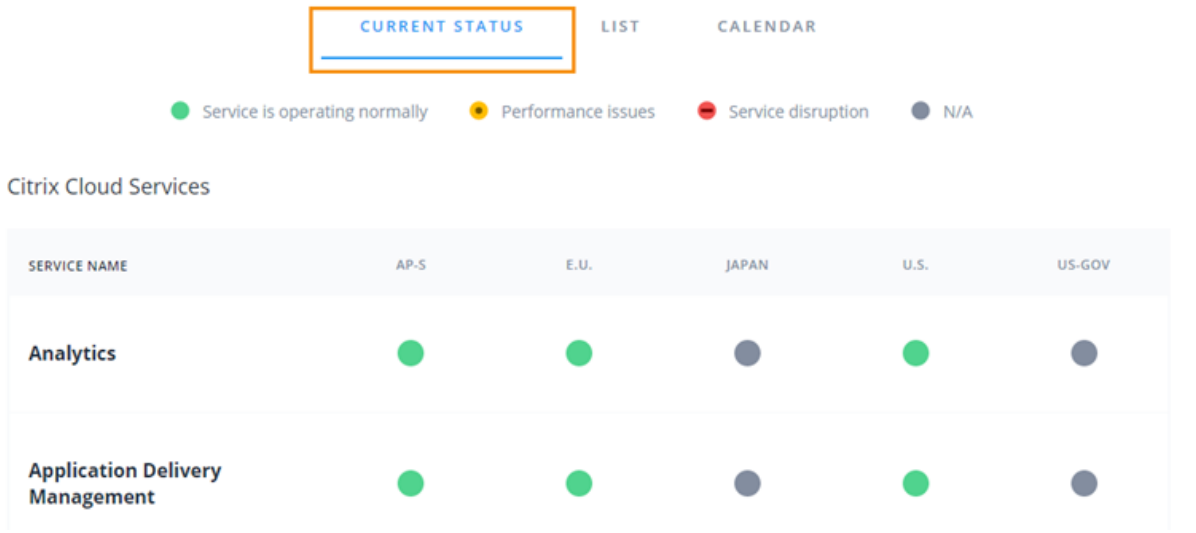


このダッシュボードを使用して、次の条件の詳細を確認します:

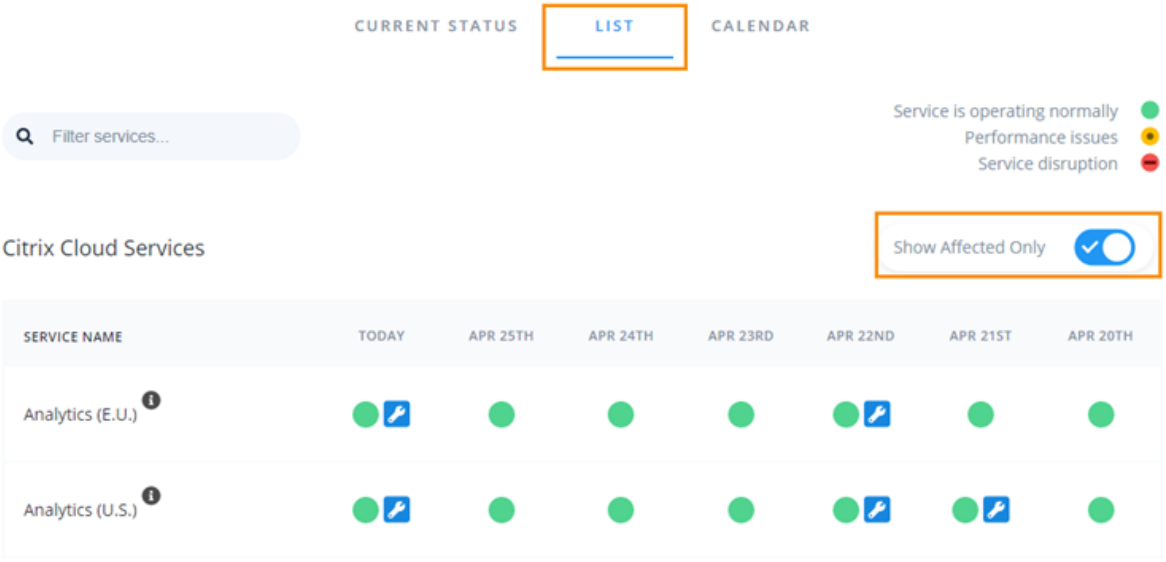
- 地理的リージョンごとにグループ化された、すべての Citrix Cloud サービスの現在のヘルス状況
- 過去 7 日間の各サービスのヘルス履歴
- 特定のサービスのメンテナンス期間

ヘルスおよびメンテナンスの状況を表示する

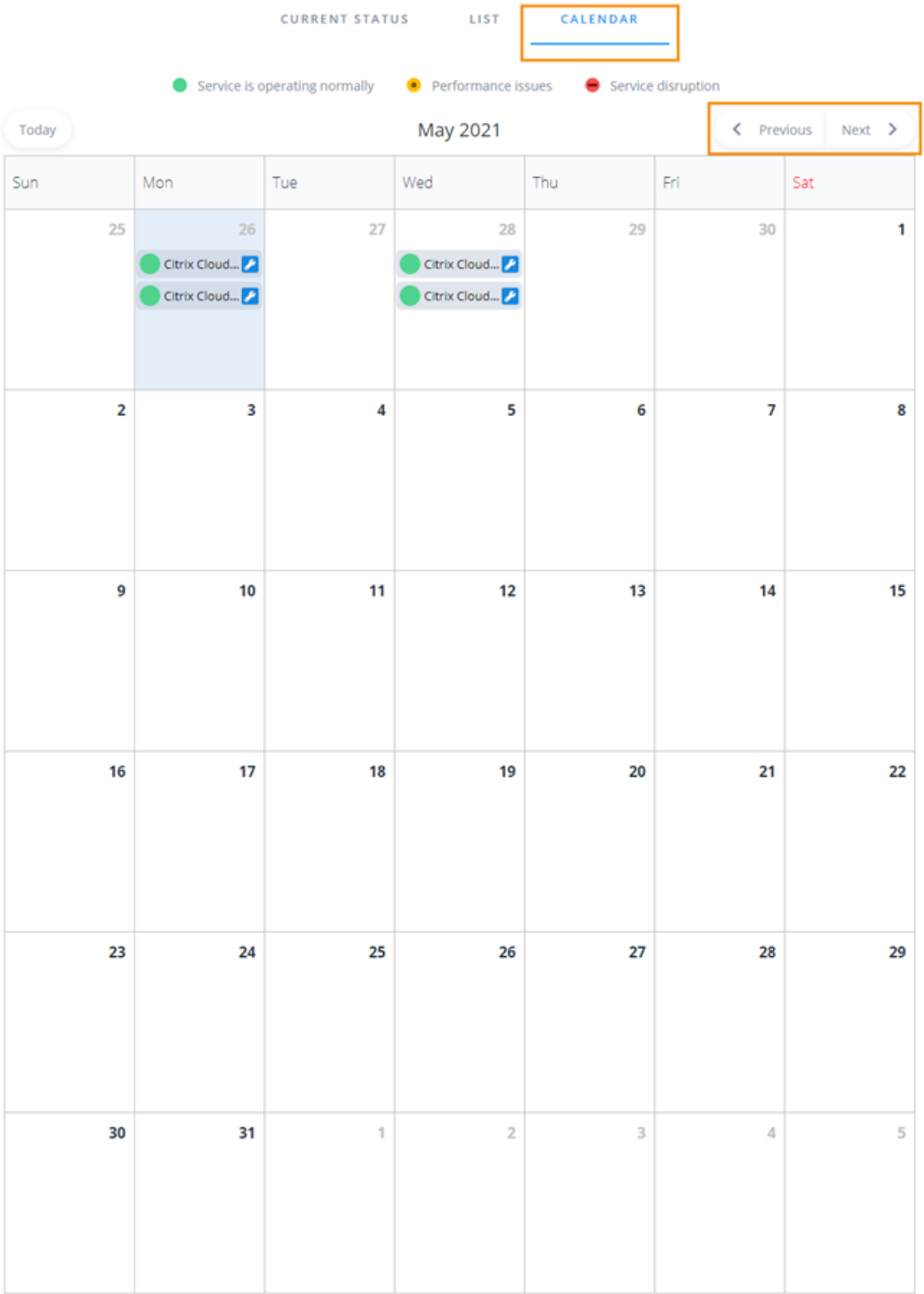
[**Current Status**] を選択して、各地理的リージョンのすべての Citrix Cloud サービスとプラットフォームコンポーネントの現在のヘルス状況を表示します。



[**List**] を選択して、過去 7 日間のすべての Citrix Cloud サービスとプラットフォームコンポーネントのヘルス状況を表示します。過去 7 日間にメンテナンスまたはヘルスイベントが発生したサービスのみを表示するには、[**Show Affected Only**] を選択します。



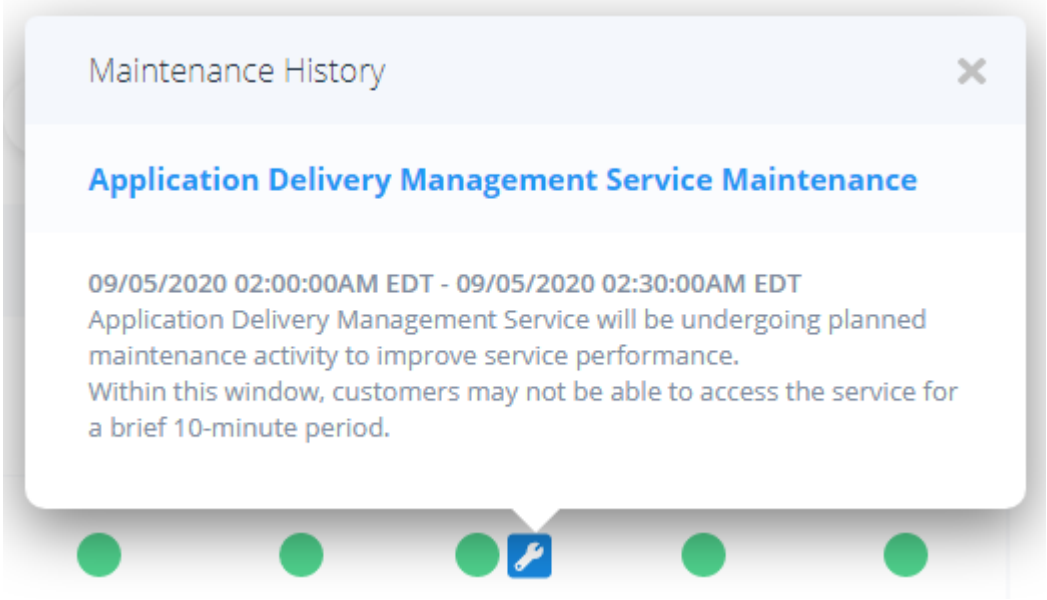
[**Calendar**] を選択して、サービスのメンテナンス期間のカレンダービューを表示します。[**Next**] または [**Previous**] を選択して、毎月のスケジュールされたメンテナンスイベントをスクロールします。



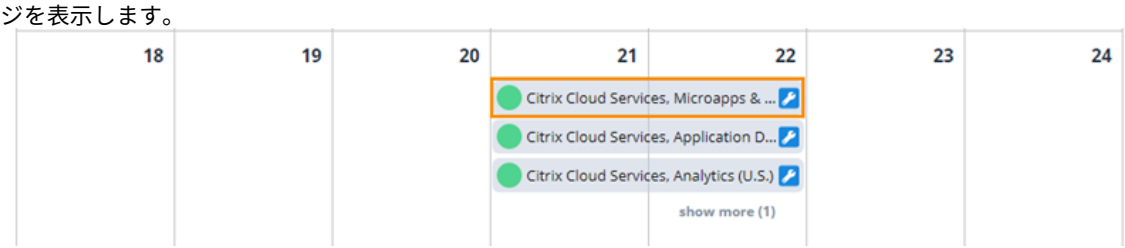
サービスインシデントの詳細を表示する

影響を受けるサービスのサービスヘルスインシデントに関する詳細情報を表示するには、次の手順に従います:

- [List] ビューで、サービスインジケーターの横にあるアイコンをクリックして、サービスヘルスインシデントに関する詳細情報を表示します。



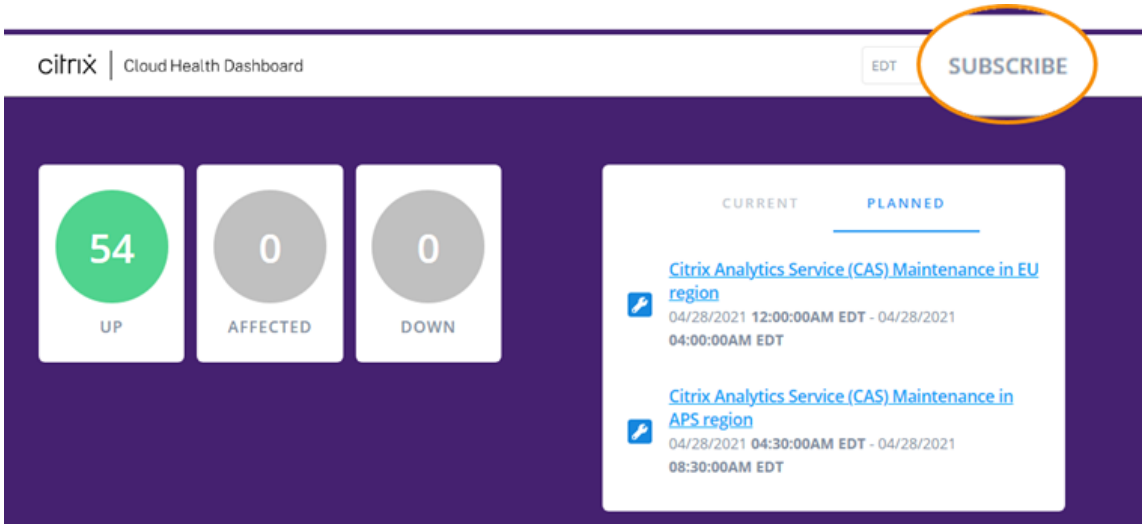
- [Calendar] ビューで、サービスエントリをクリックして、スケジュールされたメンテナンス期間の状況ページを表示します。



通知にサブスクライブ

次の方法を使用して、サービスヘルスイベントに関する通知を受け取ることができます:

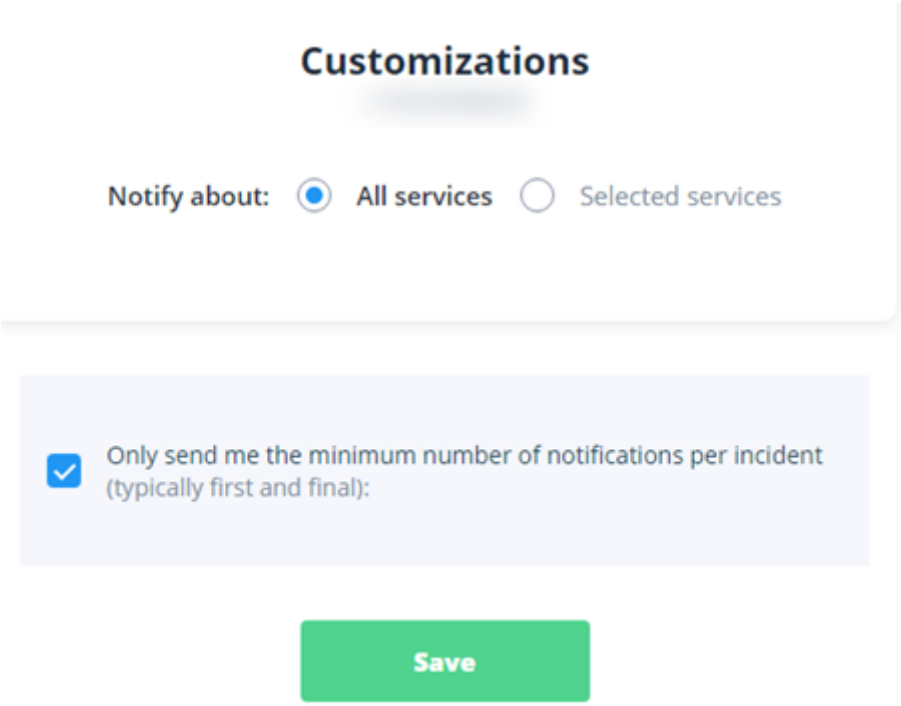
- ダッシュボードの右上にある [**Subscribe**] を選択し、使用する通知方法を選択します。メールや電話など、いくつかの方法から選択できます。



- RSS リーダーに次の URL を入力して、Citrix Cloud Health RSS フィードにサブスクライブします:
  - 1 つのフィードでサービスインシデントとメンテナンスの通知を受信するには、`https://status.cloud.com/?format=atom`にサブスクライブします。
  - サービスインシデント通知のみを受信するには、`https://status.cloud.com/atom/incidents`にサブスクライブします。
  - メンテナンス通知のみを受信するには、`https://status.cloud.com/atom/maintenances`にサブスクライブします。

すべての地理的リージョンのすべてのサービス通知にサブスクライブするには:

1. ダッシュボードの右上隅にある［**Subscribe**］を選択し、使用する通知方法を選択します。
2. 選択したサブスクリプション方法の連絡先の詳細または URL を入力します。［次へ］をクリックします。
3. ［**Customizations**］ページで、［**All services**］を選択して、すべての地理的リージョンのすべてのサービスの通知を受信します。
4. 各インシデントの最初と最後の通知のみを受信するには、［**Only send me the minimum number of notifications per incident**］を選択します。
5. ［保存］をクリックします。



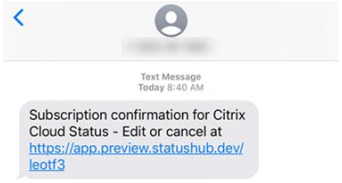
特定のサービスまたはリージョンの通知にサブスクライブするには:

1. ダッシュボードの右上隅にある［**Subscribe**］を選択し、使用する通知方法を選択します。
2. 選択したサブスクリプション方法の連絡先の詳細または URL を入力します。［次へ］をクリックします。
3. ［**Customizations**］ページから、［**Selected services**］を選択します。サポートされているすべてのリージョンのすべてのサービスを表示する複数ページの一覧が表示されます。
4. 通知を受け取る地理的リージョンのサービスを選択します。地理的リージョンのすべてのサービスについて通知を受けるには、［**Aggregate by groups**］を選択してから、リージョンを選択します。
5. 各インシデントの最初と最後の通知のみを受信するには、［**Only send me the minimum number of notifications per incident**］を選択します。
6. ［保存］をクリックします。

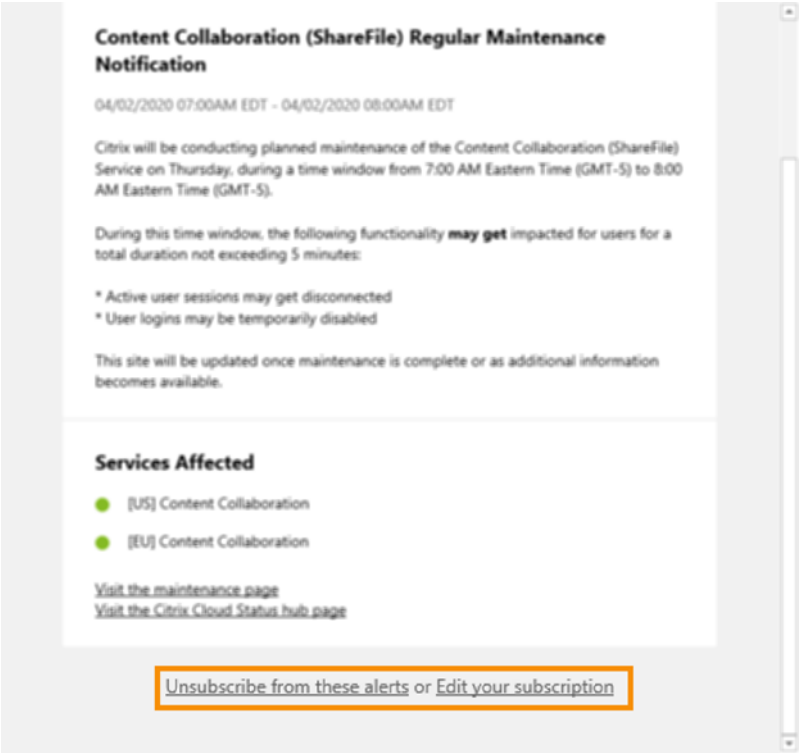
通知のサブスクリプションの解除

サブスクリプション方法に応じて、サブスクリプションを解除または変更するためのリンクは、受信する確認メッセージ（電話通知にサブスクライブする場合など）または各通知メッセージ（メール通知にサブスクライブする場合など）に含まれます。例:

- サブスクリプションオプション付きの電話通知:



- サブスクリプションオプション付きの通知メール:



すべての通知のサブスクリプションを解除し、すべてのサブスクリプション方法を削除するには:

1. サブスクリプション確認メッセージまたは既存の通知を見つけて、サブスクリプションを解除するリンクを選択します。一部のサブスクリプション方法では、サブスクリプションを編集またはキャンセルするために 1 つのリンクが提供される場合があります。
2. サブスクリプション方法に応じて、[**Edit Subscriptions**] ページで次のオプションのいずれかを使用します:
   - [**Remove all subscriptions**] を選択します。
   - [**Unsubscribe**]を選択します。[**Unsubscribe methods**]ページから、[**Remove all subscriptions**] を選択します。

特定のサブスクリプション方法のすべての通知からサブスクリプションを解除するには:

1. サブスクリプション確認メッセージまたは既存の通知を見つけて、サブスクリプションを解除するリンクを選択します。一部のサブスクリプション方法では、サブスクリプションを編集またはキャンセルするために 1 つのリンクが提供される場合があります。
2. サブスクリプション方法に応じて、[**Edit Subscriptions**] ページで次のオプションのいずれかを使用します:
   - 削除するサブスクリプション方法を選択します。サブスクリプションはすぐに削除されます。
   - [**Unsubscribe**] を選択します。[**Unsubscribe methods**] ページから、削除するサブスクリプション方法を選択します。サブスクリプションはすぐに削除されます。

サービス通知の変更

1. サブスクリプション確認メッセージまたは既存の通知を見つけて、サブスクリプションを編集するためのリンクを選択します。一部のサブスクリプション方法では、サブスクリプションを編集またはキャンセルするために 1 つのリンクが提供される場合があります。
2. [**Edit Subscriptions**] ページから、管理するサブスクリプション方法を選択します。
3. [**Customizations**] ページで、必要に応じて通知を受け取るサービスを選択するか、通知を不要にするサービスをオフします。
4. [保存] を選択します。

Citrix Cloud サポートフォーラム

Citrix Cloud サポートフォーラムでは、ヘルプを要求したり、フィードバックや改善案を送信したり、他のユーザーの会話を表示したり、トピックを作成したりできます。

Citrix のサポートスタッフメンバーはこれらのフォーラムを追跡し、質問に回答します。他の Citrix Cloud コミュニティのメンバーも、支援を提供したりディスカッションに参加することがあります。

フォーラムのトピックを閲覧する場合、サインインする必要はありません。ただし、投稿したり、トピックに返信するためには、サインインが必要です。サインインするには、既存の Citrix アカウント資格情報を使用するか、Citrix Cloud アカウントの作成時に指定したメールアドレスとパスワードを使用してください。新しい Citrix アカウントを作成するには、アカウントの作成またはリクエストに移動します。

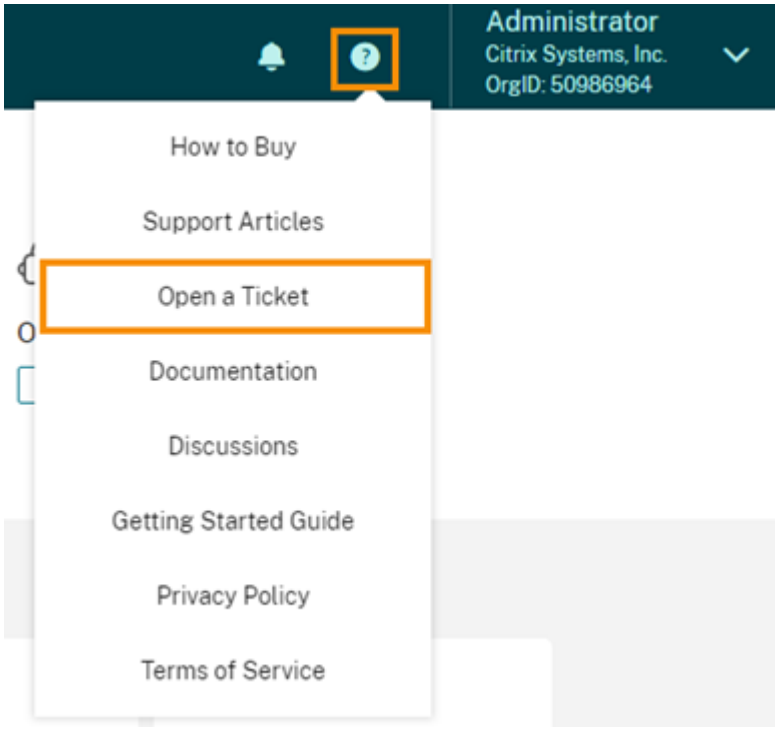
テクニカルサポート

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。

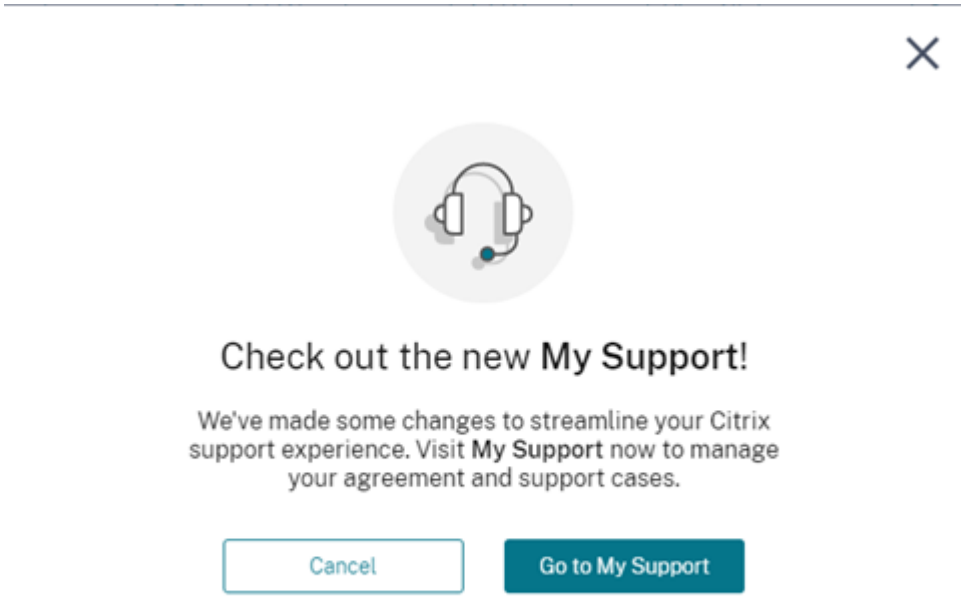
Support Knowledge Center にアクセスするには、https://support.citrix.com/case/manageに移動します。

または、Citrix Cloud の場合:

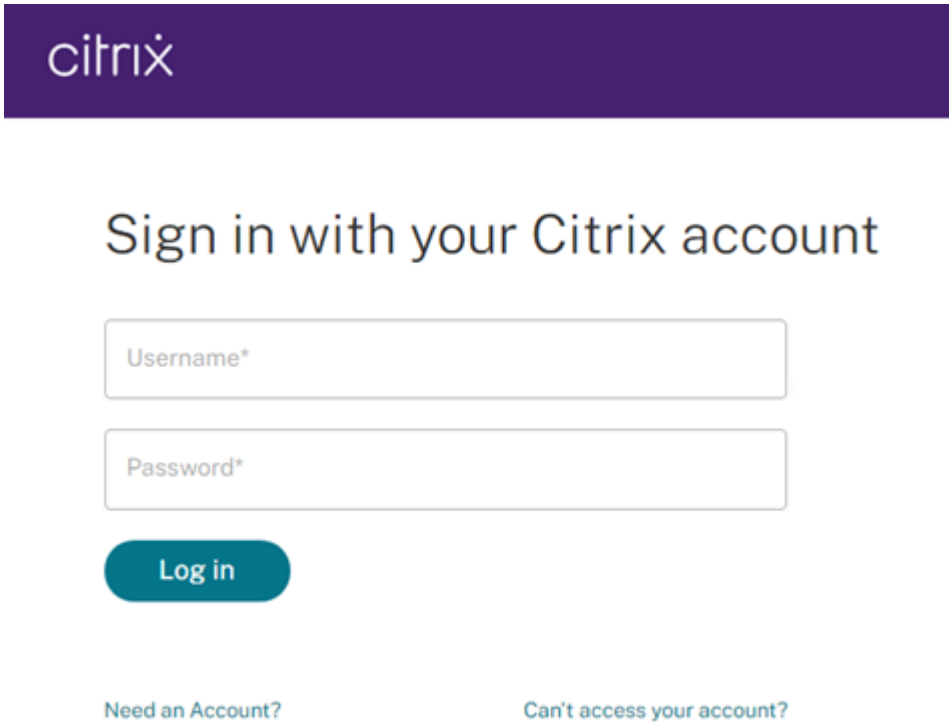
1. 画面の右上にある [ヘルプ] アイコンを選択します



2. ［チケットを開く］**>** ［**My Support** に移動］の順に選択します。

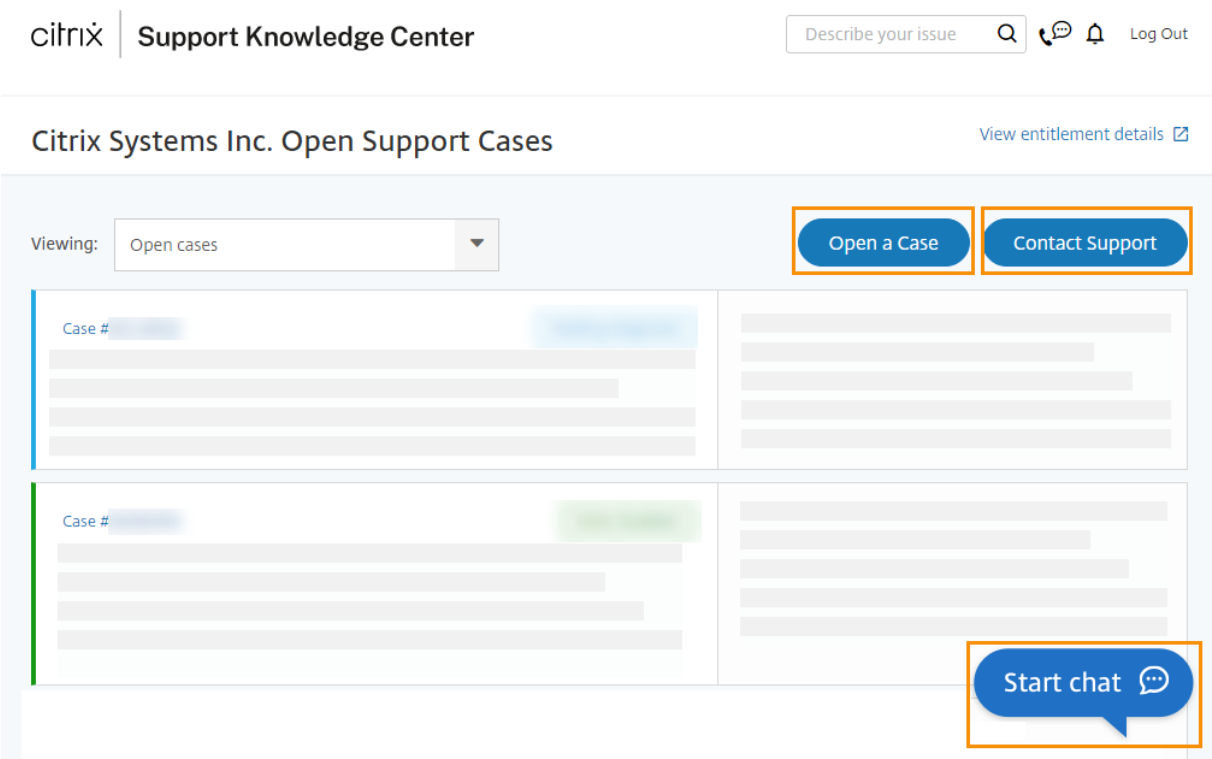


3. Citrix アカウントでサインイン



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:［ケースを開く］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地域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。



サポート記事とドキュメント

Citrix Cloud を活用し、シトリックス製品で発生する可能性のある問題を解決するために、十分な製品とサポートコンテンツが用意されています。

教育リソース

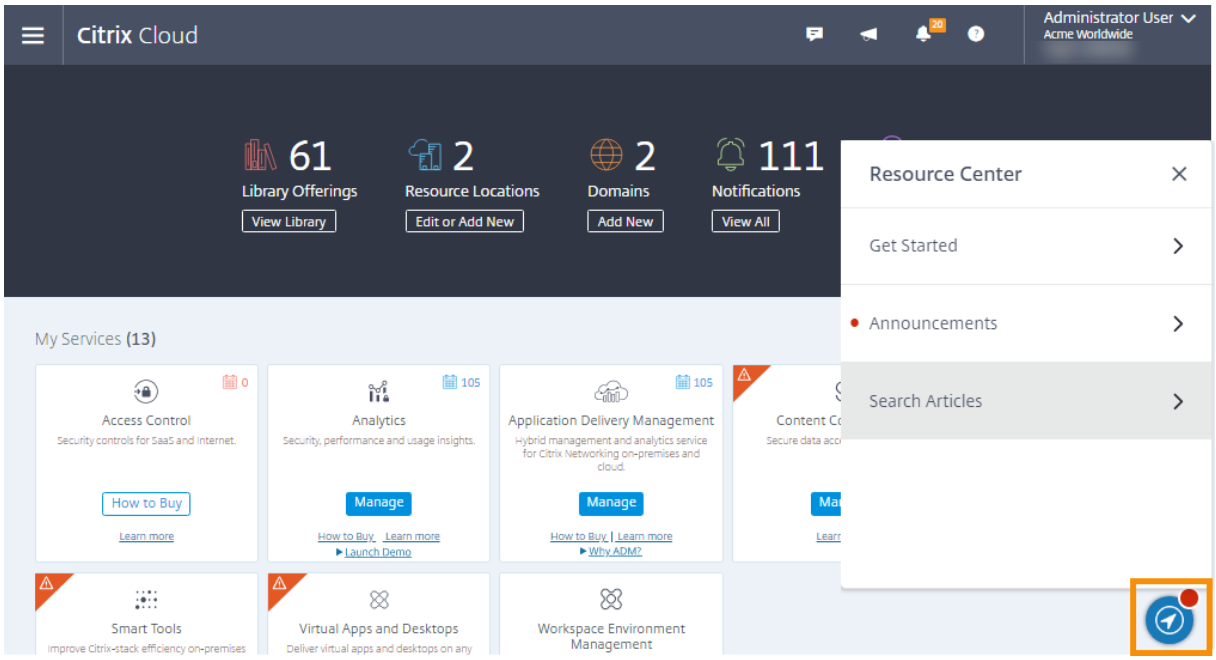
Citrix Cloud Learning Series ポータルには、Citrix Cloud とそのサービスを導入して実行するための教育モジュールがあります。概要から、計画と構築のサービスまで、すべてのモジュールを順番に確認できます。次のコースでクラウドの旅を始めましょう:

- Citrix Cloud の基礎
- Citrix ID と認証の概要
- StoreFront から Workspace への移行

Citrix Education 動画ライブラリでは、主要な展開タスクと、Citrix Cloud サービスで使用するコンポーネントのトラブルシューティングについて説明したオンライン動画レッスンを提供しています。Cloud Connector のインストールや VDA の登録、およびこれらのコンポーネントのトラブルシューティングなどのタスクに関する詳細をご覧ください。

Citrix Cloud リソースセンター

Citrix Cloud リソースセンターは、Citrix Cloud の使用開始、機能の詳細、問題解決のための検索に役立ちます。ページの右下にある青いコンパスアイコンをクリックします。この機能は、Citrix Cloud プラットフォーム、Virtual Apps and Desktops、Application Delivery Management サービスで利用できます。



- 開始：現在使用しているサービスに固有の主なタスクについて、簡単なガイド付きのチュートリアルを提供します。また、サービス機能の詳細を学び、エンドユーザーが活用できるようにセットアップするためのトレーニングおよび登録用リソースへのリンクもあります。
- お知らせ：新しくリリースされた機能の通知と、重要なシトリックスからのお知らせへのリンクを提供します。機能の通知を選択すると、機能の簡単なガイド付きチュートリアルが表示されます。
- 記事を検索：一般的なタスクに関する製品ドキュメントと Knowledge Center 記事の一覧を提供し、Citrix Cloud 内から多くの記事を見つけるのに役立ちます。[**How do I...**] ボックスに検索ワードを入れて、使用中のサービスごとに絞り込んだ記事の一覧を表示します。通常、サポート記事が一覧の最初に表示され、その後に製品ドキュメント記事が続きます。

Citrix Tech Zone

Citrix Tech Zoneには、Citrix Cloud およびそのほかのシトリックス製品の詳細を知るために役立つ情報が含まれています。ここで、Citrix テクノロジの設計、構築、展開に関する識見を提供するリファレンスアーキテクチャ、図、ビデオ、技術資料を参照できます。

サードパーティ通知

June 15, 2021

- Citrix Cloud サードパーティ通知（PDF）
- Citrix Analytics Service サードパーティ通知（PDF）
- Virtual Apps and Desktops サードパーティ通知（PDF）
- Virtual Apps and Desktops Standard for Azure サードパーティ通知（PDF）
- Citrix ShareFile Sync for Mac サードパーティ通知（PDF）
- Citrix ShareFile Sync for Windows サードパーティ通知（PDF）
- Secure Browser サービス（PDF）
- Citrix Endpoint Management サードパーティ通知（PDF）
- Citrix Cloud Linux VDA Image Service サードパーティ通知（PDF）
- クラウドサービス用のコネクタアプライアンスのサードパーティ通知（PDF）
- Citrix マイクロアプリサービスのサードパーティ製品についての通知（PDF）

Citrix Cloud へのサインアップ

July 29, 2021

ここでは、Citrix Cloud 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。

> ヒント：
>
> 「Citrix Cloud の基礎」コースの「Citrix Cloud の利用を開始する」教育モジュールには、この記事で説明しているタスクについて説明した短い動画があります。また、このコースをすべて履修すると、Citrix Cloud、組織にとってのメリット、および Citrix Cloud サービスで対処できる重要なユースケースの理解のために必要なしっかりとした基礎を身につけることができます。

Citrix アカウントとは何ですか**?**

Citrix アカウント（Citrix.com アカウントまたは My Citrix アカウント）では、購入したライセンスへのアクセスを管理できます。Citrix アカウントでは、組織 ID（OrgID）が一意の識別子として使用されます。Citrix アカウントにアクセスするには、ユーザー名（Web ログイン）またはアカウントにリンクされているメールアドレスでhttps://www.citrix.comにログインします。

> 重要：
>
> ユーザー名は単一で一意の Citrix アカウントに割り当てられますが、メールアドレスは複数の Citrix アカウントに割り当てることができます。

OrgID とは何ですか**?**

OrgID は、Citrix 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。そのため企業には通常、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、単一の会社が複数の OrgID を所有できます。

特定の OrgID は定期的にクリーンアップされ、必要な場合、重複分がマージされます。有効かつアクティブな OrgID とマージする OrgID がある場合は、マージする OrgID をシトリックスカスタマーサポートに連絡することができます。

> 注:
>
> 企業は資産の管理方法に基づいて OrgID を既に設定しているため、使用する OrgID や所有する OrgID の数が不明の場合は、お客様の会社の IT 部門またはシトリックス管理者にお問い合わせください。必要な場合は、シトリックスカスタマーサポートが OrgID の検索をお手伝いします。シトリックスカスタマーサポート（https://www.citrix.com/contact/support.html）にお問い合わせください。

Citrix Cloud アカウントとは何ですか**?**

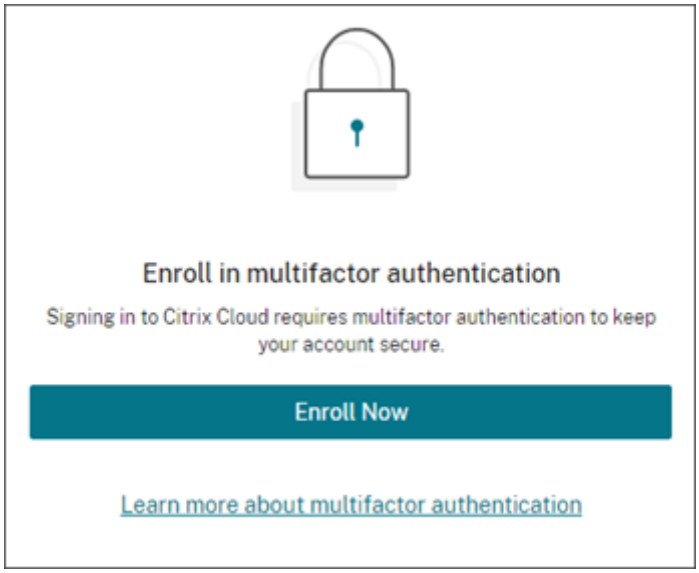
Citrix Cloud アカウントで 1 つまたは複数の Citrix Cloud サービスを使用して、アプリケーションとデータを安全に配信できます。Citrix Cloud アカウントは、Citrix アカウントと同様に OrgID によって一意に識別されます。組織が OrgID をセットアップした方法に基づいて、適切な Citrix Cloud アカウントを選択し、同じ OrgID を使用して購入と管理者のアクセスも実行できるようにすることが重要です。たとえば、OrgID 1234 を使用している会社の設計部門が Virtual Apps and Desktops をオンプレミスで使用している場合、Citrix Cloud を試用するには、OrgID 1234 の管理者が OrgID に関連付けられた Web ログインまたはメールアドレスを使用する必要があります。したがって、Virtual Apps and Desktops のサブスクリプションの購入を決定した場合、OrgID 1234 に発注でき、スムーズに製品版に移行できます。

> 重要:
>
> 特定の Citrix アカウントにアクセスできるユーザーが、その Citrix アカウントの OrgID に関連付けられている Citrix Cloud アカウントに自動的にアクセスできるようになるわけではありません。ユーザーが Citrix Cloud にアクセスできるようになると、サービスに影響を及ぼす可能性があるため、Citrix Cloud アカウントにアクセスするユーザーを管理することが重要です。

多要素認証の要件

Citrix Cloud アカウントを安全に保つために、Citrix Cloud ではすべてのお客様が多要素認証に登録する必要があります。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。

シトリックスの既存のお客様の場合、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入力すると、Citrix Cloud で登録を求めるプロンプトが表示されます。シトリックスを初めて使用する場合は、サインアッププロセス中に Citrix アカウントを作成した後、Citrix Cloud で登録を求めるプロンプトが表示されます。

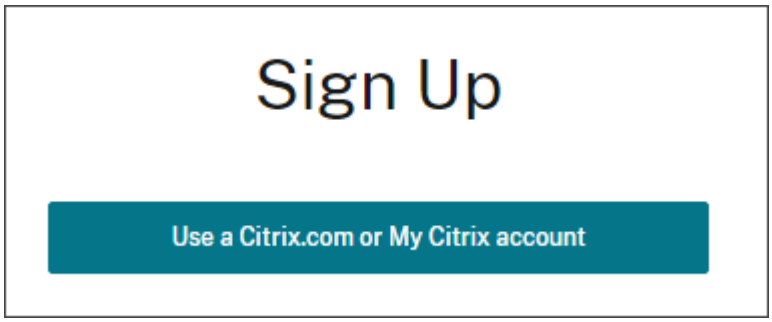


手順 **1**：登録ページにアクセスする

Web ブラウザーを使用して、https://onboarding.cloud.comにアクセスします。

シトリックスの既存のお客様であるか、**Citrix.com** または **My Citrix** アカウントをお持ちの場合

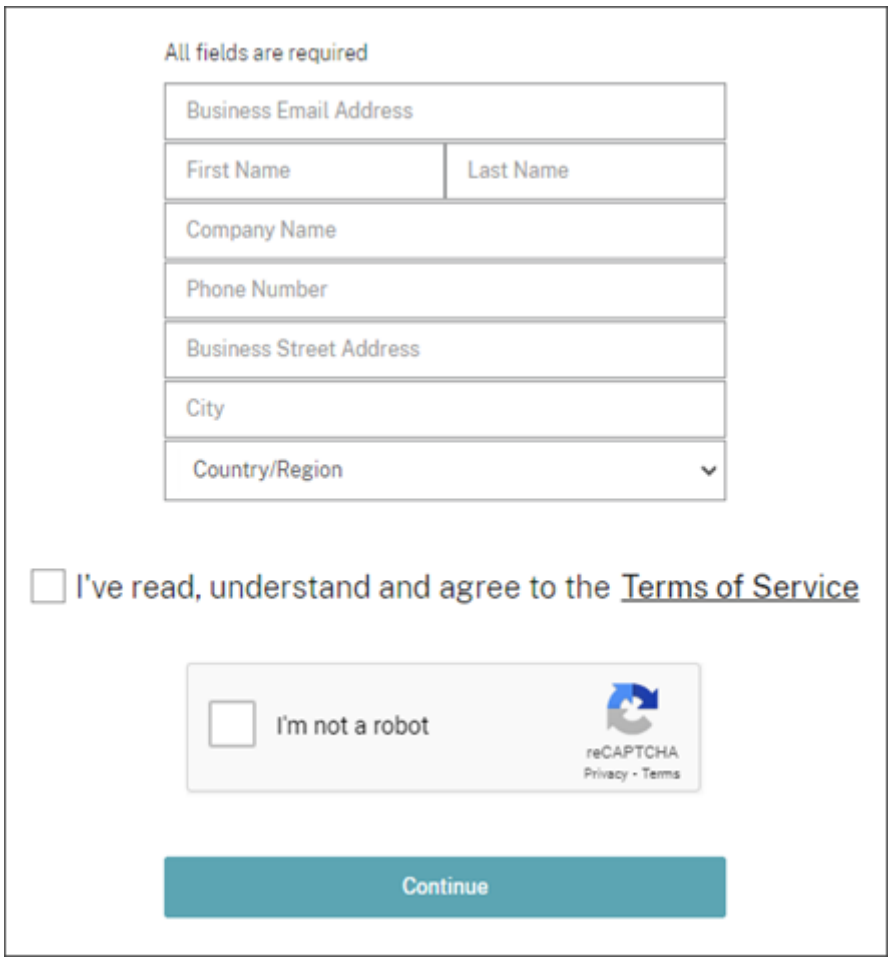
1. ［**Citrix.com** または **My Citrix** アカウントを使用］を選択します。



2. ユーザー名とパスワードを入力するか（Web ログイン）、Citrix.com アカウントに関連付けられているメールアドレスとパスワードを入力します。
3. 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。
4. この記事の「手順 5：多要素認証に登録する」で説明されているように、登録処理を完了します。

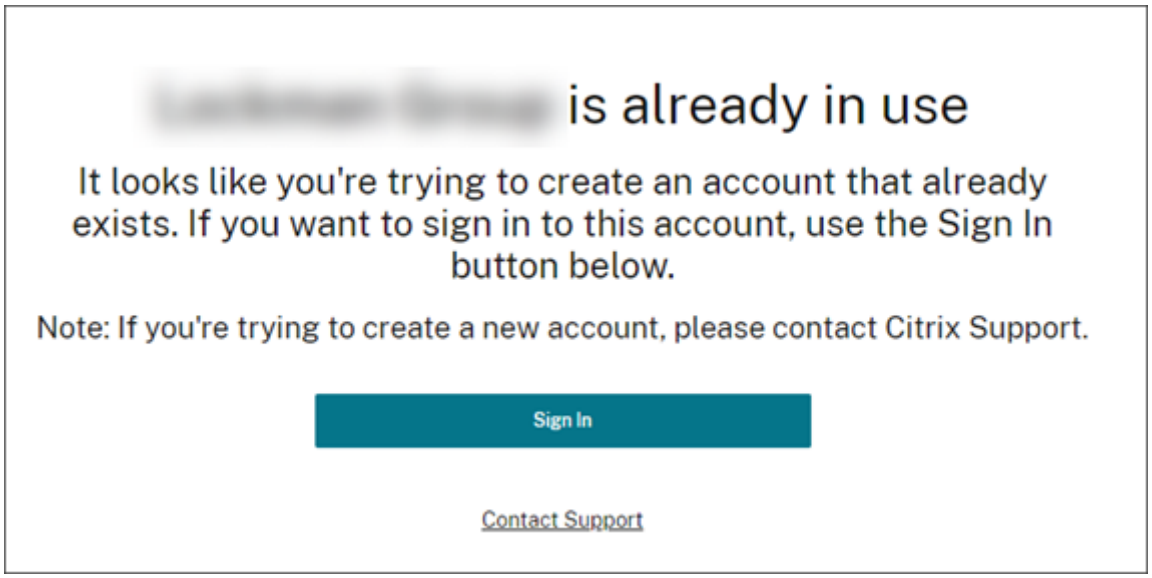
Citrix および **Citrix Cloud** を初めて使用する場合

フォームフィールドに入力し、［続行］を選択します。



会社のメールアドレスと会社の住所を使用するようにしてください。個人のメールアドレスまたは住所を使用すると、トライアルのリクエスト処理に時間がかかることがあります。

アカウントが既に使用中の場合

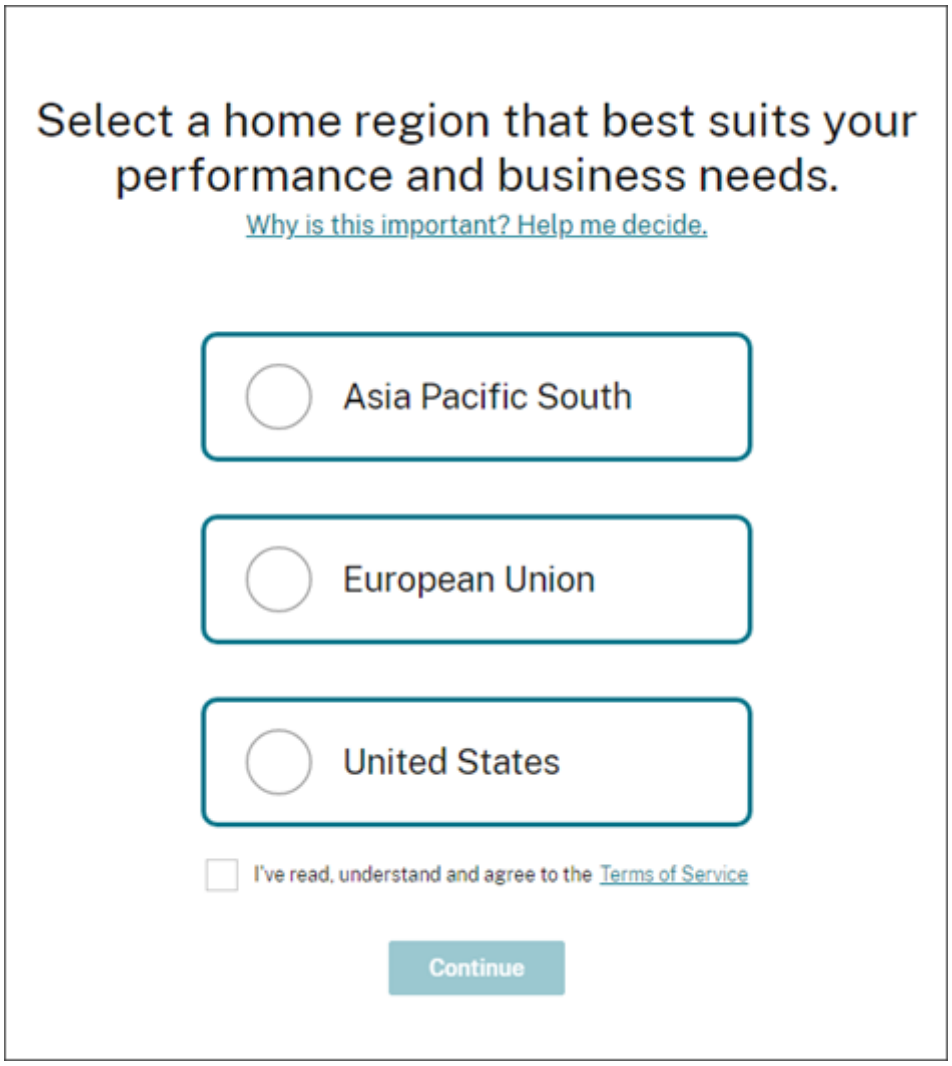


このメッセージが表示された場合、使用した Citrix アカウントの別の管理者が、既に Citrix Cloud アカウントを作成しています。

Citrix Cloud アカウントでは、管理者はサービスをより詳細に管理できるため、Citrix Cloud アカウントを作成する最初の管理者は、別の管理者が既に Citrix アカウントのメンバーであっても明示的にアクセス権を付与する必要があります。

［承認のリクエスト］を選択することで、そのアカウントのすべての既存管理者にリクエストの通知が送信されます。既存の管理者が組織を離れた場合は、シトリックスサポートにお問い合わせください。

手順 **2**：**Citrix Cloud** 地域を選択する

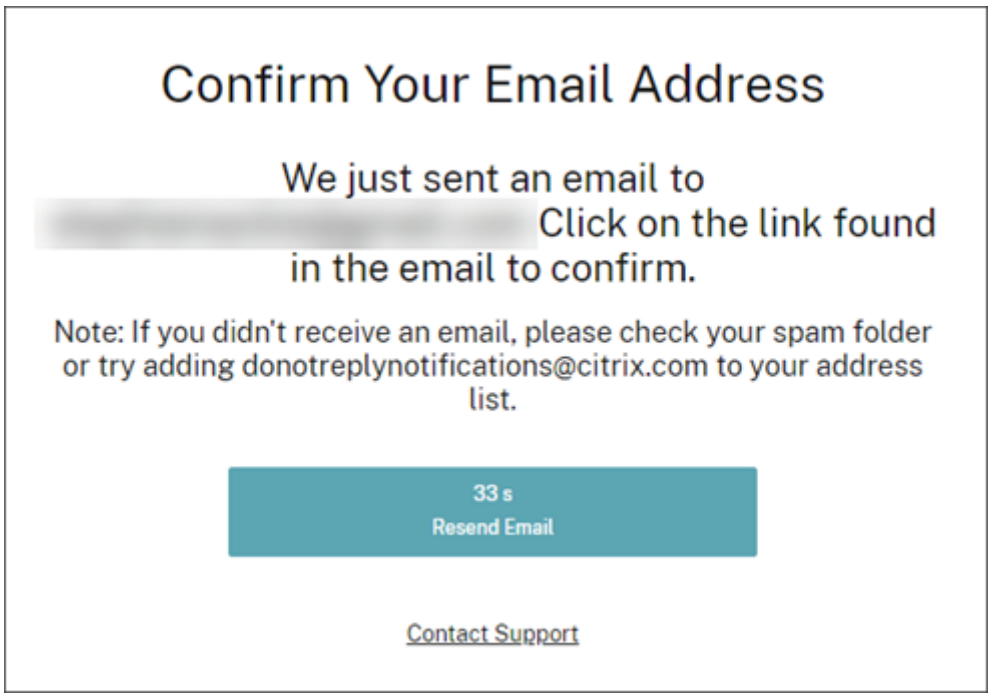


Citrix Cloud 地域は、Citrix Cloud サービスを提供するためのサービスとデータを操作、保存、複製できる地理的境界です。サービスの提供には、地域内の 1 つまたは複数の国（州や地方を含む）にある複数のパブリッククラウドまたはプライベートクラウドが使用されることがあります。Citrix Cloud 地域について詳しくは、「地理的な考慮事項」を参照してください。

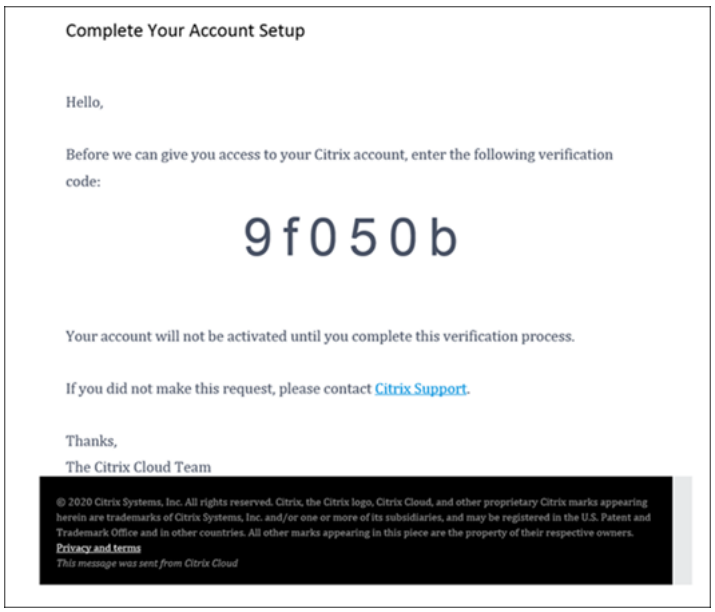
> 重要：
>
> 地域を選択した後、選択を元に戻したり変更したりすることはできません。

手順 **3**：メールアドレスを確認する

メールアドレスを確認していない場合は、確認するよう求められることがあります。



次に、Citrix Cloud から確認メールが送信されます。以下のようなメールを受信します:

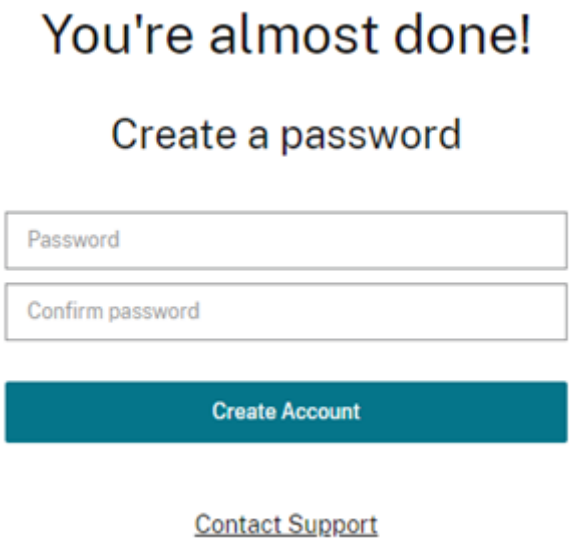


受信した確認メールでメールアドレスを確認した後、Citrix Cloud アカウントが有効になります。

手順 **4**: パスワードを選択する

> 注:
>
> Citrix Cloud では、Citrix アカウントを初めて作成する場合にのみ、パスワードを選択するように求められます。

Citrix Cloud のパスワードを入力して確認し、アカウントの作成を完了します。

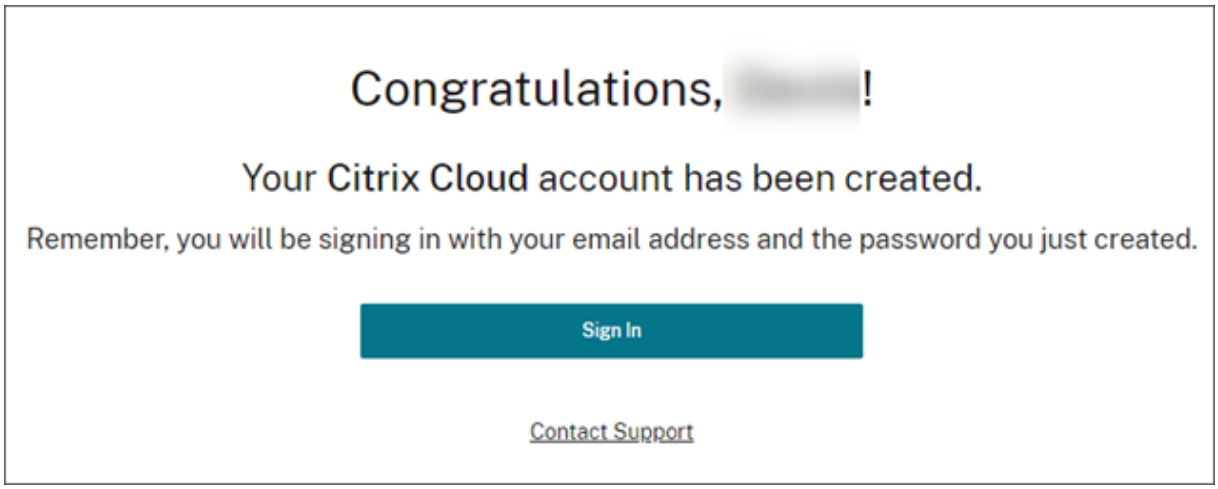


選択したパスワードは大文字と小文字が区別され、以下がすべて含まれている必要があります:

- 長さが 8 文字以上
- 1 つ以上の大文字
- 1 つ以上の数字
- 1 つの記号: ! @ # $ % ^ * ? + = -

有効なパスワードに辞書の単語を含めることはできません。パスワードを選択した後、そのパスワードが十分に複雑ではない、または既知の侵害されたパスワードのデータベースにあると判断した場合、Citrix Cloud は次回サインインするときにパスワードの変更を要求する場合があります。詳しくは、「パスワードを変更する」を参照してください。

アカウントの作成後、Citrix Cloud にサインインできます。



手順 **5**：多要素認証に登録する

管理者アカウントの安全を確保するため、Citrix Cloud ではサインイン時に多要素認証を使用するよう要求されます。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。

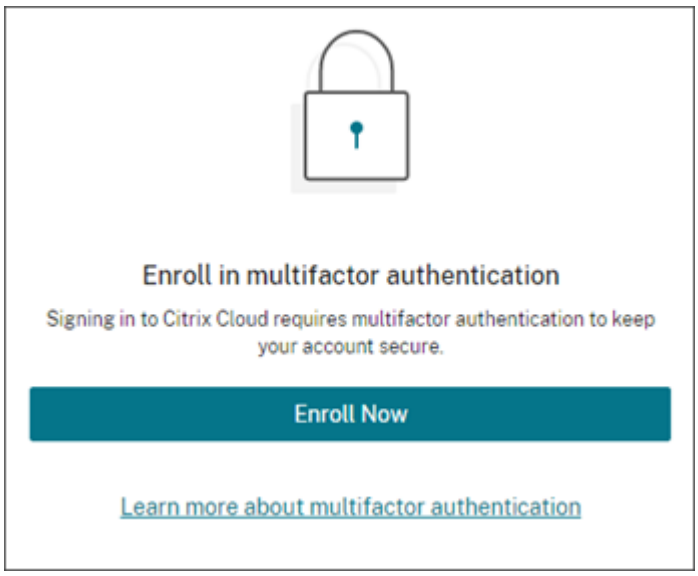
多要素認証に登録していない場合、サインイン時に登録するよう Citrix Cloud から求められます。

登録時に、Citrix Cloud は QR コードとキーを提示します。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 は、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に 1 回のみ使用できるバックアップコードも生成します。

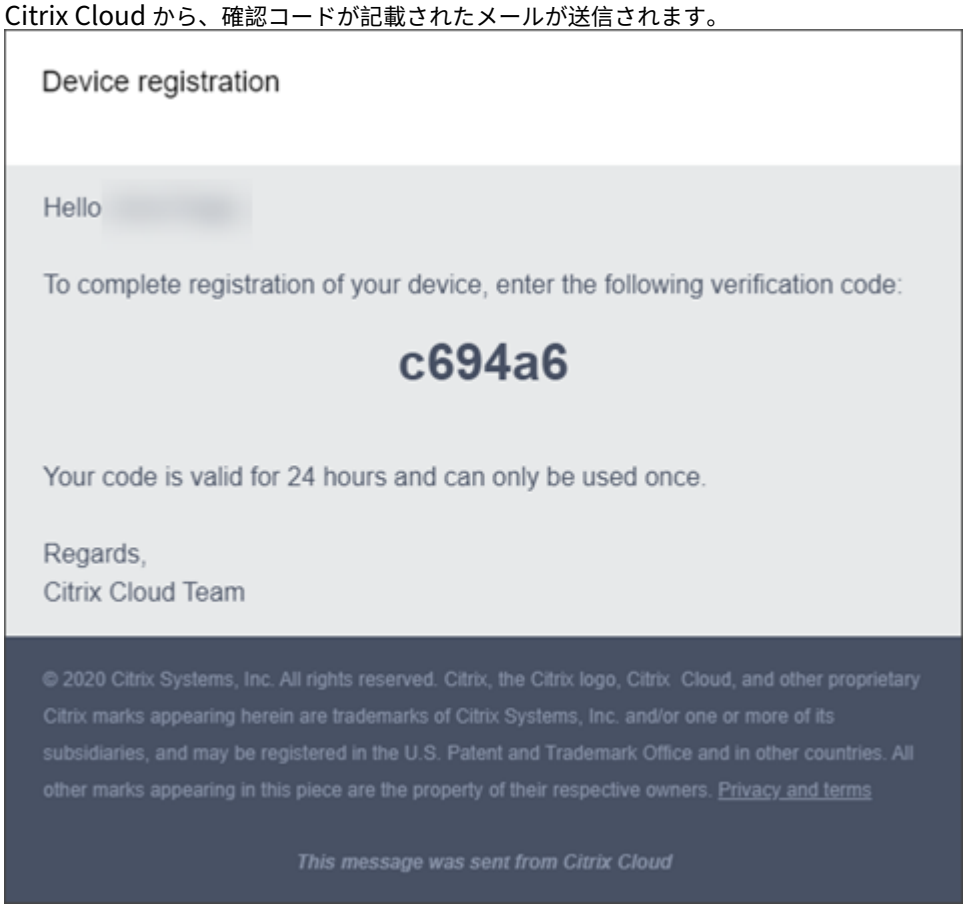
> 注:
>
> - Citrix Cloud にサインインするときは、Citrix Cloud のサインインページがhttps://accounts.cloud.comに表示されていることを確認してください。別の URL（`https://accounts-internal.cloud.com`など）を使用して Citrix Cloud にサインインすると、多要素認証の登録が失敗します。
> - Citrix Cloud 経由で多要素認証に登録できるのは、Citrix ID プロバイダーの管理者のみです。Azure AD を使用して Citrix Cloud 管理者を管理する場合、Azure 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 社のサイトでAzure 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 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。あとから別のデバイスを登録すると、Citrix Cloud 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、「多要素認証用のデバイスを変更する」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

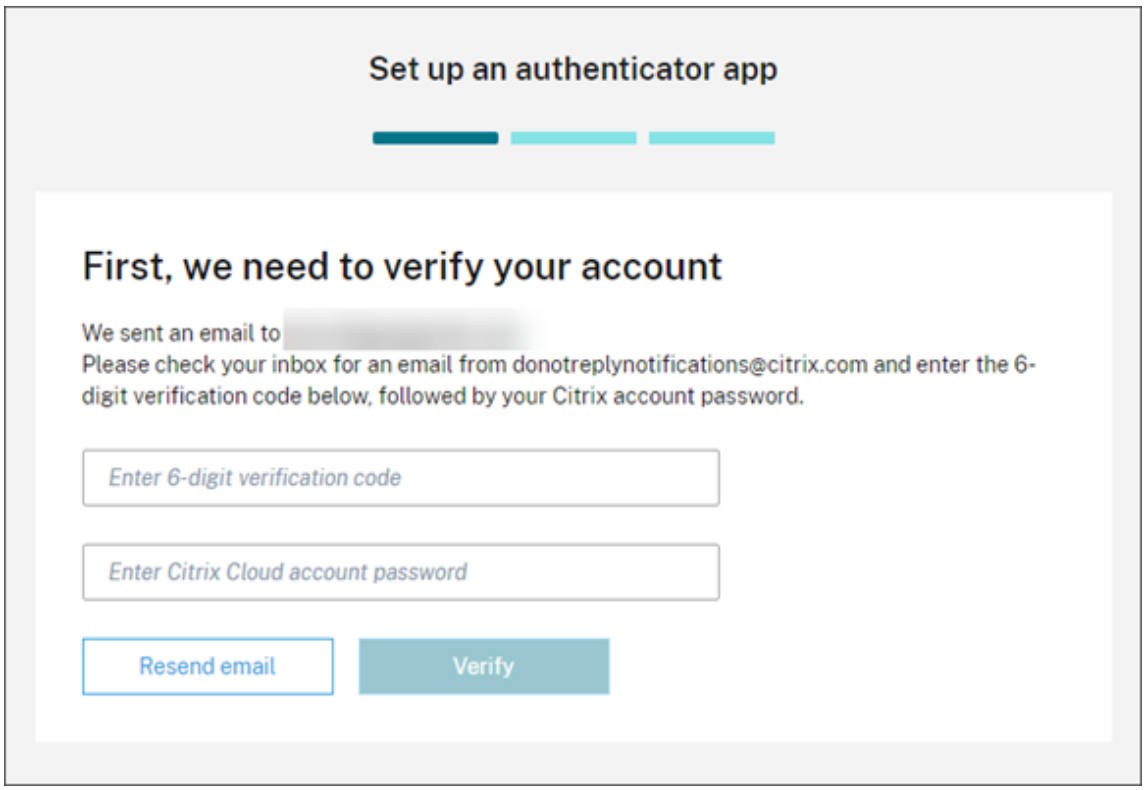
1. https://citrix.cloud.comにアクセスして、URL がhttps://accounts.cloud.comにリダイレクトされるかを検証します。Citrix Cloud の資格情報でサインインします。
2. 多要素認証に登録するよう求められたら、［今すぐ登録］を選択します。



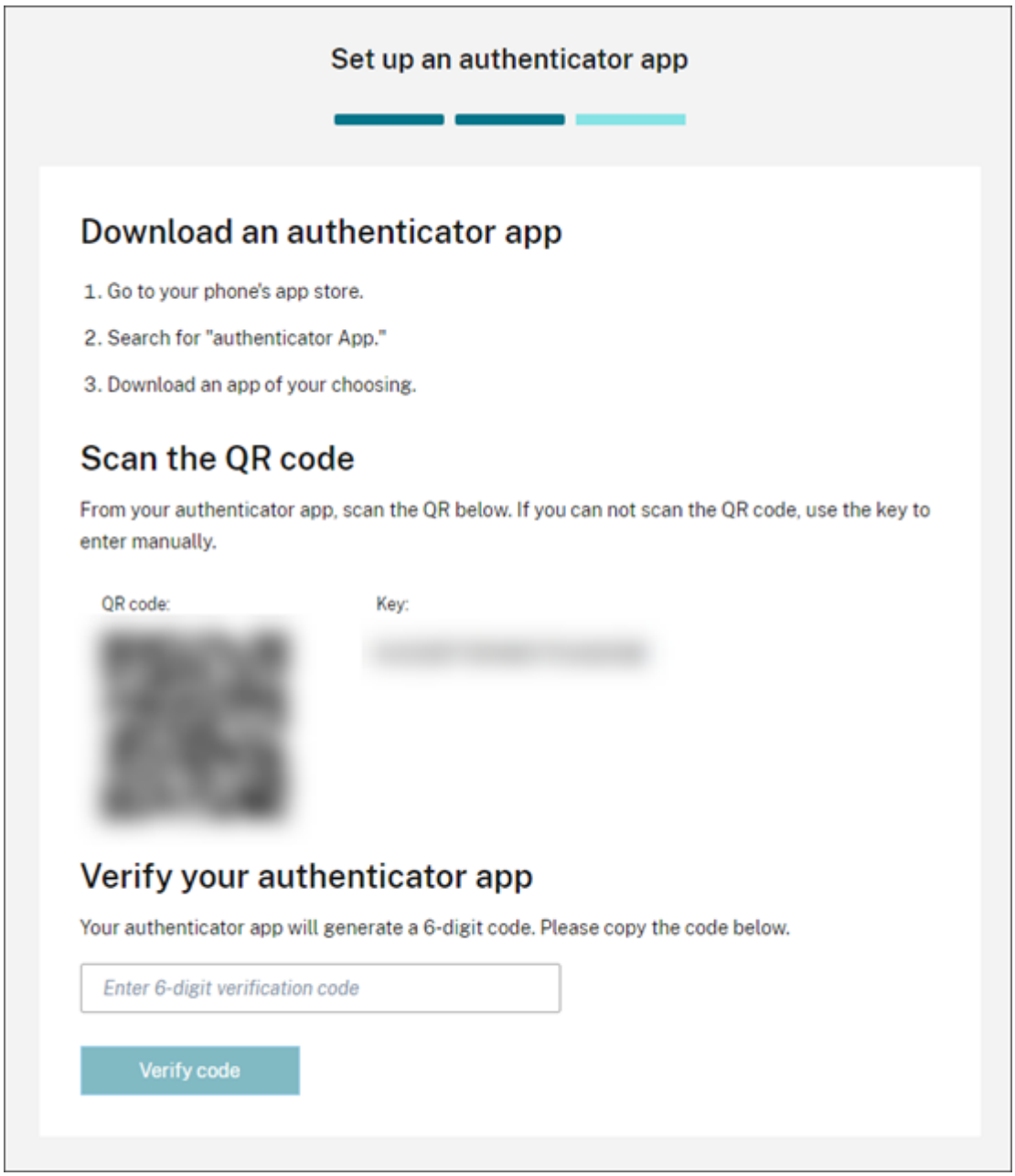
Citrix Cloud から、確認コードが記載されたメールが送信されます。



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

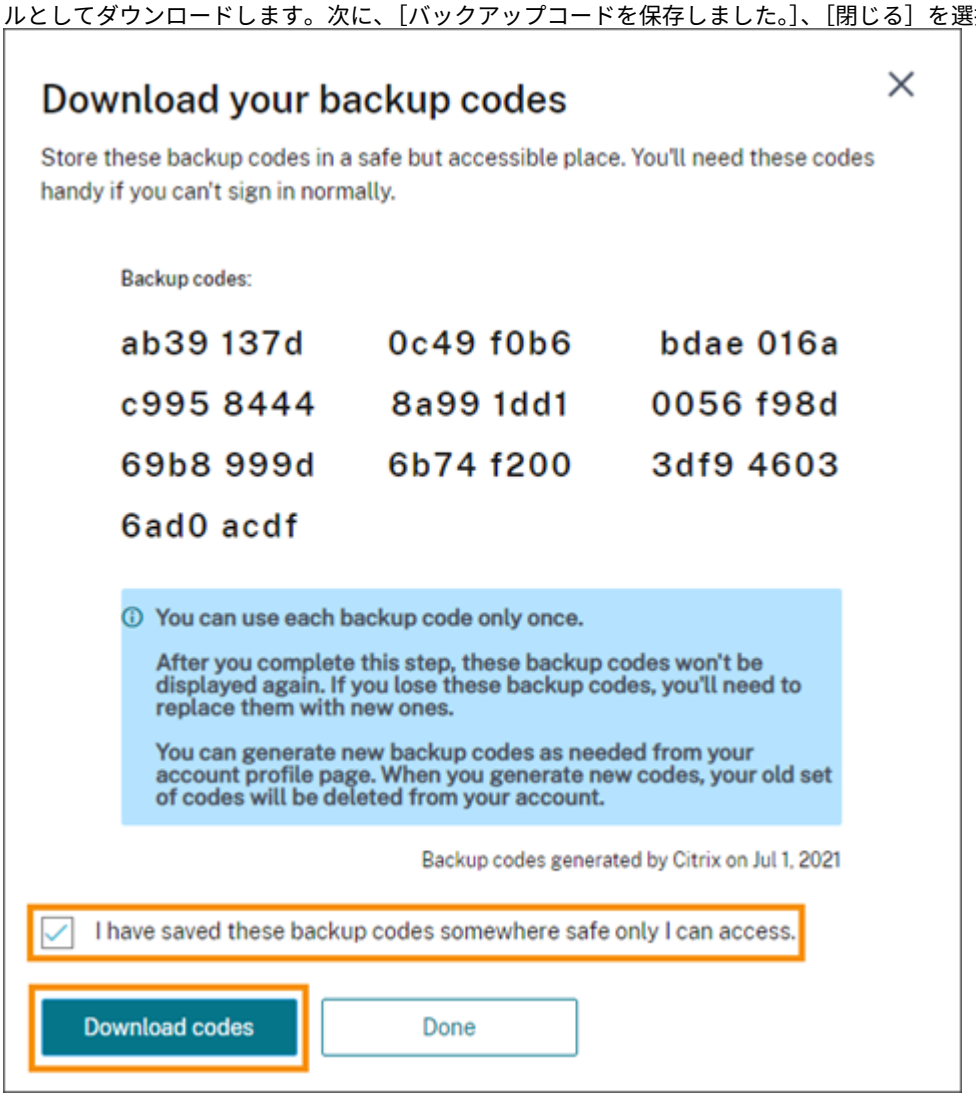


4. 認証アプリで QR コードをスキャンするか、キーを手動で入力します。認証アプリが Citrix Cloud のエントリを表示し、6 桁のコードを生成します。



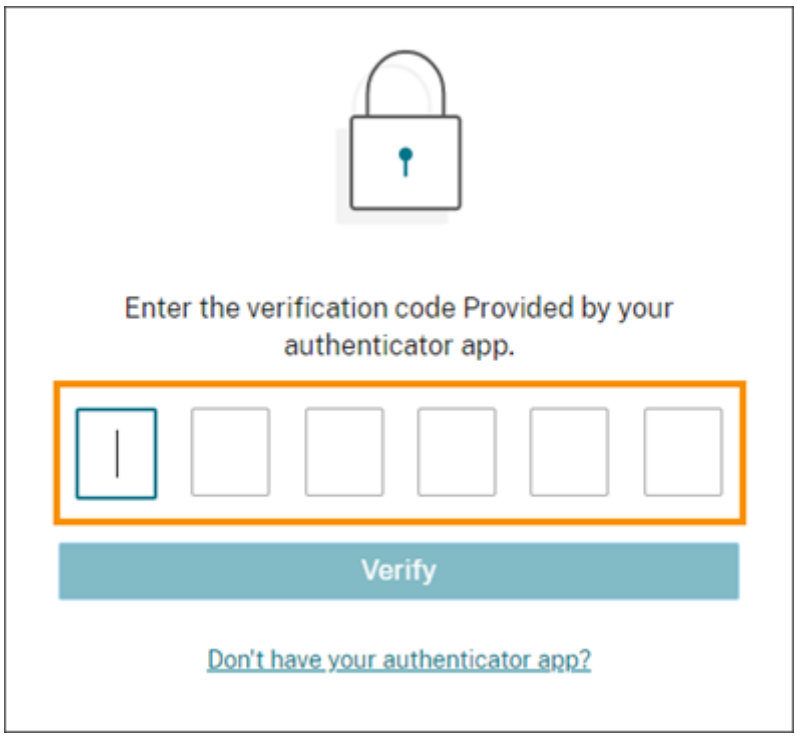
5. [認証アプリを確認する] で認証アプリのコードを入力して [コードを確認する] を選択します。
6. デバイスを紛失した場合、または認証アプリを使用できない場合のために、以下のアカウントの復旧方法を構成します:
   - 復旧用の電話番号 (必須): [復旧用の電話番号を追加する] を選択して、Citrix サポートがユーザーの本人確認のために連絡できる電話番号を入力します。Citrix サポートは、サインインのサポートに必要な場合にのみこの電話番号を使用します。固定電話の電話番号を使用することをお勧めします。
   - バックアップコード (必須): 認証アプリを使用できない場合のサインインに役立つ 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 管理者の資格情報でサインインすると、Citrix Cloud は認証アプリから確認コードの入力を要求します。



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、リカバリ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。

- 多要素認証用のデバイスを変更する
- 確認方法を管理する。

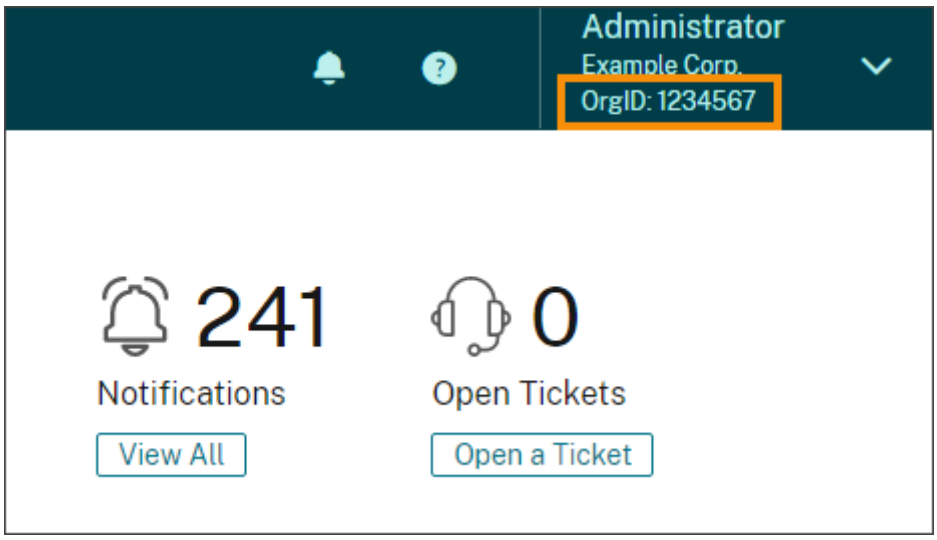
手順 6：OrgID を確認して管理者を招待する

Citrix Cloud アカウントをセットアップできました。Citrix Cloud を使用する前に、OrgID を確認し、Citrix Cloud アカウントをともに管理する他の管理者を招待してください。

アカウントの **OrgID** を確認する

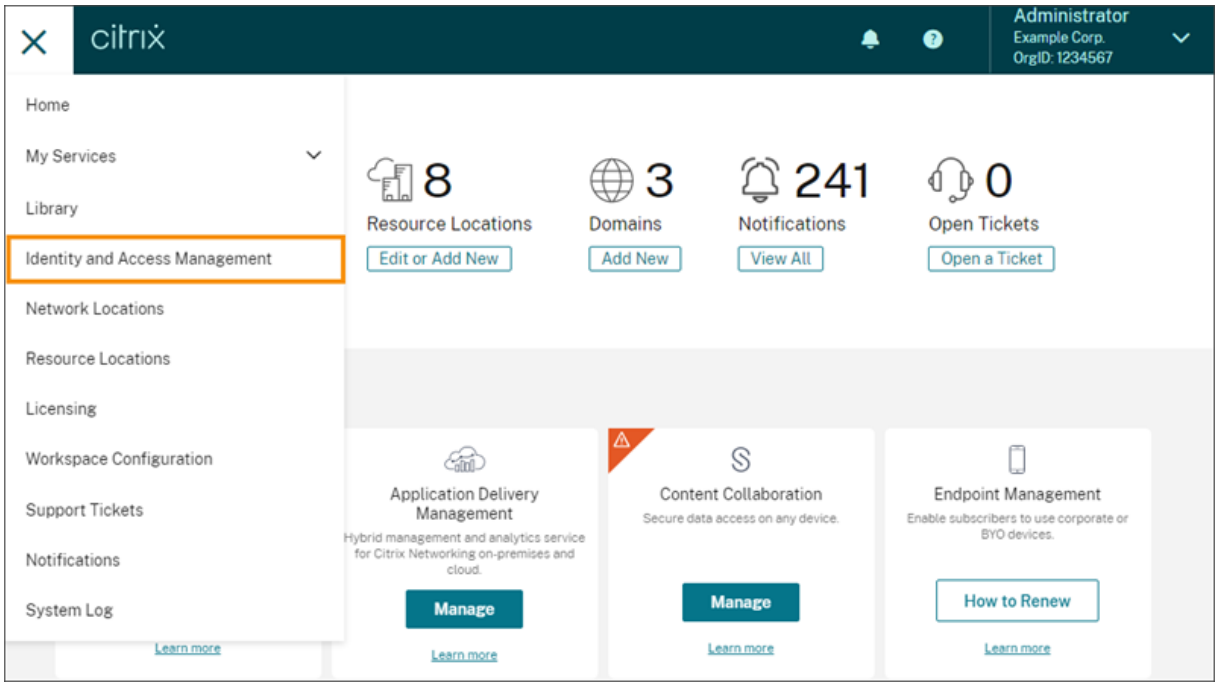
アカウントの OrgID が注文に使用する OrgID と一致していることを確認してください。Citrix Cloud のメリットの 1 つは、サービス（Virtual Apps and Desktops サービスなど）を試用してから購入する場合、同じアカウントを使用できるため、トライアルで作成したすべての設定が購入後も保持されることです。つまり、正しい OrgID でトライアルを開始することは、購入時の手間を省くことになります。

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



他の管理者を招待する

他の管理者が Citrix.com の Citrix アカウントにアクセスできる場合でも、Citrix Cloud アカウントへの招待が必要であることに注意してください。このためには、Citrix Cloud 管理コンソールで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。詳しくは、「Citrix Cloud アカウントに管理者を追加する」を参照してください。



手順 **7**: **Citrix Cloud** サービスのトライアルをリクエストする

トライアルは、必要なオンプレミスのインフラストラクチャまたはパブリッククラウド、アプリケーション、Microsoft Active Directory でのテスト用に設計されています。サービス、ワークスペース、リソースの場所をセッ

トアップおよび構成できます。

トライアル期間中、サブスクリプションパッケージの購入を決定した場合は、いつでも購入することができます。作成した設定はすべて保存され、継続して使用できます。

トライアルをリクエストするには、試したいサービスで［トライアルのリクエスト］をクリックします。詳しくは、「Citrix Cloud サービスのトライアル」を参照してください。

地理的な考慮事項

September 17, 2021

この記事では、Citrix Cloud が使用する商用リージョンと、各リージョン内での Citrix Cloud 商用サービスについて説明します。

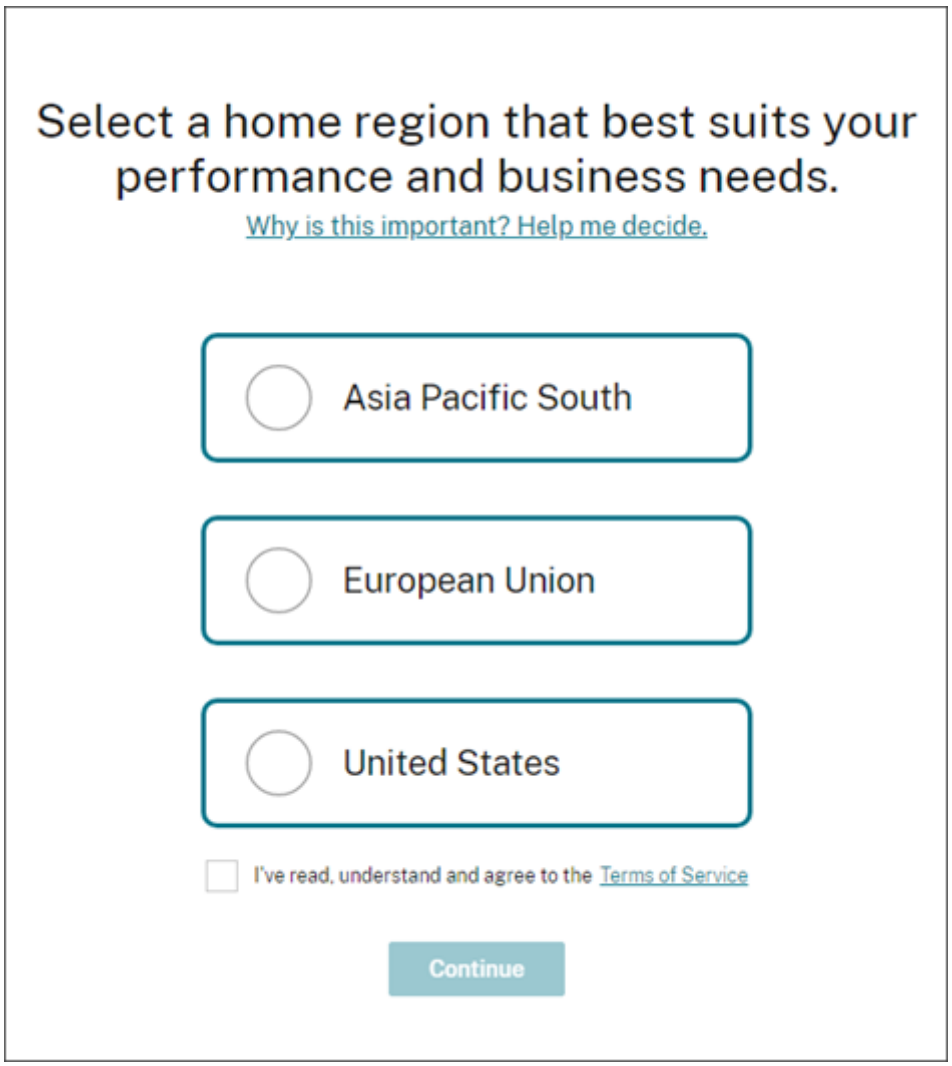
シトリックスの公共部門および専用クラウドプラットフォームの地理的なリージョンとサービスについて詳しくは、この記事の「シトリックスの他のクラウドプラットフォーム」を参照してください。

リージョンの選択

所属する組織が Citrix Cloud に参加した後、最初のサインインで、以下の地域から選択するよう求められます:

- 米国
- 欧州連合
- 南アジア太平洋

組織のユーザーおよびリソースの大半が所在しているリージョンを選択してください。



重要な注意事項:

- リージョンを選択できるのは、組織がサービスに参加した最初の 1 回のみです。後から地域を変更することはできません。
- あるリージョンで他のリージョンのサービスを使用しても、パフォーマンスへの影響はほとんどありません。Citrix Cloud サービスは、グローバルでの使用を前提に設計されています。たとえば、オーストラリアにユーザーが存在し、コネクタがある米国の顧客は、遅延に関して最小限の影響しか受けません。
- Citrix Cloud がサポートするリージョンにいない場合でも、Citrix Cloud を使用できます。単純に、ユーザーの大半がいる場所から最も近いリージョン、またはデータの整合性を保護するために最適な制御機能を提供するリージョンを選択してください。

地域に格納されているデータの種類

地域には、使用環境に関する特定のメタデータが格納されています。例:

- Citrix Cloud 管理者の詳細（名前、ユーザー名、パスワードなど）。

- インストールするコネクタによって選択した地域経由で送信されたトラフィックのデータ。たとえば、（オンプレミスで管理されている、またはパブリッククラウドベンダーのサブスクリプション経由の）ドメインコントローラーを使用した認証データは選択した地域にとどまります。
- ユーザーをライブラリサービスに割り当てるためのデータ。たとえば、Microsoft Office をユーザー向けのサービスとしてライブラリに追加し、5 ユーザーを利用者としてサービスに追加すると、各ユーザーをそのサービスに関連付けるデータ（ユーザー名やドメイン名など）は地域に格納されます。
- 地域で使用できるサービスのユーザーに関するデータ。たとえば、所在のリージョンで Endpoint Management を使用すると、名前、住所、電話番号などのデータはそのリージョンに格納されます。

各地域でのサービスの利用

組織で選択した地域にかかわらず、すべてのサービスがグローバルで利用可能です。また、サービスを実行するために、必要に応じてシトリックスのアフィリエイトまたはサブプロセッサによってデータがグローバルに処理される場合があります。Virtual Apps and Desktops サービスなどの特定のサービスには、地域専用のインスタンスがあります。ただし、一部のサービスは、米国ベースのインスタンスのみを利用できます。

組織用として選択したリージョンでサービスが使用できない場合、必要に応じて特定の情報（認証データなど）がリージョン間で転送されることがあります。

サービスがグローバルで複製されると、そのサービスのすべてのデータはすべての地域に格納されます。

サービス	米国	EU	南アジア太平洋
Citrix Cloud コントロールプレーン	はい	はい	はい
Citrix Analytics	はい	はい	いいえ（米国地域の使用が必須）
Citrix Application Delivery Management	はい	はい	はい
Citrix Content Collaboration	はい***	はい***	いいえ - 米国または EU から選択**
Citrix Endpoint Management	はい**	はい**	はい**
SD-WAN Orchestrator	はい	はい	いいえ（米国地域の使用が必須）
Secure Browser サービス	はい*	はい*	はい*
Citrix Virtual Apps and Desktops サービス	はい*	はい*	はい*

サービス	米国	EU	南アジア太平洋
Citrix Virtual Apps and Desktops Standard for Azure	はい*	はい*	はい*
Citrix Virtual Apps Essentials	はい*	はい*	はい*
Citrix Virtual Desktops Essentials	はい*	はい*	はい*
Web App Firewall	はい	はい	いいえ（米国地域の使用が必須）
Citrix Workspace	はい*	はい*	はい*
Workspace Environment Management	はい	はい	はい
ネットワークサービス	はい	いいえ（米国地域の使用が必須）	いいえ（米国地域の使用が必須）
License Usage Insights（CSP のみ）	グローバルで複製	グローバルで複製	グローバルで複製
Citrix Gateway アクセスノード/POP	複数の WW ノード。最適なユーザーエクスペリエンスのために必要に応じてトラフィックをルーティング。	複数の WW ノード。最適なユーザーエクスペリエンスのために必要に応じてトラフィックをルーティング。	複数の WW ノード。最適なユーザーエクスペリエンスのために必要に応じてトラフィックをルーティング。
Citrix Secure Internet Access ノード/POP	複数の WW ノード。最適なユーザーエクスペリエンスのために必要に応じてトラフィックをルーティング。	複数の WW ノード。最適なユーザーエクスペリエンスのために必要に応じてトラフィックをルーティング。	複数の WW ノード。最適なユーザーエクスペリエンスのために必要に応じてトラフィックをルーティング。

* サービスは Citrix Cloud の地域を使用します。

** 複数の地域の複数の場所から選択します。本記事の「Endpoint Management サービスの場所」を参照してください。

***ストレージゾーンは複数の場所から選択できます。本記事の「Content Collaboration の場所とストレージゾーン」を参照してください。

各サービスで格納されるデータについて詳しくは、各サービスのセキュリティの技術概要を参照してください。

Endpoint Management サービスの場所

ホーム地域から次の Endpoint Management サービスの場所のいずれかを選択できます:

- 米国東部
- 米国西部
- 欧州西部
- 東南アジア
- シドニー

Secure Internet Access サービスの場所

最高のエクスペリエンスを保証するために、可用性とエンドユーザーの近接性に基づいて、次の Secure Internet Access サービスの場所にトラフィックがルーティングされます。

北米

- 米国、バージニア州スターリング
- カナダ、トロント
- 米国、カリフォルニア州ロサンゼルス
- 米国、カリフォルニア州アーバイン
- 米国、ワシントン州シアトル
- 米国、コロラド州デンバー
- 米国、ノースカロライナ州シャーロット
- 米国、テキサス州ダラス
- 米国、テキサス州アレン
- 米国、フロリダ州マイアミ
- 米国、イリノイ州シカゴ
- 米国、ニューヨーク州ニューヨーク
- 米国、マサチューセッツ州ボストン
- カナダ、バンクーバー

南米

- メキシコ、ケレタロ
- ブラジル、サンパウロ
- アルゼンチン、ブエノスアイレス
- コロンビア、ボゴタ

アジア太平洋

- オーストラリア、パース
- オーストラリア、シドニー
- 日本、東京
- シンガポール、シンガポール
- インド、ムンバイ
- インド、デリー

アフリカ

南アフリカ、ヨハネスブルグ

中東

- アラブ首長国連邦、ドバイ
- トルコ、イスタンブール

西ヨーロッパ

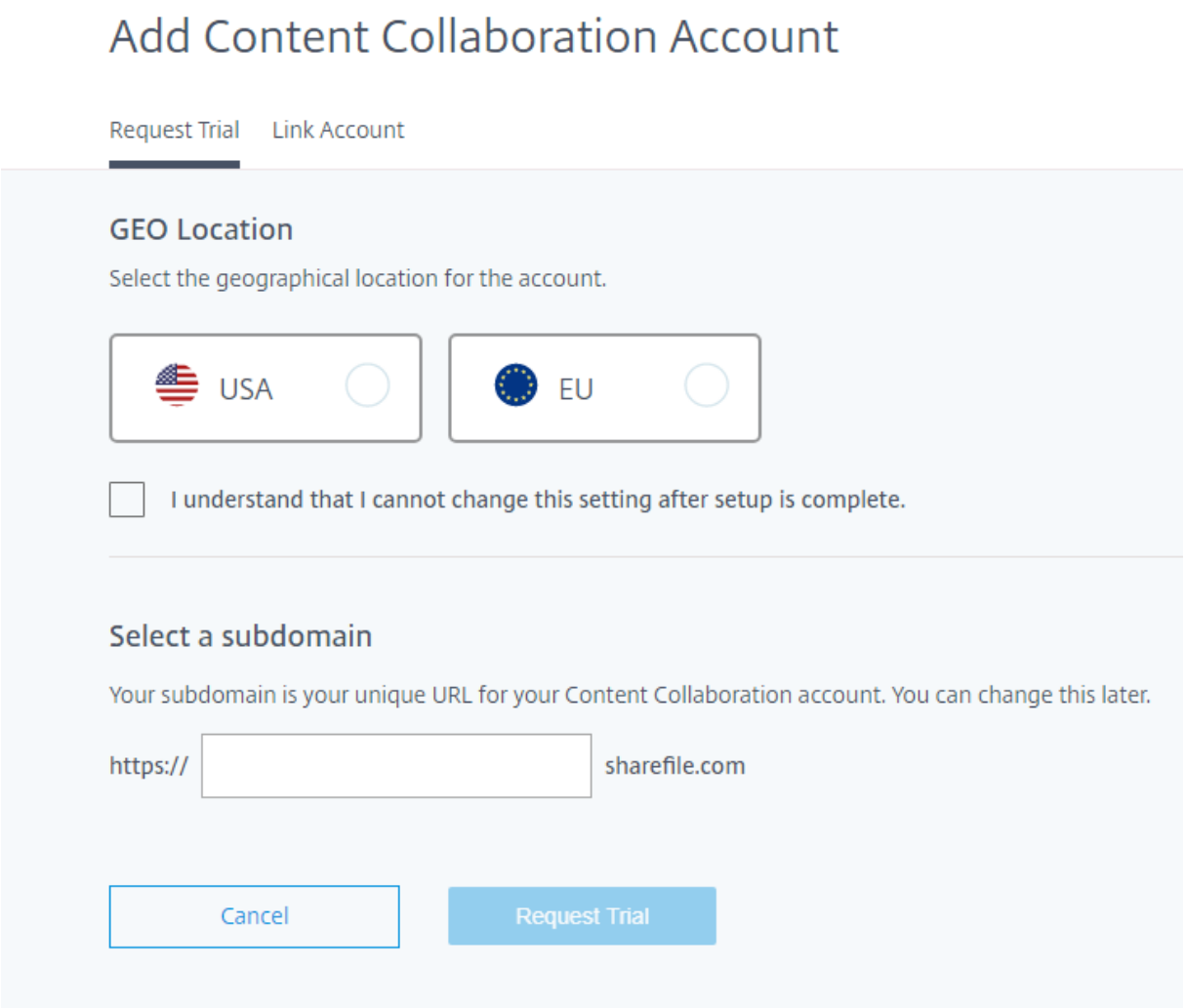
- 英国、ロンドン
- 英国、マンチェスター
- ドイツ、フランクフルト
- ドイツ、デュッセルドルフ
- ドイツ、マンハイム
- フランス、パリ

ヨーロッパ

- フィンランド、ヘルシンキ
- オランダ、アムステルダム
- スウェーデン、ストックホルム
- ポーランド、ワルシャワ
- スペイン、マドリッド
- ブルガリア、ソフィア
- スイス、チューリッヒ
- イタリア、ミラノ

Content Collaboration の場所とストレージゾーン

Citrix Cloud で Content Collaboration アカウントをセットアップする場合、米国または欧州の地域を選択できます。Content Collaboration の地域は、Citrix Cloud のホーム地域とは異なります。ただし、Citrix Cloud のホーム地域と同様、Content Collaboration アカウントを設定した後で Content Collaboration の地域を変更することはできません。



Citrix Cloud 内で作成された Content Collaboration アカウントの場合、デフォルトのストレージゾーンは最初は米国地域内です。

Citrix Cloud 以外で作成された ShareFile Enterprise アカウントの場合、ストレージゾーンは選択した地域（米国または EU のいずれか）にあります。Citrix Cloud にリンクしても、選択内容は変更されません。

Content Collaboration アカウントのセットアップ後、世界中のストレージゾーンを有効または無効にすることができ、新しいデフォルトゾーンを選択することもできます。また、Content Collaboration 管理コンソールで有効になっているストレージゾーンに基づいて、個別のユーザーまたはフォルダーにデフォルトの詳細を指定することもできます。次の場所から選択します：

- 日本
- シンガポール
- オーストラリア
- 欧州連合
- 米国 - 東部
- 米国 - 西部
- 米国 - 北西部
- ブラジル

シトリックスの他のクラウドプラットフォーム

Citrix Cloud に加えて、シトリックスは Citrix Cloud から分離された他のクラウドを提供しています。

Citrix Cloud Government

Citrix Cloud Government は、米国政府機関および米国内の他の公共部門の顧客が、規制およびコンプライアンスの要件に従って Citrix クラウドサービスを使用できるようにします。Citrix Cloud Government は、Citrix Cloud Government サービスを提供するためのサービスとデータを操作、保存、複製できる地理的境界です。サービスの提供には、米国内の 1 つまたは複数の州にある複数のパブリッククラウドまたはプライベートクラウドが使用されることがあります。

Citrix Cloud Government および提供されるサービスは、米国リージョンでのみ使用できます。

詳しくは、Citrix Cloud Government製品ドキュメントを参照してください。

Citrix Cloud Japan

Citrix Cloud Japan は、日本のお客様が、Citrix が管理する専用環境で Citrix Cloud サービスを使用できるようにします。Citrix Cloud Japan は、Citrix Cloud サービスを提供するためのサービスとデータを操作、保存、複製できる地理的境界です。

Citrix Cloud Japan および提供されるサービスは、日本でのみ使用できます。

詳しくは、Citrix Cloud Japan製品ドキュメントを参照してください。

Citrix Cloud のアカウントの確認

September 23, 2020

ユーザーは、Citrix Cloud アカウントの確認を求められることがあります。以下のような場合、メールの確認が必要になります:

- 長期間 Citrix Cloud にログインしていなかった。
- メールアドレスを変更した。
- 新しい管理者を Citrix Cloud に追加した。

よくある質問

確認の頻度はどのくらいですか? アカウントの確認は一度きりのイベントです。サインインのたびに確認されたり、アカウントで何か変更を行うたびに確認されたりすることはありません。頻繁に確認が行われる場合、シトリックステクニカルサポートにお問い合わせください。

アカウントに何か不具合が発生したのですか? いいえ。アカウントの確認を求められたからといって、アカウントや使用中の Citrix Cloud サービスに不具合が起こったというわけではありません。シトリックスがお客様の情報を安全に保護するための手順の一部にすぎません。

メールを受信していません。どのように対処すればよいですか? 次の手順を実行します:

- 差出人が「Citrix」のメールを受信トレイで探してください。
- 受信トレイにない場合、フォルダーを検索してください。迷惑メールフィルターやメールルールによってメールが迷惑メールフォルダーや削除済みアイテムフォルダーに移動された可能性があります。
- また、メールアカウントが正しいことも確認してください。確認メールは、アカウントのファイルで現在指定されているメールアドレスに送信されます。通常このメールアドレスは、Citrix Cloud に最初に登録したアドレス、または Citrix Cloud アカウントに招待された時のアドレスです。

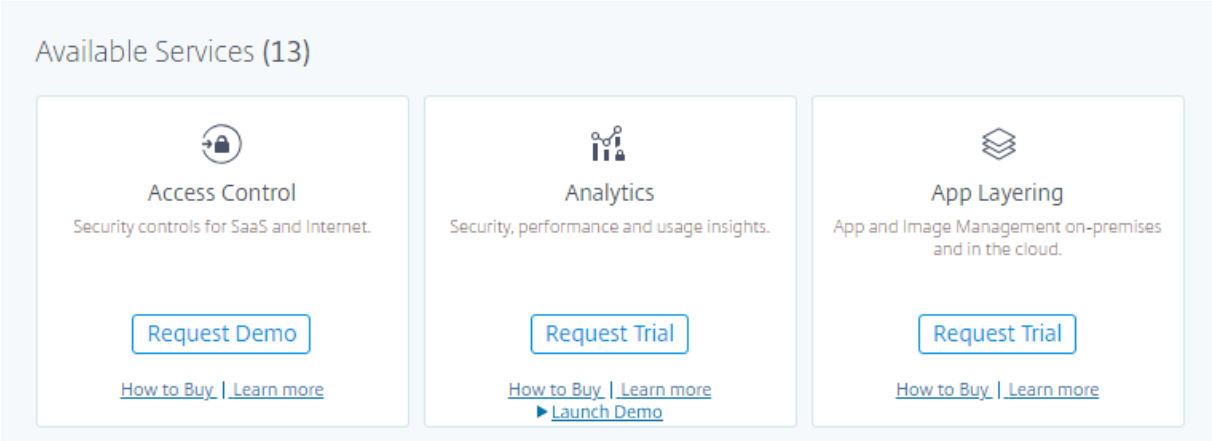
シトリックステクニカルサポートへの連絡

ここで説明していない問題が発生している場合は、シトリックステクニカルサポートに連絡してサポートケースを開いてください。

Citrix Cloud サービスのトライアル

September 17, 2021

個別の Citrix Cloud サービスのトライアルは、Citrix Cloud 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、Citrix Cloud 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。一部のサービスでは、トライアルを入手する前にデモを要求する必要があります。詳しくは、本記事の「サービスデモの要求」を参照してください。

Citrix Cloud 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。

> ヒント:
>
> 「Citrix Cloud の基礎」コースの「Citrix Cloud の利用を開始する」教育モジュールには、トライアルの申請方法について説明した短い動画があります。また、このコースをすべて履修すると、Citrix Cloud、組織にとってのメリット、および Citrix Cloud サービスで対処できる重要なユースケースの理解のために必要なしっかりとした基礎を身につけることができます。

サービストライアルに関する事実

	Citrix Cloud 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。
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
Virtual Apps and Desktops サービス	完全な機能セット

	Citrix Cloud トライアル
Endpoint Management	完全な機能セット
カスタマイズ可能	はい

サービスデモの要求

一部のサービスでは、サービスを試す前に Citrix の営業担当者にデモを要求する必要があります。デモを要求すると、組織のクラウドサービスのニーズについて Citrix の営業担当者と話し合うことができ、サービスを正常に試用するために必要なすべての情報を入手できます。

1. Citrix Cloud アカウントにサインインします。
2. 管理コンソールから、試用するサービスの ［デモの要求］をクリックします。そのサービスのデモ要求ページが表示されます。
3. フォームに記入して送信します。Citrix の営業担当者が詳細について連絡し、サービスの利用方法について説明します。

サービストライアルをリクエストする

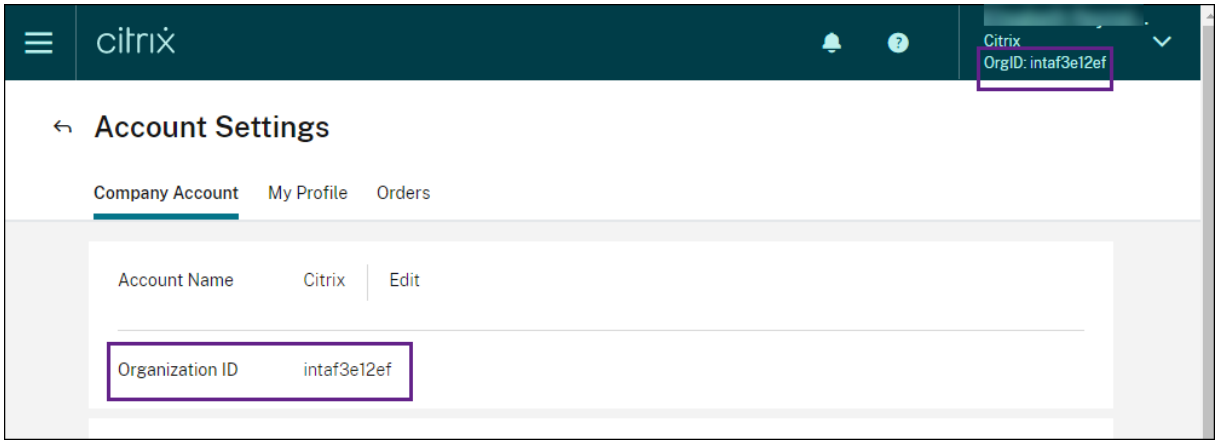
トライアルをリクエストするには、Citrix Cloud アカウントにログオンします。管理コンソールで、試用するサービスの ［トライアルのリクエスト］をクリックします。トライアルが承認され使用の準備が整うと、メールの通知が届きます。トライアルの完了まで、60 日間使用できます。

> 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。

Citrix Cloud サービスを購入する

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/products/citrix-cloud/を参照してください。

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



> 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。

Citrix Cloud サービスのサブスクリプション延長

July 28, 2021

この記事では、購入した Citrix Cloud サービスのサブスクリプションがどのように期限切れになるのか、およびサブスクリプションを延長する方法について説明します。Virtual Apps and Desktops Essentials などの月単位サブスクリプションで購入されるサービスと、Virtual Apps and Desktops サービスなどの年間サブスクリプションまたは複数年サブスクリプションで購入されるサービスでは、サービスの有効期限の切れ方が異なります。

この記事の _ 月単位サブスクリプション _ とは、月ごとに購入されるサービスを指します。_ 年間サブスクリプション _ とは、年間ベースで購入されるサービスを指します。_ 複数年サブスクリプション _ とは、複数年ベースで購入されるサービスを指します。

> ヒント:
>
> 「Citrix Cloud の基礎」コースの「Citrix Cloud の利用を開始する」教育モジュールには、サブスクリプションの期限切れプロセスについて説明した短い動画があります。また、このコースをすべて履修すると、Citrix Cloud、組織にとってのメリット、および Citrix Cloud サービスで対処できる重要なユースケースの理解のために必要なしっかりとした基礎を身につけることができます。

有効期限前

月単位サブスクリプションの場合、Citrix Cloud は有効期限が切れる前に通知を送信しません。

年間および複数年サブスクリプションの場合、既存のサブスクリプションの期限切れが近づいたときに、Citrix

Cloud から一定の間隔で通知が送信されます。これらの通知は、サブスクリプションを延長してサービスの中断を回避するよう促します。Citrix Cloud 管理コンソールには、次の通知が表示されます：

- 有効期限の 90 日前：黄色いバナーが開き、延長が必要なサービスとその有効期限が表示されます。この通知は 7 日ごとに、またはサービスが延長されるまでコンソールに表示されます。
- 有効期限の 7 日前：赤いバナーが開き、延長が必要なサービスと有効期限が表示されます。この通知は、サービスが延長されるまで、または 30 日間の猶予期間が経過するまでコンソールに表示されます。

これらの通知の表示は閉じることができますが、7 日後に再び表示されます。

また、延長が必要なサービスの一覧とその有効期限が記載されたメール通知も送信されます。この通知は、次の間隔で送信されます。

- 有効期限の 90 日前
- 有効期限の 60 日前
- 有効期限の 30 日前
- 有効期限の 7 日前
- 有効期限の 1 日前

有効期限切れ後：サービスの猶予期間

サービスのサブスクリプションが期限切れになると猶予期間が与えられるので、ユーザーはサブスクリプションを延長したり、サービスからデータを削除したりできます。提供される猶予期間は、月単位サブスクリプションと年間サブスクリプションで異なります。

毎月のサービスサブスクリプション

毎月のサービスサブスクリプションをキャンセルした場合は、有効期限日に Citrix から期限切れの通知メールが送信されます。有効期限日は、サブスクリプションをキャンセルした月の最終日です。有効期限が切れた後も、Citrix は管理者とユーザーが引き続きサービスにアクセスすることを 5 日間許可します。この間、管理者は列挙および削除機能のみに制限されます。Citrix は、5 日間の猶予期間中にリソースを使用しているときに発生した料金を請求します。

猶予期間中にサブスクリプションを延長しない場合、Citrix は、猶予期間が経過したときに管理者とユーザーがサービスにアクセスするのをブロックします。リマインダー通知メールは、次の間隔で送信されます：

- 有効期限の 1 日後（サービスがブロックされる 5 日前）
- 有効期限の 3 日後（サービスがブロックされる 2 日前）

猶予期間が経過すると、サービスに関連するすべてのリソースがシャットダウンされ、電源がオフになります。猶予期間が終了した後にサービスに追加したデータを取得する必要がある場合は、サービスの有効期限から 30 日以内であれば Citrix テクニカルサポートにリクエストを送信できます。

年間および複数年のサービスサブスクリプション

年間および複数年のサブスクリプションの場合、サブスクリプションの有効期限が切れた後も引き続き 30 日間サービスにアクセスできます。期間中にサブスクリプションを延長しないと、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。リマインダー通知は、次の間隔で送信されます。

- 有効期限の 15 日後（サービスがブロックされる 15 日前）
- 有効期限の 22 日後（サービスがブロックされる 7 日前）
- 有効期限の 29 日後（サービスがブロックされる 1 日前）

メール通知には、有効期限が切れたサービスとその有効期限一覧が含まれています。

この 30 日間の猶予期間中にサブスクリプションを延長すると、サブスクリプション期間はサービスの元の有効期限の日付から開始します。たとえば、サービスが 5 月 31 日に期限切れとなり、6 月 25 日（猶予期間が終了する前）にサブスクリプションを延長すると、5 月 31 日に延長したサブスクリプション契約が開始されます。

有効期限切れ後：サービスのブロックとデータの保持

猶予期間中にサービスサブスクリプションが延長されない場合、Citrix は次の方法でサービスへのアクセスをブロックします：

- 有効期限が切れた月単位サブスクリプションの場合、管理者とユーザーのアクセスは有効期限の 5 日後にブロックされます。
- 有効期限が切れた年間および複数年のサブスクリプションの場合、管理者とユーザーのアクセスは、有効期限の 30 日後にブロックされます。

サービスの有効期限日を過ぎてから 30 日間は、サービスに追加したデータは Citrix によって保持されます。30 日間の保持期間が終了する前にサブスクリプションを延長すると、管理者とユーザーはデータをそのまま使用してサービスにアクセスできます。延長されたサブスクリプションは次のように開始します：

- 月単位サブスクリプションの場合、最初の月のサブスクリプションの開始日は、延長契約を購入した日です。その後、サブスクリプションは翌月の 1 日に自動的に更新されます。
- 年間および複数年のサブスクリプションの場合、延長サブスクリプションの開始日は、延長契約を購入した日です。

30 日間の保有期間が終了する前にサブスクリプションを延長しないと、シトリックスによりサービスがリセットされ、追加したデータがすべて削除されます。Citrix によるクラウド環境の管理を許可することに同意した場合（たとえば、Virtual Apps and Desktops サービスで Citrix Essentials サービスまたは Azure クイック展開オプションを使用する場合）、Citrix は 30 日間の保有期間終了後に次のアクションを実行します：

- Citrix データベースからすべての顧客関連データを削除する。
- Citrix 管理の VM など、ご利用のクラウド環境で Citrix がプロビジョニングしている Citrix Cloud サービスに関連したすべてのリソースを削除する。特定の Citrix Cloud サービスに含まれる Citrix 管理のコンポーネントについて詳しくは、そのサービスのドキュメントを参照してください。

顧客管理の **Azure** サブスクリプション

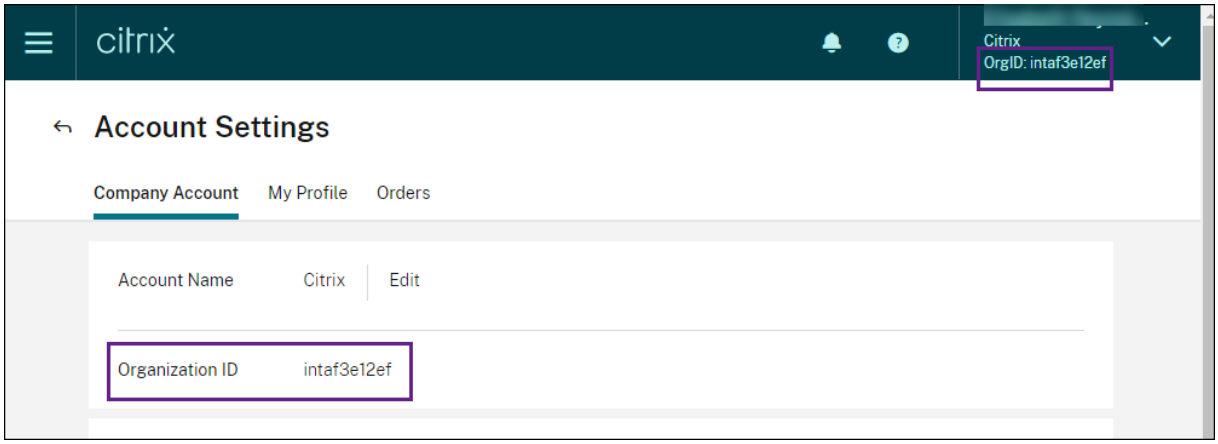
Citrix Cloud サービスで独自の Azure サブスクリプションを使用している場合は、Azure サブスクリプションをサービスに接続するときに、そのサービスによってアプリがインストールされます。Citrix Cloud サービスのサブスクリプションを延長しない場合、30 日間の保有期間が終了してもこのアプリは Azure のサブスクリプションから削除されません。Azure サブスクリプションからサービスを完全に削除するには、このアプリを手動で削除する必要があります。次のいずれかの方法でこのアプリを削除できます:

- 管理者がまだサービスへのアクセスをブロックされていない場合は、サービス内からこのアプリを削除します。
- 管理者がサービスへのアクセスをブロックされている場合は、Azure ポータル内からこのアプリを削除します。

サービスの延長の購入

Citrix Cloud サービスのサブスクリプションの延長するには、https://www.citrix.com/ja-jp/products/citrix-cloud/にアクセスします。

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



システムおよび接続要件

September 17, 2021

Citrix Cloud では、管理機能（Web ブラウザー経由）およびご利用中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。この記事には、ご利用中のリソースと Citrix Cloud 間の接続を確立するためのシステム要件、必要なアクセス可能インターネットアドレス、および考慮事項について記載されています。

システム要件

Citrix Cloud の最小構成要件は、以下のとおりです。

- Active Directory ドメイン
- ドメインに参加している Citrix Cloud Connector 用の 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。
- ワークロードおよび StoreFront などの他のコンポーネントをホストするための物理マシンまたは仮想マシン（ドメイン参加済み）。特定のサービスのシステム要件について詳しくは、各サービスの Citrix ドキュメントを参照してください。

スケールとサイズの要件について詳しくは、「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。

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
- Microsoft Internet Explorer 11
- 最新バージョンの Apple Safari

Citrix Cloud 管理コンソール

Citrix Cloud 管理コンソールは、https: //citrix.cloud.com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。

ファイアウォール構成

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。

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、アドレス`https://citrix-cloud-content.customer.pendo.io/`を利用できるようにしてください。

以下サービスは、Pendo コンテンツを表示します:

- Analytics
- Content Collaboration
- Virtual Apps and Desktops
- Workspace

Pendo は、シトリックス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 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。

オンプレミス製品の登録

オンプレミス製品の登録を実行するために Citrix ライセンスサーバーで Citrix Cloud を使用している場合、次のアドレスを使用できることを確認します:

- `https://trust.citrixnetworkapi.net`（コードを取得する場合）
- `https://trust.citrixworkspacesapi.net/`（ライセンスサーバーが登録されていることを確認する場合）
- `https://cis.citrix.com`（データをアップロードする場合）
- `https://core-eastus-release-a.citrixworkspacesapi.net`
- `https://core.citrixworkspacesapi.net`
- `ocsp.digicert.com port 80`
- `crl3.digicert.com port 80`
- `crl4.digicert.com port 80`
- `ocsp.entrust.net port 80`
- `crl.entrust.net port 80`

Citrix ライセンスサーバーにプロキシサーバーを使用している場合、プロキシサーバーがライセンスサーバー製品ドキュメントの「プロキシサーバーの構成」の説明どおりに構成されていることを確認します。

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 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。Citrix Cloud 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に必要な条件については、「システム要件」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 Citrix Cloud 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。

Cloud Connector をホストするマシンには、Citrix Cloud との安定したネットワーク接続が必要です。ネットワークコンポーネントは、HTTPS と、長期間有効で安全な Web ソケットをサポートしている必要があります。ネットワークコンポーネントでタイムアウトが設定されている場合、設定は 2 分より長くする必要があります。

Cloud Connector と Citrix Cloud との接続の問題をトラブルシューティングするには、Cloud Connector 接続性チェックユーティリティを使用してください。このユーティリティは、Cloud Connector マシンで一連のチェックを実行して、Citrix Cloud および関連サービスに到達できることを確認し、不足している接続アドレスを Internet Explorer の信頼済みサイトゾーンに追加するのに役立ちます。環境でプロキシーサーバーを使用している場合、すべての接続検査はプロキシーサーバーを介してトンネリングされます。ユーティリティをダウンロードするには、シトリックスサポートの Knowledge Center でCTX260337を参照してください。

Cloud Connector の一般的なサービス接続要件

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。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。

サービスを適切に操作し、消費するには、この記事の各アドレスが利用可能である必要があります。次の一覧では、ほとんどの Citrix Cloud サービスや機能に共通したアドレスを表示します。Citrix Cloud 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。

- `https://*.citrixworkspacesapi.net`（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://*.cloud.com`（Citrix Cloud 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）
  - すべてのサブドメインを有効にできないお客様は、代わりに次のアドレスを使用できます:
    * `https://cwsproduction.blob.core.windows.net`
    * `https://ccprodaps.blob.core.windows.net`
    * `https://ccprodeu.blob.core.windows.net`

- https://*.servicebus.windows.net（ログ、Active Directory エージェント、Machine Creation Services で使用される 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。

オンプレミス製品の登録を実行するために Citrix ライセンスサーバーで Citrix Cloud を使用している場合、追加で必要な連絡先アドレスに関しては、本記事の「オンプレミス製品の登録」を参照してください。

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 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。

クラウドサービス用の **Citrix** コネクタアプライアンス

コネクタアプライアンスは、ハイパーバイザーに展開できるアプライアンスです。コネクタアプライアンスをホストするハイパーバイザーは、Citrix Cloud 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。コネクタアプライアンスは Citrix Cloud 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。

コネクタアプライアンスをインストールするために必要な条件については、「システム要件」を参照してください。

操作には、ポート 443 を使用して発信する必要があります。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、以下のアドレスが利用できる必要があります：

- https://*.cloud.com

- https://*.citrixworkspacesapi.net
- https://*.citrixnetworkapi.net
- https://*.*.nssvc.net
  - すべてのサブドメインを有効にできないお客様は、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

Citrix Analytics Service の接続性

- 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/
- 追加要件: 前提条件

サービスへのデータソースの配布準備について詳しくは、「データソースを構成する方法」を参照してください。

Content Collaboration サービスの接続性

Citrix リソースの場所/Cloud Connector:

- Cloud Connector の一般的なサービス接続要件
- https://*.sharefile.com
- その他の要件: ShareFile ファイアウォール構成と IP アドレス（CTX208318）
- 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/

管理コンソール:

- https://*.citrixworkspacesapi.net
- https://*.cloud.com
- その他の要件: ShareFile ファイアウォール構成と IP アドレス（CTX208318）

Endpoint Management サービスの接続性

Citrix リソースの場所/Cloud Connector:

- Cloud Connector の一般的なサービス接続要件
- 追加要件: /ja-jp/citrix-endpoint-management/endpoint-management.html

管理コンソール:

- https://*.citrix.com

- https://*.citrixworkspacesapi.net
- https://*.cloud.com
- https://*.blob.core.windows.net
- 追加要件：/ja-jp/citrix-endpoint-management/endpoint-management.html

Citrix Gateway サービスの接続性

- Cloud Connector の一般的なサービス接続要件
- https://*.*.nssvc.net
  - すべてのサブドメインを有効にできないお客様は、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

SD-WAN Orchestrator サービスの接続性

完全なインターネット接続要件については、「Citrix SD-WAN Orchestrator サービス使用の前提条件」を参照してください。

Secure Browser サービスの接続性

Citrix リソースの場所/Cloud Connector：

Cloud Connector の一般的なサービス接続要件

管理コンソール：

- https://*.cloud.com
- https://*.citrixworkspacesapi.net
- https://browser-release-a.azureedge.net
- https://browser-release-b.azureedge.net

Citrix Secure Workspace Access サービスの接続性

- https://*.netscalergateway.net
- https://*.*.nssvc.net
  - すべてのサブドメインを有効にできないお客様は、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

Virtual Apps and Desktops サービスのサービス接続

Citrix リソースの場所/Cloud Connector：

- Cloud Connector の一般的なサービス接続要件
- https://[customerid].xendesktop.net。この[customerid]は、Citrix Cloud 管理コンソールの［セキュアクライアント］タブ（[**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］）に表示される顧客 ID パラメーターです。
  - Citrix Virtual Apps Essentials を使用しているお客様は、代わりにhttps://*.xendesktop.netを使用する必要があります。
- https://*.*.nssvc.net
  - すべてのサブドメインを有効にできないお客様は、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

Cloud Connector が Virtual Apps and Desktops サービスと通信する方法の概要については、Citrix Tech Zone Web サイトの「Virtual Apps and Desktops の図」を参照してください。

管理コンソール:

- https://*.citrixworkspacesapi.net
- https://*.citrixnetworkapi.net
- https://*.cloud.com
- https://[customerid].xendesktop.net。この[customerid]は、Citrix Cloud 管理コンソールの［セキュアクライアント］タブ（[**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］）に表示される顧客 ID パラメーターです。
  - Citrix Virtual Apps Essentials を使用しているお客様は、代わりにhttps://*.xendesktop.netを使用する必要があります。
- https://*.*.nssvc.net（Virtual Apps and Desktops Standard for Azure の場合は不要）
  - すべてのサブドメインを有効にできないお客様は、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
- 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/

Citrix Workspace Service の接続性

- https://*.cloud.com
- 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/

利用者が Workspace 経由で Citrix Files と Content Collaboration のコンテンツに正常にアクセスできるようにするには、CTX208318に記載されたドメインを許可することをお勧めします。

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

コンソールと FAS サービスは、それぞれユーザーのアカウントとネットワークサービスアカウントを使用して次のアドレスにアクセスします。

- ユーザーアカウントの下の FAS 管理コンソール
  - `*.cloud.com`
  - `*.citrixworkspacesapi.net`
  - サードパーティの ID プロバイダーが必要とするアドレス（環境で使用されている場合）
- ネットワークサービスアカウントの下の FAS サービス：`*.citrixworkspacesapi.net`

環境にプロキシサーバーが含まれている場合は、FAS 管理コンソールのアドレスを使用してユーザープロキシを構成します。また、ネットワークサービスアカウントのアドレスが環境に応じて適切に構成されていることを確認してください。

Workspace Environment Management サービスの接続性

`https://*.wem.cloud.com`

Citrix Cloud への接続

November 11, 2020

リソースを Citrix Cloud に接続するには、環境内でコネクタを展開し、_ リソースの場所 _ を作成します。

リソースの場所には、利用者にクラウド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。これらのリソースは、Citrix Cloud コンソールで管理します。リソースの場所に含まれるリソースは、使用している Citrix Cloud サービスおよび利用者に提供するサービスによって異なります。

リソースの場所を作成するには、ドメインに少なくとも 2 つの Cloud Connector をインストールします。Cloud Connector は、Citrix Cloud とリソースの間で通信するために必要です。Cloud Connector の展開について詳しくは、以下の記事を参照してください：

リソースの種類

リソースの場所に含まれるリソースは、使用している Citrix Cloud サービスおよび利用者に提供するサービスによって異なります。各リソースで異なるタイプのコネクタが使用されます。大半のサービスは Citrix Cloud Connector を利用しますが、特定のサービスではコネクタアプライアンスが必要です。

Citrix Cloud Connector を使用するサービス

たとえば、Virtual Apps and Desktops サービスを通じてアプリケーションとデスクトップへのアクセスを提供する場合、リソースの場所には次のものが含まれます：

- Active Directory のユーザードメインとリソースドメイン
- Citrix Hypervisor などのハイパーバイザー
- Virtual Desktop Agent（VDA）を実行しているサーバー
- リソースへのセキュアな外部アクセスを実現するオンプレミスの Citrix Gateway または Citrix Gateway サービス
- ユーザーが使いやすい単一のアプリストアを介してリソースにアクセスできるための、オンプレミスの StoreFront サーバー

Cloud Connector が Virtual Apps and Desktops サービスと通信する方法の概要については、「Citrix Tech Zone の図」を参照してください。

Cloud Connector を使用する Citrix Cloud サービスの一覧については、「Cloud Connector が必要なサービス」を参照してください。

コネクタアプライアンスを使用するサービス

たとえば、アプリケーションからアクションや通知を Workspace やその他のチャネルに直接配信したい場合、リソースの場所には次の項目を含めることができます:

- リソースの場所にあるシステムへの Citrix Workspace マイクロアプリサービスのアクセス
- リソースの場所から外部システムへの Citrix Workspace マイクロアプリサービスのアクセス

コネクタアプライアンスを使用する Technical Preview 段階のサービスがほかにも存在する可能性があります。

リソースの場所

リソースの場所は、パブリッククラウド、プライベートクラウド、支社、またはデータセンターのいずれであっても、リソースがある場所であればどこにでも配置できます。既にクラウドまたはデータセンターにリソースを所有している場合、リソースはそのまま残ります。Citrix Cloud で使用するために別の場所に移動する必要はありません。

場所の選択は、以下の要素の影響を受けることがあります:

- 利用者との距離
- データとの距離
- 拡張の必要性
- セキュリティ属性

配置するリソースの場所の数に制限はありません。リソースの場所に必要なオーバーヘッドはわずかです。

リソースの場所の展開例

- データから近い距離に位置する必要がある利用者やアプリケーションのために、本社のデータセンターに最初のリソースの場所を構築する。
- グローバルユーザーのために、パブリッククラウドに 2 番目のリソースの場所を追加する。または、支社で別のリソースの場所を構築して、支社の従業員が最適に利用できるアプリケーションを提供する。

- 別のネットワークにさらにリソースの場所を追加して、限定されたアプリケーションを提供する。これによって、これ以外のリソースの場所を調整する必要なく他のリソースや利用者に表示される内容を制限できます。

命名制限

リソースの場所に割り当てる名前は、次の制限に準拠する必要があります:

- 最大文字数: 64 文字
- 許可されていない文字:
  - ##、$、%、^、&、?、+
  - かっこ: [ ]、{ }
  - パイプ（|）
  - 小なり記号（<）と大なり記号（>）
  - スラッシュとバックスラッシュ（/、\）
- Citrix Cloud アカウントが使用する他のリソースの場所の名前と一致していない（大文字と小文字は区別）

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 間の特定の通信に「最も優先される」と指定するリソースの場所です。プライマリのリソースの場所にある Cloud Connector が、ユーザーのログオンとプロビジョニング操作に使用されます。「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 にすばやくログオンできます。

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。(/ja-jp/citrix-cloud/citrix-cloud-management/identity-access-management/primary-resource-locations.html)

Citrix Cloud Connector

September 17, 2021

Citrix Cloud Connector は、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する Citrix コンポーネントで、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。これによって、配信インフラストラクチャを管理する手間が省けます。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。

Cloud Connector が必要なサービス

Virtual Apps and Desktops サービスには Cloud Connector が必要です。Cloud Connector が Virtual Apps and Desktops サービスと通信する方法の概要については、Citrix Tech Zone の「Virtual Apps and Desktops の図」を参照してください。

Citrix Endpoint Management では、Endpoint Management サービスへのエンタープライズ接続に Cloud Connector が必要です。Secure Browser サービスでは、認証された外部 Web アプリのために Cloud Connector が必要です。

Cloud Connector の機能

- **Active Directory**（**AD**）: 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。
- **Virtual Apps and Desktops** の公開：リソースの場所にあるリソースから公開できるようにします。
- **Endpoint Management**: モバイルデバイス管理（MDM）およびモバイルアプリケーション管理（MAM）環境を使用して、デバイスポリシーとアプリポリシーを管理し、ユーザーにアプリケーションを配信できるようにします。
- マシンカタログのプロビジョニング：マシンをリソースの場所に直接プロビジョニングできます。

> 注:
>
> 操作は可能ですが、Citrix Cloud への接続が利用できない期間、機能が低下する可能性があります。Citrix Cloud コンソールから Cloud Connector の正常性を監視できます。

Cloud Connector の通信

Cloud Connector 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、Cloud Connector 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 Cloud Connector からクラウドに対して確立されます。受信接続は受け入れられません。

Cloud Connector 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 Cloud Connector をインストールします。各リソースの場所に少なくとも 2 つの Cloud Connector を使用することをお勧めします。ある Cloud Connector を一定期間使用できない場合、他の Cloud Connector がその接続を維持できます。各 Cloud Connector はステートレスであるため、使用可能なすべての Cloud Connector 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。完全に自動化されています。

1 つの Cloud Connector が利用可能である限り、Citrix Cloud との通信は失われません。エンドユーザーからリソースの場所にあるリソースへの接続は、可能な限り Citrix Cloud への接続に依存しません。これにより、Citrix Cloud に接続できるかに関係なく、リソースの場所でリソースにアクセスできるようになります。

Cloud Connector の入手場所

Citrix Cloud 内から Cloud Connector ソフトウェアをダウンロードできます。

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. 既存のリソースの場所がない場合、［リソースの場所］ページで ［ダウンロード］をクリックします。プロンプトが表示されたら、**cwcconnector.exe** ファイルを保存します。
4. リソースの場所があり Cloud Connector がインストールされていない場合は、Cloud Connector バーをクリックし、［ダウンロード］を選択します。プロンプトが表示されたら、**cwcconnector.exe** ファイルを保存します。

Cloud Connector のインストール場所

サポートされるプラットフォーム、オペレーティングシステム、バージョンについては、「システム要件」を参照してください。

Windows Server 2012 R2、Windows Server 2016、または Windows Server 2019 を実行している専用マシンに Cloud Connector をインストールします。このマシンをドメインに参加させ、Citrix Cloud から管理するリソースと通信できるようにする必要があります。

> 重要:
>
> - Active Directory ドメインコントローラーに Cloud Connector やその他の Citrix コンポーネントをインストールしないでください。
> - 他のシトリックス展開の一部であるマシン（たとえば、Virtual Apps and Desktops 展開の Delivery Controller）に Cloud Connector をインストールしないでください。

展開について詳しくは、次の記事を参照してください:

- Active Directory での Cloud Connector 展開シナリオ
- Cloud Connector のインストール

Citrix Cloud Connector の技術詳細

September 17, 2021

Citrix Cloud Connector は、Windows Server 2012 R2、Windows Server 2016、または Windows Server 2019 にインストールされた Windows サービスのコレクションのコンポーネントです。

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に、各リソースの場所に少なくとも 2 つの Cloud Connector をインストールしてください。

ハードウェア要件

各 Cloud Connector には、少なくとも次のものが必要です:

- 仮想 CPU×2
- 4GB のメモリ
- 20GB のディスクスペース

仮想 CPU メモリを増やすと、Cloud Connector をより大規模なサイトにスケールアップできます。推奨の構成については、「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 2019
- Windows Server 2016
- Windows Server 2012 R2

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。Microsoft の Web サイトから最新バージョンをダウンロードします。

> 注:
>
> Cloud Connector で Microsoft .NET Core を使用しないでください。.NET Framework の代わりに.NET Core を使用すると、Cloud Connector のインストールが失敗する場合があります。Cloud Connector では.NET Framework のみを使用してください。

サーバーの要件

Virtual Apps and Desktops サービスで Cloud Connector を使用している場合、マシン構成の手順については「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。

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。この設定が有効な場合、Cloud Connector が Citrix Cloud 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 を有効にしてください。Windows Update を構成するときに、業務時間外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

ルするようにします。ただし、最低 4 時間は、自動再起動を許可しないでください。Citrix Cloud プラットフォームは、更新が再起動を待機していることを識別したときにマシンの再起動を処理し、一度に 1 つの Cloud Connector のみを再起動できるようにします。更新後にマシンを再起動する必要がある場合は、グループポリシーまたはシステム管理ツールを使用してフォールバック再起動を構成できます。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。証明書を受信すると、クライアントは証明書を発行した CA を信頼するか、および証明書が CRL に含まれるかをチェックします。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 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認証局の 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/en-us/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://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ります：
  - `https://*.digicert.com`

- 以下の証明書がインストールされています:
  - https://dl.cacerts.digicert.com/DigiCertAssuredIDRootCA.crt
  - https://dl.cacerts.digicert.com/DigiCertSHA2AssuredIDCodeSigningCA.crt
  - https://cacerts.digicert.com/DigiCertGlobalRootG2.crt
  - https://cacerts.digicert.com/DigiCertGlobalRootCA.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

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。マルチドメイン環境については、この記事の「Active Directory での Cloud Connector 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 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、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

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、「システムおよび接続要件」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

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 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 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、「Cloud Connector の入手場所」を参照してください。

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の管理を容易にします。	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 Cloud Services Agent Discovery	XenApp および XenDesktop のレガシーオンプレミス Citrix 製品の管理を容易にします。	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 Connection Lease Exchange Service	ワークスペースのサービス継続性のために、Workspace アプリと Cloud Connector 間で接続リースファイルを交換できるようにします	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
Citrix NetScaler CloudGateway	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

サービス名	説明	実行アカウント
Citrix Remote HCL Server	Delivery Controller と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 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

Active Directory での **Cloud Connector** 展開シナリオ

安全な内部ネットワーク内に Cloud Connector をインストールします。

単一フォレストに単一ドメインがある場合、そのドメインに Cloud Connector をインストールするだけで、リソースの場所が確立されます。環境内に複数のドメインがある場合、利用可能なリソースにユーザーがアクセスできるよう、Cloud Connector をインストールする場所を検討する必要があります。

> 注:
>
> 以下のリソースの場所は、ブループリントの一部となります。リソースがホストされている場所に応じて、他の物理的な場所でもこのブループリントを使用する必要があります。

単一フォレストに単一ドメインが存在する場合に、単一の **Cloud Connector** セットを展開

このシナリオでは、すべてのリソースとユーザーオブジェクトが 1 つのドメイン（forest1.local）に含まれています。単一の Cloud Connector セットが 1 つのリソースの場所に展開され、forest1.local ドメインに参加します。

- 信頼関係：なし - 単一ドメイン
- [**ID** およびアクセスの管理] に表示されるドメイン：forest1.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

単一フォレストに親子ドメインが存在する場合に、単一の **Cloud Connector** セットを展開

このシナリオでは、親ドメイン（forest1.local）とその子ドメイン（user.forest1.local）が 1 つのフォレスト内に存在します。親ドメインはリソースドメインとして機能し、子ドメインはユーザードメインです。単一の Cloud Connector セットが 1 つのリソースの場所に展開され、forest1.local ドメインに参加します。

- 信頼関係：親と子のドメインの信頼
- ［**ID** およびアクセスの管理］に表示されるドメイン：forest1.local、user.forest1.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

> 注:
>
> Citrix Cloud が子ドメインを認識するには、Cloud Connector の再起動が必要な場合があります。

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）、単一の **Cloud Connector** セットを展開

このシナリオでは、1 つのフォレスト（forest1.local）にリソースドメインが含まれ、もう 1 つのフォレスト（forest2.local）にユーザードメインが含まれます。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 1 つのリソースの場所に展開され、forest1.local ドメインに参加します。

- 信頼関係: フォレストの信頼
- ［**ID** およびアクセスの管理］に表示されるドメイン：forest1.local
- Citrix Workspace にログオンできるユーザー：forest1.local のユーザーのみ
- 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

> 注:
>
> 2 つのフォレスト間の信頼関係は、ユーザーフォレスト内のユーザーがリソースフォレスト内のマシンにログオンできるように設定する必要があります。

Cloud Connector はフォレストレベルの信頼を通過できないため、Citrix Cloud コンソールの ［**ID** およびアクセスの管理］ページに forest2.local ドメインは表示されません。そのため、次の制限事項が発生します:

- リソースは、Citrix Cloud の forest1.local に配置されたユーザーとグループにのみ公開できます。ただし、forest2.local のユーザーを forest1.local のセキュリティグループ内に入れ子にすることで、この問題に対処できます。
- Citrix Workspace は、forest2.local ドメインのユーザーを認証できません。

これらの制限事項の回避策としては、「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）、Cloud Connector セットを各フォレストに展開」の説明に従って、Cloud Connector を展開します。

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）、**Cloud Connector** セットを各フォレストに展開

このシナリオでは、1 つのフォレスト（forest1.local）にリソースドメインが含まれ、もう 1 つのフォレスト（forest2.local）にユーザードメインが含まれます。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。1 つの Cloud Connector セットが forest1.local ドメインに展開され、2 つ目のセットが forest2.local ドメインに展開されます。

- 信頼関係: フォレストの信頼
- [**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

Cloud Connector の正常性を表示する

Cloud Connector の［リソースの場所］ページには、リソースの場所にあるすべての Cloud Connector の状態が表示されます。

イベントメッセージ

Cloud Connector は、Windows イベントビューアーで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 ダウンロードでは、次の XML ファイルにこれらのメッセージが含まれます:

- 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。

イベントログ

デフォルトでは、イベントログは、Cloud Connector をホストしているマシンの C:\ProgramData\Citrix\WorkspaceCloud\Log ディレクトリにあります。

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。

Cloud Connector 接続

Cloud Connector が「切断」になっている場合、Cloud Connector 接続チェックユーティリティによって、Citrix Cloud およびその関連サービスに到達できることを検証できます。

Cloud Connector 接続チェックユーティリティは、Cloud Connector をホストしているマシンで実行されます。環境でプロキシサーバーを使用している場合、ユーティリティはすべての接続チェックをプロキシサーバー経由でトンネリングし、接続を検証できます。このユーティリティは、必要に応じて不足している Citrix の信頼済みサイトを Internet Explorer の信頼済みサイトゾーンに追加することもできます。

このユーティリティのダウンロードおよび使用方法について詳しくは、シトリックスサポートの Knowledge Center でCTX260337を参照してください。

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。

Cloud Connector のプロキシとファイアウォールの構成

September 17, 2021

Cloud Connector は、認証されていない Web プロキシサーバーを介したインターネットへの接続をサポートしています。インストーラーとインストールするサービスの両方が Citrix Cloud に接続します。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。

接続の要件

HTTP トラフィックを使用するポート 443（送信のみ）を使用します。必須の接続可能アドレスの一覧については、「システムおよび接続要件」を参照してください。ほとんどの Citrix Cloud サービスに共通のアドレスの一覧とその機能については、「Cloud Connector の一般的なサービス接続要件」を参照してください。

Citrix Cloud に必要な連絡先アドレスは、IP アドレスではなくドメイン名として指定されます。IP アドレスは変更される可能性があるため、ドメイン名を許可すると、Citrix Cloud への接続が安定した状態に保たれます。また、シトリックスによって Citrix Cloud プラットフォームの改善と強化が続けられているため、これらのドメインを具体的なアドレスではなくワイルドカード（たとえば、*.citrixworkspacesapi.net）として許可することは、顧客の Citrix Cloud への接続に影響を与えずに顧客に改善のメリットをもたらすことにつながります。地理的リージョンに基づくトラフィックフェールオーバーなど、プラットフォームの重要な機能の中には、複数のサブドメインの下で通話をルーティングできることに依存するものがあります。許可されたワイルドカードドメインの代わりに許可されたサブドメインを指定すると、これらの機能が顧客が明示的に許可していないサブドメインを使用する可能性があるため、停止のリスクが高まります。ワイルドカードドメインを指定すると、Citrix Cloud サービスごとに多数のサブドメインを許可リストに登録するという過度の負担を顧客にかけることなく、これらの機能を使用できます。

> 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 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。

Cloud Connector 接続の確認

Cloud Connector 接続性チェックユーティリティでは、いくつかの接続チェックを使用して、Cloud Connector と Citrix Cloud 間の接続を確認できます。環境でプロキシサーバーを使用している場合、このユーティリティによって Cloud Connector でプロキシ設定を構成し、プロキシサーバー経由の接続をテストできます。プロキシサーバーが構成されると、接続テストはプロキシサーバー経由でトンネリングされます。

Cloud Connector 接続チェックユーティリティのダウンロードおよび使用について詳しくは、CTX260337を参照してください。

> 注:
>
> Cloud Connector 接続チェックユーティリティは、商用の Citrix Cloud アカウントでのみ使用できます。Citrix Cloud Government または Citrix Cloud Japan では使用しないでください。

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。

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。（上記のように）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。

```
1 netsh winhttp import proxy source =ie
2 <!--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 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:
>
> 自動検出スクリプト、PAC スクリプト、または認証済みプロキシはサポートされていません。

内部リソースへの接続

Windows プロキシの設定により、Cloud Connector が Web プロキシを介して内部リソースへのアクセスを試みる場合があります。これらのリソースは、必要な接続 URLが許可されていても、Cloud Connector と Virtual Apps and Desktops サービスに接続できない場合があります。また、HTTP 接続コマンドで URL として IP アドレ

スが使用されるため、Web プロキシが Cloud Connector と Azure サービスバス間の接続をブロックすることがあります。その結果、一部のリソース機能が失敗することがあります。たとえば、Citrix Provisioning でマシンカタログを正常に作成できません。

これらの内部リソースが期待どおりに接続できるようにするには、各リソースの完全修飾ドメイン名または IP アドレスを Cloud Connector マシンのプロキシバイパスリストに追加します。この問題について詳しくは、シトリックスサポート Knowledge Center のCTX241222を参照してください。

Citrix フェデレーション認証サービスと **Citrix Cloud** の接続

コンソールと FAS サービスは、それぞれユーザーのアカウントとネットワークサービスアカウントを使用して次のアドレスにアクセスします。

- ユーザーアカウントの下の FAS 管理コンソール
  - `*.cloud.com`
  - `*.citrixworkspacesapi.net`
  - サードパーティの ID プロバイダーが必要とするアドレス（環境で使用されている場合）
- ネットワークサービスアカウントの下の FAS サービス：`*.citrixworkspacesapi.net`

環境にプロキシサーバーが含まれている場合は、FAS 管理コンソールのアドレスを使用してユーザープロキシを構成します。また、ネットワークサービスアカウントのアドレスが netsh または同様のツールを使用して構成されていることを確認します。

Cloud Connector のインストール

July 29, 2021

Cloud Connector ソフトウェアは、インタラクティブにインストールすることも、コマンドラインを使用してインストールすることもできます。

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。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：

- インストールを実行するユーザーを認証する
- インストーラーの権限を確認する
- Cloud Connector サービスをダウンロードして構成する

インストール前に確認する情報

- システム要件：Cloud Connector をホストするマシンを準備すること。
- Tech Zone 記事エンドポイントのセキュリティとウイルス対策のベストプラクティスのウイルス対策の除外セクション：環境の Cloud Connector に対してセキュリティとパフォーマンスの適切なバランスを判断

するためのガイドラインを示しています。これらのガイドラインを組織のウイルス対策チームとセキュリティチームとともに確認し、実稼働環境に適用する前に厳格なラボベースのテストを実施することを強くお勧めします。

- システムおよび接続要件：Cloud Connector をホストするすべてのマシンが Citrix Cloud と通信できることを確認してください。
- Cloud Connector のプロキシとファイアウォールの構成：Web プロキシまたは厳密なファイアウォールルールを持つ環境に Cloud Connector をインストールする場合。
- Cloud Connector のスケールおよびサイズの考慮事項：Cloud Connector をホストするマシンの構成に関する、テスト済み最大容量の詳細とベストプラクティスの推奨事項を提供します。

インストールの考慮事項とガイダンス

- Active Directory ドメインコントローラーや、リソースの場所のインフラストラクチャにとって重要なマシンに Cloud Connector をインストールしないでください。Cloud Connector の定期的な保守では、これらの追加リソースの停止を引き起こすマシン操作を実行します。
- Cloud Connector をホストしているマシンに他のシトリックス製品をダウンロードしたりインストールしたりしないでください。
- 他のシトリックス製品展開に属するマシン（たとえば、Citrix Virtual Apps and Desktops 展開の Delivery Controller）に Cloud Connector をダウンロードまたはインストールしないでください。
- 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 のインストーラーは、Citrix Cloud からダウンロードします。そのため、ブラウザーが実行可能ファイルをダウンロード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。マシンを別のドメインに参加させる必要がある場合は、Cloud Connector をアンインストールしてから、マシンを別のドメインに参加させた後に再インストールしてください。
- インストールしたら、すべての Cloud Connector の電源をオンのままにして、Citrix Cloud への常時接続を確保します。

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 がリソースの場所内のマシンと確実に通信できるようになります。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。

（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

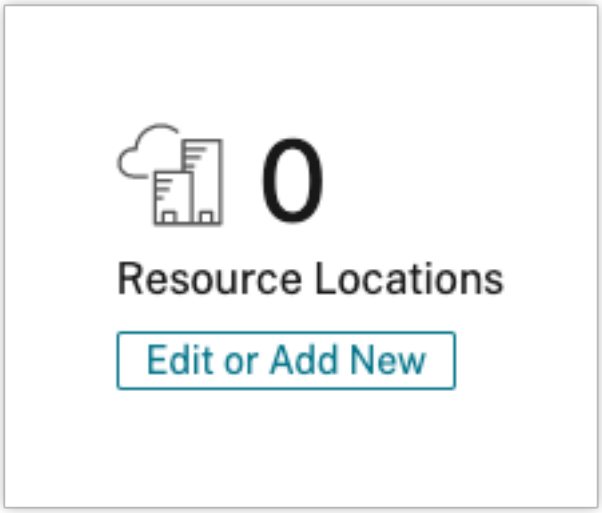
Connector をインストールしたマシンを複製すると、Cloud Connector サービスは実行されず、マシンは Citrix Cloud に接続できなくなります。

インタラクティブインストール

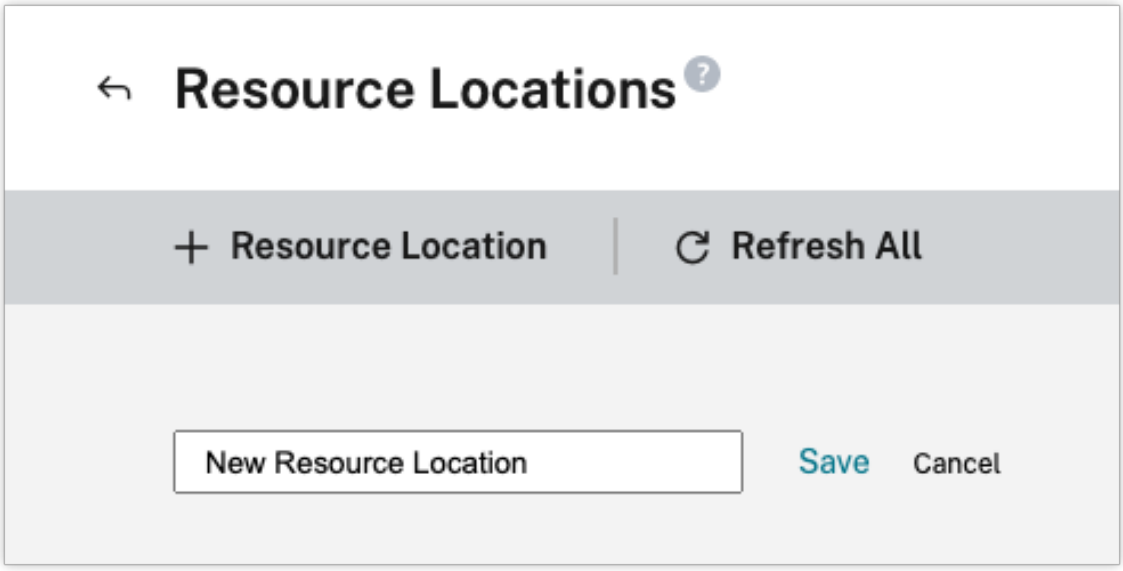
グラフィカルインストーラーインターフェイスを使用して、Cloud Connector をダウンロードしインストールできます。これを行う前に、Citrix Cloud 管理コンソールで 1 つまたは複数のリソースの場所を作成して、Cloud Connector を展開する必要があります。リソースの場所について詳しくは、「リソースの場所」を参照してください。

リソースの場所を作成するには

1. Citrix Cloud Connector をインストールする予定のマシンに、Windows 管理者としてサインインします。
2. https://citrix.cloud.comにアクセスして、管理者アカウントにサインインします。
3. Citrix Cloud コンソールで、メインメニューから ［リソースの場所］に移動する、またはページ上部の ［リソースの場所］にある ［編集または新規追加］を選択します。



4. ［リソースの場所］ページの上部にある ［+ リソースの場所］を選択し、わかりやすい新しい名前で保存します。

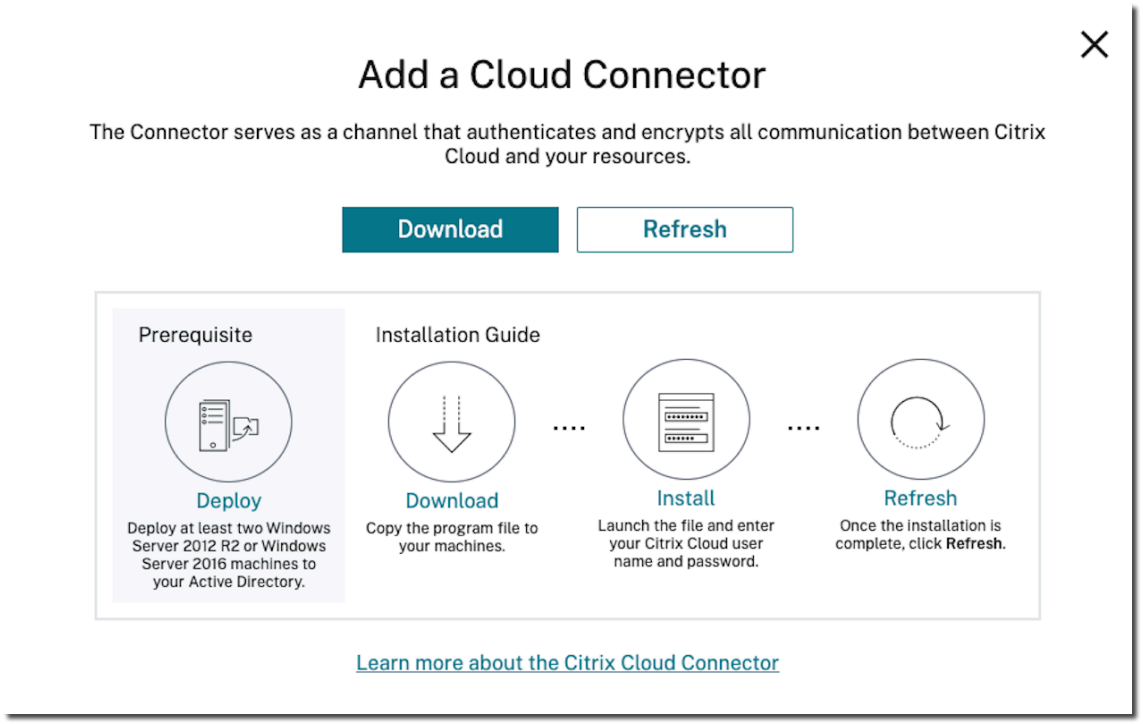


5. Cloud Connector に使用する各マシンで、これらの手順を繰り返します。

Citrix Cloud Connector ソフトウェアのダウンロード

1. 管理するリソースの場所を見つけて ［**+ Cloud Connectors**］を選択します。

2. 開いたウィンドウで ［ダウンロード］を選択します。**cwcconnector.exe** ファイルをコネクタマシンのローカルファイルの場所に保存します。



Citrix Cloud Connector ソフトウェアのインストール

1. **cwcconnector.exe** インストーラーファイルを右クリックして、［管理者として実行］を選択します。インストーラーは、最初の接続性チェックを実行して、Citrix Cloud に接続できることを確認します。
2. メッセージが表示されたら Citrix Cloud にサインインします。
3. Cloud Connector をインストールして構成するには、ウィザードの指示に従います。インストールが完了すると、インストーラーは最終的な接続性チェックを実行して、Cloud Connector と Citrix Cloud 間の通信を検証します。
4. Citrix Cloud Connector として使用する他のマシンで、これらの手順を繰り返します。可用性を高めるため、リソースの場所ごとに Cloud Connector を 2 つ以上インストールすることをお勧めします。

Citrix Cloud では、リソースの場所の ［**Connectors**］ページに、新しくインストールした Cloud Connector が表示されます。

インストール後、Citrix Cloud の ［**ID** およびアクセス管理］**>**［ドメイン］にも管理者のドメインが登録されます。詳しくは、「ID およびアクセス管理」を参照してください。

複数の顧客および既存のリソースの場所でのインストール

複数の顧客アカウントの管理者である場合、Citrix Cloud は、Cloud Connector に関連付ける顧客アカウントを選択するよう要求します。

顧客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 に関連付けるリソースの場所を選択するように求められます。

コマンドラインインストール

サイレントまたは自動インストールがサポートされています。ただし、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。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。

要件

Citrix Cloud 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:

- Citrix Cloud Connector をインストールする Citrix Cloud 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、作成するユーザーと同じレベルの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する必要があります。これは、そのセキュアクライアントにもフルアクセス権限があることを意味します。
- 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、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 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 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。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て表示されます。
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を確保するには、インストーラーに JSON 構成ファイルを提供する必要があります。このファイルは、インストールの完了後に削除する必要があります。構成ファイルでサポートされている値は次のとおりです:

- **customerName**: 必須。[ID およびアクセス管理] の Citrix Cloud コンソールの [API アクセス] ページに表示される顧客 ID。
- **clientId**: 必須。管理者が作成できるセキュアクライアント ID で、[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。[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。

> 注:
>
> パラメーターを使用したクライアント ID とクライアントシークレットの指定はサポートされなくなりました。自動インストールには構成ファイルを使用する必要があります。

次の手順

1. Citrix Cloud Connector の更新スケジュールを設定します。Citrix Cloud Connector の更新と更新スケジュールの管理については、「Connector の更新」を参照してください。
2. ワークスペース利用者を認証するための ID プロバイダーを設定します。**［ID およびアクセス管理］コンソールで、デフォルトの Citrix ID プロバイダーを Active Directory などの ID プロバイダーに変更できます。詳しくは、「Active Directory を Citrix Cloud に接続するには」を参照してください。

インストール問題のトラブルシューティング

このセクションでは、インストール中に発生する可能性がある問題を診断および修正するいくつかの方法について詳しく説明します。インストール問題のトラブルシューティングについて詳しくは、「Citrix Cloud Connector トラブルシューティングガイド」を参照してください。

インストールログ

利用可能なログファイルを最初に調べることで、インストール時に発生した問題のトラブルシューティングを行うことができます。

インストール中に発生したイベントは、**Windows** イベントビューアーで確認できます。**%LOCALAPPDATA%\Temp\CitrixLogs\CloudServicesSetup** にある Cloud Connector のインストールログを確認することもできます。
また、インストール後は**%ProgramData%\Citrix\WorkspaceCloud\InstallLogs** にもログが追加されます。

終了コード

インストールプロセスの成功または失敗に応じて、次の終了コードが返されることがあります:

- 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

インストールエラー

インストーラーをダブルクリックして Citrix Cloud Connector ソフトウェアをインストールすると、次のエラーメッセージが表示される場合があります:

```
Can't reach this page.
```

このエラーは、管理者としてマシンにログインして Citrix Cloud Connector をインストールする場合でも発生することがあります。このエラーを回避するには、インストーラーを右クリックして［管理者として実行］を選択し、Citrix Cloud Connector ソフトウェアを管理者として実行します。

接続エラー

Cloud Connector が Citrix Cloud と通信できていることを確認するには、以下の Citrix サービスが ［開始］状態になっていることを確認します:

- Citrix Cloud AD Provider
- Citrix Cloud Agent Logger
- Citrix Cloud Agent System
- Citrix Cloud Agent Watchdog
- Citrix Cloud Credential Provider
- Citrix Config Synchronizer Service
- Citrix High Availability Service
- Citrix NetScaler Cloud Gateway
- Citrix Remote Broker Provider
- Citrix Remote HCL Server
- Citrix Session Manager Proxy

これらのサービスについて詳しくは、「インストールされているサービス」を参照してください。

接続エラーが引き続き発生する場合は、Citrix Support Knowledge Center で入手できる Cloud Connector 接続チェックユーティリティを使用してください。詳しくは、Knowledge Center Web サイトの「CTX260337」を参照してください。

このツールを使用して、次のタスクを実行できます:

- Citrix Cloud とその関連サービスにアクセスできるかどうかのテスト。
- 誤って構成されがちな設定のチェック。
- Citrix Cloud Connector のプロキシ設定の構成。

失敗した接続性チェックを解決する方法について詳しくは、「CTX224133: Cloud Connector 接続性チェックエラー」を参照してください。

Citrix Cloud Connector のログ収集

June 7, 2021

CDF ログは、シトリックス製品内のトラブルシューティングを目的として使用されます。シトリックスサポートは、CDF トレースを使用して、アプリケーションとデスクトップの仲介、ユーザー認証、Virtual Delivery Agent（VDA）登録に関する問題を特定します。この記事では、環境で発生する可能性のある問題のトラブルシューティングと解決に使用できる Cloud Connector データをキャプチャする方法について説明します。

> 重要な注意事項:
>
> - リソースの場所にあるすべての Cloud Connector マシンでログを有効にします。
> - データの全範囲を確実にキャプチャするために、VDA にある CDFControl キャプチャツールを使用することをお勧めします。詳しくは、Citrix Support Knowledge Center のCTX111961を参照してください。Citrix Workspace アプリのログ収集について詳しくは、CTX141751を参照してください。
> - CDF トレースをシトリックスに送信するには、シトリックスサポートケースが開かれている必要があります。シトリックスのサポート技術者は、既存のサポートケースに添付されていない CDF トレースを確認することはできません。

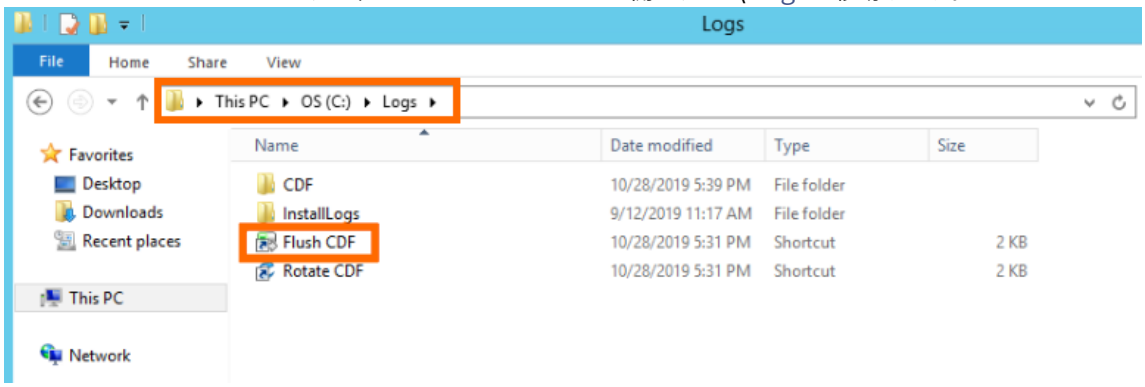
手順 1: 問題を再現する

この手順では、使用環境で発生している問題を再現します。問題がアプリの起動または仲介に関連している場合は、起動の失敗を再現します。問題が VDA 登録に関連している場合は、VDA マシンで Citrix Desktop Service を手動で再起動して、再度 VDA 登録の作成を試みます。

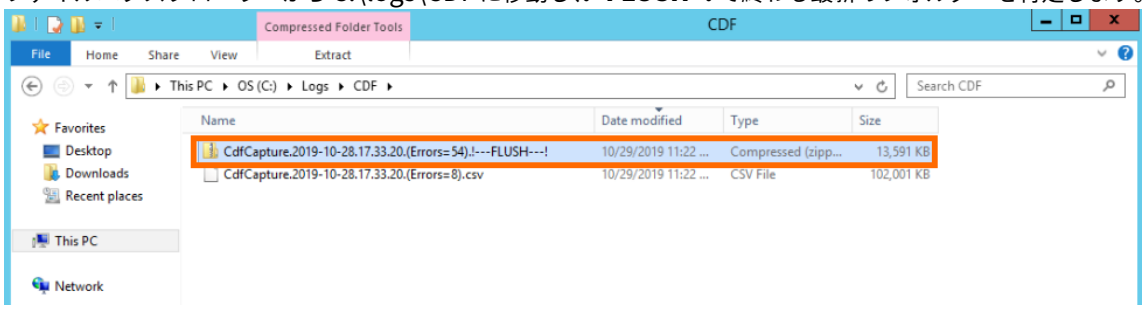
手順 2: CDF トレースを収集する

この手順では、リソースの場所にある各 Cloud Connector から CDF フラッシュトレースを収集します。

1. ドメイン管理者またはローカル管理者アカウントを使用して RDP 接続を開始することにより、Cloud Connector マシンにアクセスします。
2. Cloud Connector マシンで、ファイルエクスプローラーを開き、`C:\logs`に移動します。



3. フラッシュ **CDF** を実行します。Cloud Connector マシンのタスクバーにアイコンが短時間表示された後、消えます。
4. ファイルエクスプローラーから C:\logs\CDF に移動し、**!–FLUSH–!** で終わる最新のフォルダーを特定します。

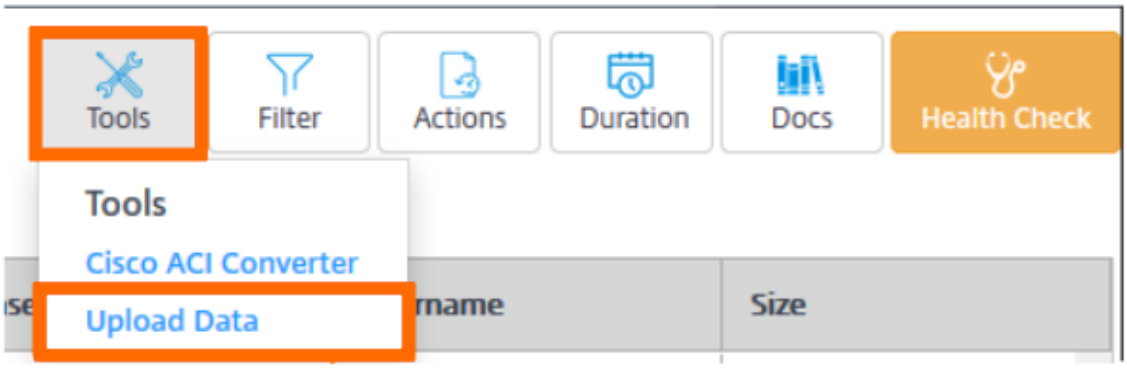


5. リソースの場所にあるすべての Cloud Connector マシンで手順 1～5 を実行し、すべての Cloud Connector のフラッシュトレースを 1 つの ZIP アーカイブに結合します。すべての Cloud Connector マシンからフラッシュトレースの ZIP アーカイブを作成しない場合は、一度に 1 ファイルずつシトリックスに送信する必要があります。

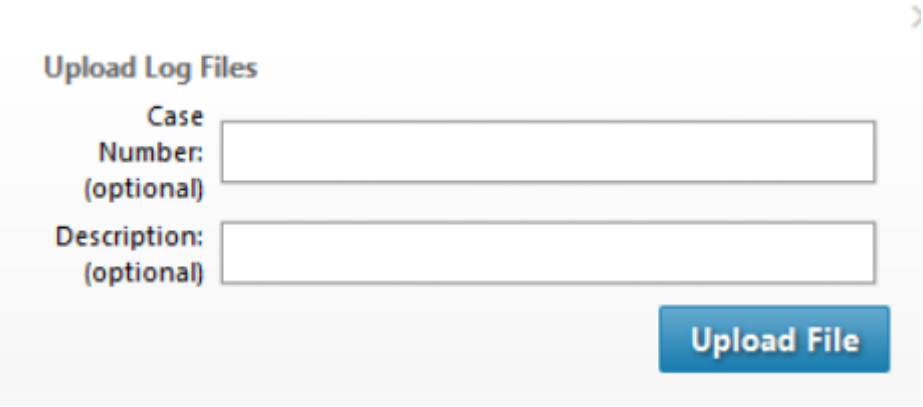
手順 **3**：シトリックスにデータを送信する

この手順では、トレースファイルをシトリックスサポートケースに添付し、レビューのために送信します。

1. https://cis.citrix.com/にアクセスし、Citrix.com の資格情報を使用してサインインします。
2. [**Diagnostics**] を選択します。
3. [**Tools**]、[**Upload Data**] の順に選択します。



4. [**Case Number**] に、既存のサポートケースのシトリックスサポートケース番号を入力してください。シトリックスサポート技術者は、データのアップロードにケース番号が添付されていないと、CDF トレースを適切に確認できません。



5. ［説明（オプション）］には簡単な説明を入力するか、このフィールドを空白のままにすることができます。
6. ［**Upload File**］を選択し、前に作成した ZIP アーカイブを選択します。すべての Cloud Connector マシンからフラッシュトレースの ZIP アーカイブを作成しなかった場合は、手順 3〜6 を繰り返して、送信する各フラッシュトレースを添付します。

フラッシュトレースを送信すると、Citrix Insight Services はそれらを処理し、指定したサポートケースに添付します。このプロセスは、ファイルのサイズによっては最大 24 時間かかる場合があります。

クラウドサービス用のコネクタアプライアンス

September 17, 2021

コネクタアプライアンスは、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。コネクタアプライアンスを使用することで、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。

コネクタアプライアンスは、次の機能を備えています：

- **Citrix Workspace** マイクロアプリサービスは、アプリケーションからのアクションと通知を Workspace または他のチャネルに提供します。

  アプリケーションデータソースからマイクロアプリサービスへの統合を構築し、アプリケーションから Workspace へアクションをプルします。次にマイクロアプリが提供する、アクションを実行可能なフォームや通知でソースシステムにライトバックし、アプリケーションワークフローが完了します。詳しくは、「マイクロアプリ」を参照してください。

  Citrix Workspace マイクロアプリサービスは、コネクタアプライアンスを使用して、次の場所からコンテンツを配信します：

  - オンプレミスのアプリケーション
  - リソースの場所経由で接続する外部システム

コネクタアプライアンスを使用する Technical Preview 段階のサービスがほかにも存在する可能性があります。

コネクタアプライアンス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コネクタアプライアンスをインストールします。各リソースの場所に少なくとも 2 つのコネクタアプライアンスを使用することをお勧めします。あるコネクタアプライアンスを一定期間使用できない場合、他のコネクタアプライアンスがその接続を維持できます。各コネクタアプライアンスはステートレスであるため、使用可能なすべてのコネクタアプライアンス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 つのコネクタアプライアンスが利用可能である限り、Citrix Cloud との通信は失われません。

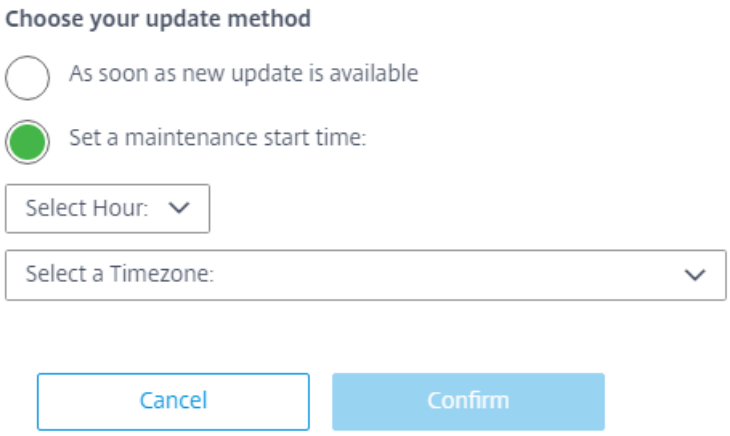
リソースの場所に対してコネクタが 1 つのみ構成されている場合、Citrix Cloud では ［リソースの場所］ページと［コネクタ］ページの両方に警告が表示されます。

コネクタアプライアンスのアップデート

コネクタアプライアンスは自動的にアップデートされます。コネクタをアップデートするためにアクションを実行する必要はありません。

アップデート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。保守期間を構成するには:

1. リソースの場所の省略記号メニューから ［リソースの場所の管理］を選択します。
2. ［更新方法を選択します］セクションで、［保守開始時刻を設定］を選択します。
3. 一覧から開始時間とタイムゾーンを選択します。
4. ［確認］をクリックします。



アップデート中に、コネクタアプライアンスを一時的に利用できなくなります。自動アップデートでは、リソースの場所のコネクタアプライアンスのみが 1 つずつのみアップデートされます。そのため、各リソースの場所に少なくとも 2 つのコネクタアプライアンスを登録し、少なくとも 1 つのコネクタアプライアンスを常に利用できるようにすることが重要です。

コネクタアプライアンスの通信

コネクタアプライアンスは、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、コネクタアプライアンス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コネクタアプライアンスからクラウドに対して確立されます。受信接続は受け入れられません。

コネクタアプライアンス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。コネクタアプライアンスの登録時に 1 つ以上の Web プロキシを定義すると、コネクタアプライアンス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、コネクタアプライアンス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。

コネクタアプライアンスでは、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.com
- https://*.citrixworkspacesapi.net
- https://*.citrixnetworkapi.net
- https://*.nssvc.net
- https://*.servicebus.windows.net
- https://iwsprodeastusuniconacr.azurecr.io
- https://iwsprodeastusuniconacr.eastus.data.azurecr.io

システム要件

コネクタアプライアンスは、次のハイパーバイザーでサポートされています:

- Citrix XenServer 7.1 CU2 LTSR
- Citrix Hypervisor 8.2 LTSR
- VMware ESXi バージョン 6.5
- Windows Server 2016 または Windows Server 2019 上の Hyper-V

- Microsoft Azure

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:

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

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、コネクタアプライアンスが DHCP を使用して DNS 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。
- このネットワークは、コネクタアプライアンス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）に設定されており、タイムサーバーと同期されています。
- コネクタアプライアンス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必要があります。

同じハイパーバイザーホストで複数のコネクタアプライアンスをホストできます。同じホスト上のコネクタアプライアンスの数は、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。

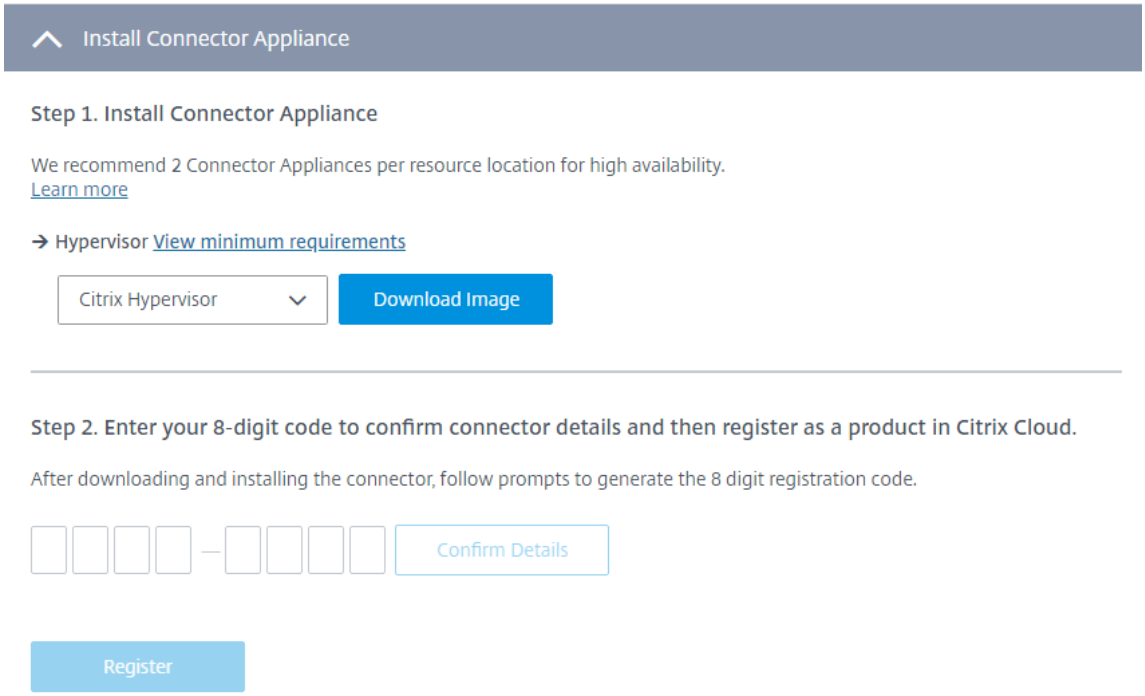
> 注:
>
> コネクタアプライアンス VM のスナップショットの複製、一時停止、および作成はサポートされていません。

コネクタアプライアンスの入手

Citrix Cloud 内からコネクタアプライアンス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. コネクタアプライアンスを登録するリソースの場所で、［コネクタアプライアンス］プラスアイコン（+）をクリックします。

   ［コネクタアプライアンスのインストール］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、コネクタアプライアンスをホストするために使用するハイパーバイザーのタイプを選択します。［画像のダウンロード］をクリックします。
6. シトリックス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。
7. プロンプトが表示されたら、提供されたコネクタアプライアンスファイルを保存します。

   コネクタアプライアンス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。
8. ［コネクタアプライアンスのインストール］タスクは開いたままにします。コネクタアプライアンス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 ［コネクタアプライアンスのインストール］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、コネクタアプライアンスを追加します。

ハイパーバイザーへのコネクタアプライアンスのインストール

Citrix Cloud からダウンロードした XVA、OVA、または ZIP ファイルには、ハイパーバイザーでホストできる自己完結型コネクタアプライアンスが含まれます。

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

Citrix Hypervisor

このセクションでは、XenCenter を使用して Citrix Hypervisor サーバーにコネクタアプライアンスをインポートする方法について説明します。

1. ダウンロードしたコネクタアプライアンス 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. コネクタアプライアンスの 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. コネクタアプライアンスをホストする Citrix Hypervisor サーバーを選択します。また、コネクタアプライアンス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. コネクタアプライアンス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、使用するコネクタアプライアンスのネットワークを選択します。［次へ］をクリックします。
7. コネクタアプライアンス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。

コネクタアプライアンスが展開され、正常に起動すると、そのコンソールにコネクタアプライアンスの 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コネクタアプライアンスに接続し、インストールプロセスを続行します。

デフォルトでは、コネクタアプライアンスは 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、コネクタアプライアンス UI にアクセスする前に、コネクタアプライアンス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、「コネクタアプライアンス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：コネクタアプライアンスを 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 ホストにコネクタアプライアンスを展開する方法について説明します。

1. ダウンロードしたコネクタアプライアンスの 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. コネクタアプライアンスの 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. コネクタアプライアンス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。コネクタアプライアンス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. コネクタアプライアンス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. コネクタアプライアンス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。

コネクタアプライアンスが展開され、正常に起動すると、そのコンソールにコネクタアプライアンスの 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コネクタアプライアンスに接続し、インストールプロセスを続行します。

デフォルトでは、コネクタアプライアンスは 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、コネクタアプライアンス UI にアクセスする前に、コネクタアプライアンス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、「コネクタアプライアンス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：コネクタアプライアンスを Citrix Cloud に登録する。

Hyper-V

このセクションでは、Hyper-V ホストでコネクタアプライアンス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コネクタアプライアンスの展開

1. Hyper-V ホストに接続します。
2. コネクタアプライアンスの 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 ファイルの内容を抽出：PowerShell スクリプトおよび`connector-appliance.vhdx`ファイル。
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。たとえば、`C:\ConnectorApplianceVMs`などです。
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］パネルでコネクタアプライアンスを識別する一意の名前を［名前］フィールドに入力します。［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］パネルで以下を実行します：

    a) 4GB の RAM を割り当てる
    b) 動的メモリを無効にする

    ［次へ］をクリックします。

10. ［ネットワークの構成］パネルで一覧からスイッチを選択します。たとえば、［既定のスイッチ］などです。［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］パネルでコネクタアプライアンス 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］に移動します。［仮想プロセッサの数］の値を 2 に変更します。［適用］をクリックし、［**OK**］をクリックします。
16. ［仮想マシン］パネルで作成したコネクタアプライアンス VM を右クリックして、［開始］を選択します。
17. コネクタアプライアンス 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。

コネクタアプライアンス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コネクタアプライアンスの IP アドレスが表示されます。この IP アドレスを使用してコネクタアプライアンスに接続し、インストールプロセスを続行します。

デフォルトでは、コネクタアプライアンスは 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、コネクタアプライアンス UI にアクセスする前に、コネクタアプライアンス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、「コネクタアプライアンス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：コネクタアプライアンスを Citrix Cloud に登録する。

PowerShell スクリプトを使用したコネクタアプライアンスの展開

`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. コネクタアプライアンスの 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
```


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 キーを押してデフォルト値 **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、また Enter キーを押してデフォルト値`connector-appliance.vhdx`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 キーを押します。
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。

   スクリプトがコネクタアプライアンス VM を作成し、起動します。

コネクタアプライアンスが展開され、正常に起動すると、そのコンソールにコネクタアプライアンスの 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コネクタアプライアンスに接続し、インストールプロセスを続行します。

次の手順：コネクタアプライアンスを Citrix Cloud に登録する。

Microsoft Azure

このセクションでは、Microsoft Azure でコネクタアプライアンス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、VM を展開できます。

`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。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. コネクタアプライアンスの 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ディレクトリを変更して、次のコマンドを実行します：

   ```
   1 .\connector-appliance-upload.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。資格情報を入力します。
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。

コネクタアプライアンスが展開され、正常に起動すると、そのコンソールにコネクタアプライアンスの 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コネクタアプライアンスに接続し、インストールプロセスを続行します。

次の手順：コネクタアプライアンスを Citrix Cloud に登録する。

Google Cloud Platform

このセクションでは、Google Cloud Platform でコネクタアプライアンスを展開する方法について説明します。

connector-appliance-gcp.zipファイルには、コネクタアプライアンスのディスクイメージであるconnector-appliance.tar.gzファイルと、コネクタアプライアンスを自動的に展開するために使用できる PowerShell スクリプトが含まれています。

Google Cloud Platform コンソールを使用したコネクタアプライアンスの展開

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) [**Create**] 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、コネクタアプライアンスインスタンスの名前を入力します。
    b) コネクタアプライアンス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、作成したばかりの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、コネクタアプライアンス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。

    [**Create**] 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。

コネクタアプライアンスが展開され、正常に起動すると、[**VM Instances**] セクションにコネクタアプライアンスの IP アドレスが表示されます。

コネクタアプライアンスに外部 IP アドレスがある場合は、この IP アドレスを使用して、Web ブラウザーからコネクタアプライアンス管理ページに移動し、インストールプロセスを続行できます。

コネクタアプライアンスに内部 IP アドレスしかない場合は、踏み台ホストを使用して、Web ブラウザーからコネクタアプライアンス管理ページに移動し、インストールプロセスを続行します。詳しくは、「https://cloud.google.com/compute/docs/instances/connecting-advanced#bastion_host」を参照してください。

次の手順: コネクタアプライアンスを Citrix Cloud に登録する。

PowerShell スクリプトを使用したコネクタアプライアンスの展開

提供されている PowerShell スクリプトを使用してコネクタアプライアンスを展開するには、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. `.\connector-appliance-upload-GCP.ps1`コマンドを実行します。
4. 開いた Web ブラウザーのウィンドウで、コネクタアプライアンス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。

コネクタアプライアンスが展開され、正常に起動すると、スクリプトによりコネクタアプライアンスの内部 IP アドレスが表示されます。または、Google Cloud Platform コンソールで、コネクタアプライアンスの内部 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、コネクタアプライアンスの 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 アドレスにあるコネクタアプライアンス管理ページに移動し、インストールプロセスを続行します。詳しくは、「https://cloud.google.com/compute/docs/instances/connecting-advanced#bastion_host」を参照してください。

次の手順：コネクタアプライアンスを Citrix Cloud に登録する。

コネクタアプライアンスを **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、コネクタアプライアンスを Citrix Cloud に登録します。

コネクタアプライアンスをハイパーバイザーにインストールして起動すると、コンソールにコネクタアプライアンスの IP アドレスが表示されます。コンソールには、コネクタアプライアンス 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. コネクタアプライアンスの 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。

   コネクタアプライアンス UI は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。コネクタアプライアンス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。

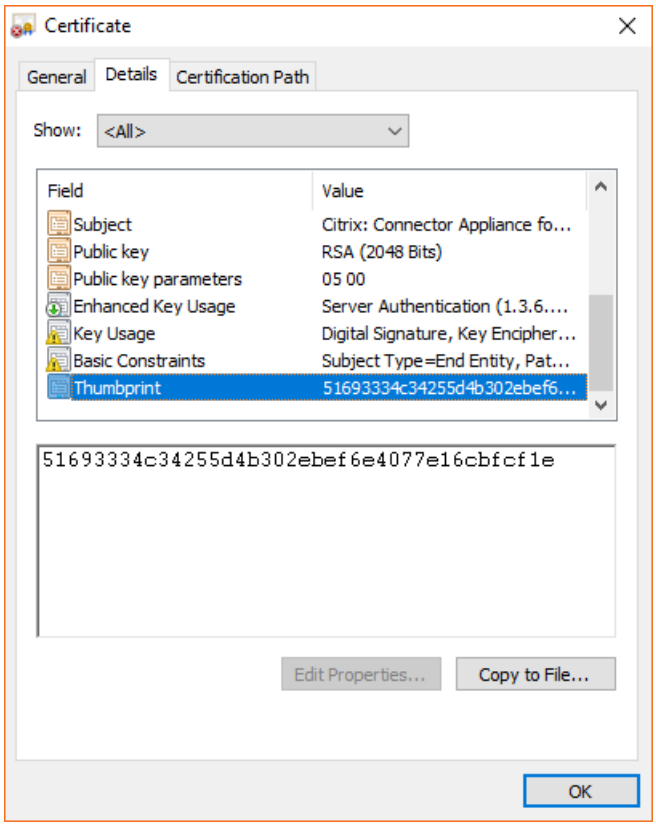
   たとえば、Google Chrome ブラウザーで、以下の手順を実行します:

   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。

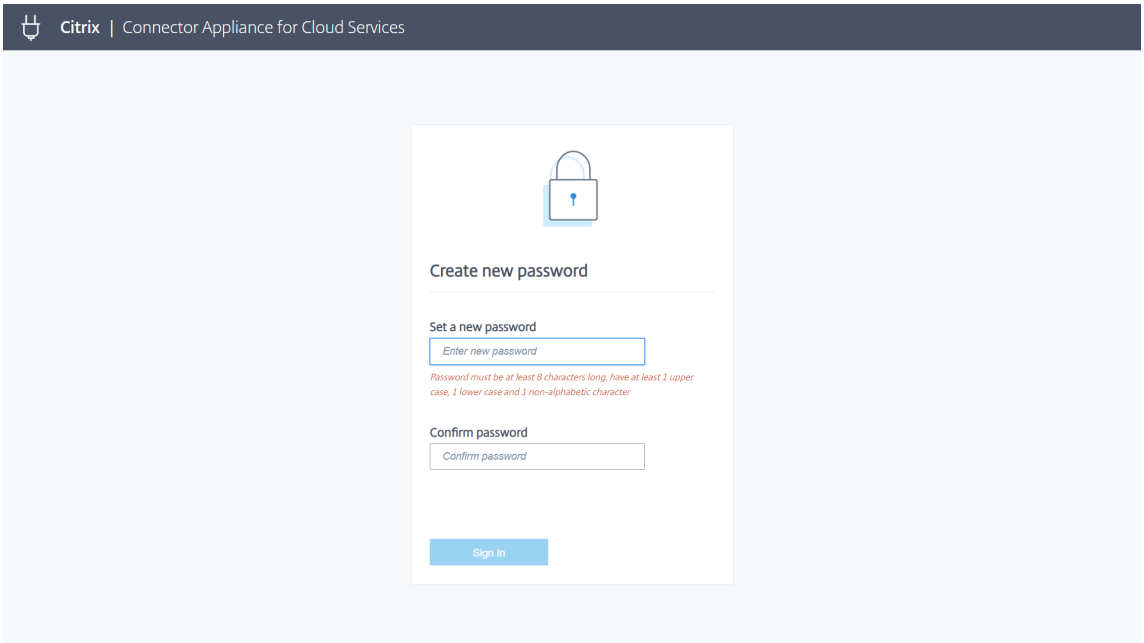
      拇印フィールドの値とコンソールで提供された SSL フィンガープリントが一致する場合、ブラウザーがコネクタアプライアンス UI に直接接続していることを確認できます。



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. コネクタアプライアンス 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。



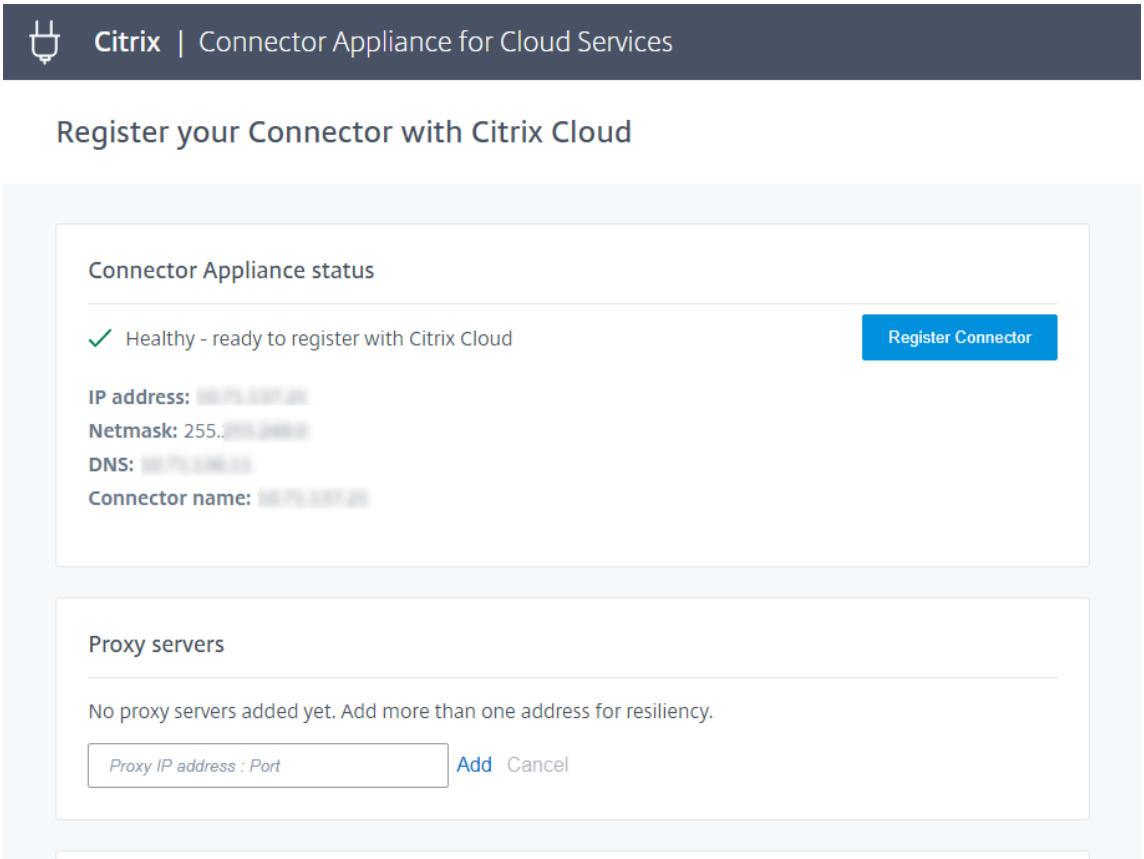
設定するパスワードは次の要件を満たしている必要があります:

- 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. ここで設定したパスワードでサインインします。

［コネクタアプライアンス管理ページ］が開きます。



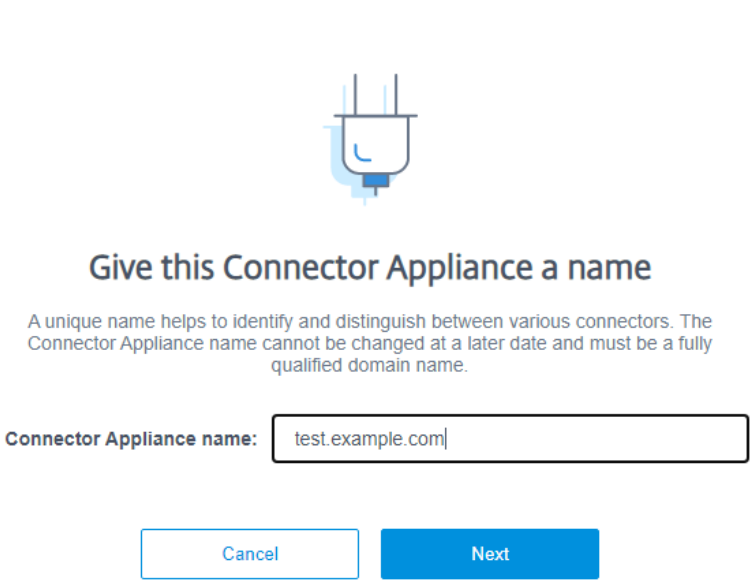
5. （オプション）1 つ以上の Web プロキシを使用する場合、ここでプロキシアドレスを追加できます。認証されていないプロキシのみがサポートされています。

   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、「コネクタアプライアンスの通信」を参照してください。

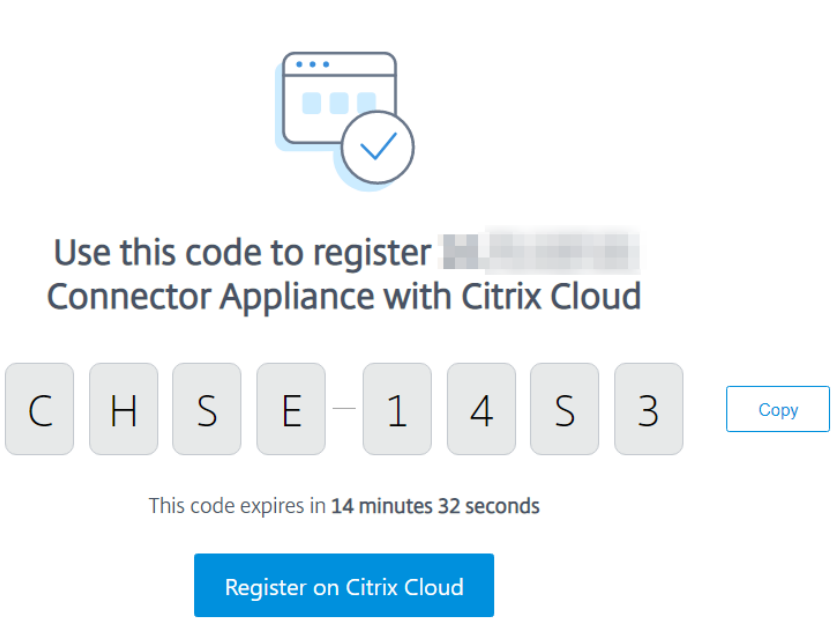
6. ［コネクタの登録］をクリックして、登録タスクを開きます。

7. コネクタアプライアンス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コネクタアプライアンスを区別するのに役立ちます。コネクタアプライアンスを登録した後は、名前を変更することはできません。

   ［コネクタアプライアンス名］フィールドに名前を入力し、［次へ］をクリックします。



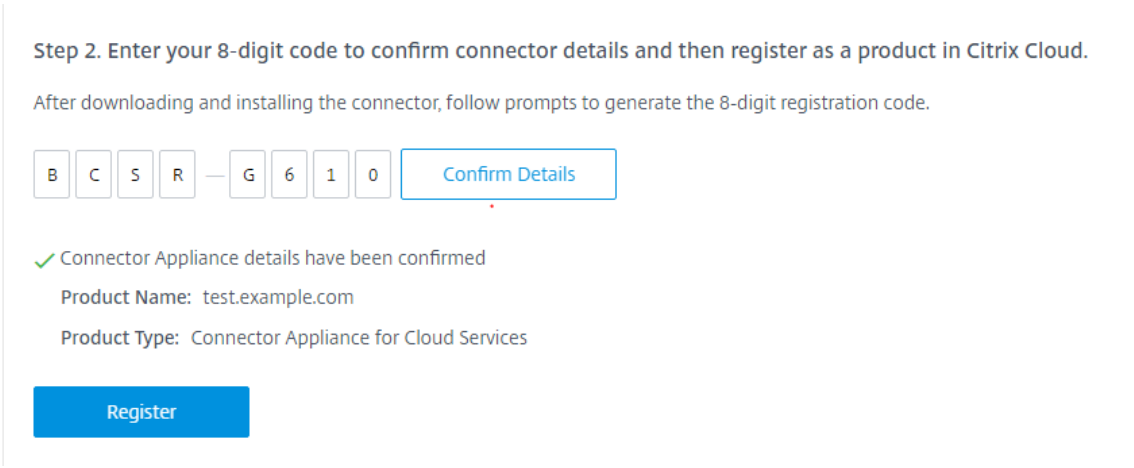
Web ページで、Citrix Cloud での登録に使用するコードが提供されます。このコードは 15 分で期限切れになります。



8. ［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。
9. ［リソースの場所］ Web ページに戻ります。
10. ［コネクタアプライアンスのインストール］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、コネクタアプライアンスが存在し、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。



11. ［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。

12. ［閉じる］をクリックします。

［コネクタアプライアンス管理ページ］では、コネクタアプライアンス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。

コネクタアプライアンスの登録後

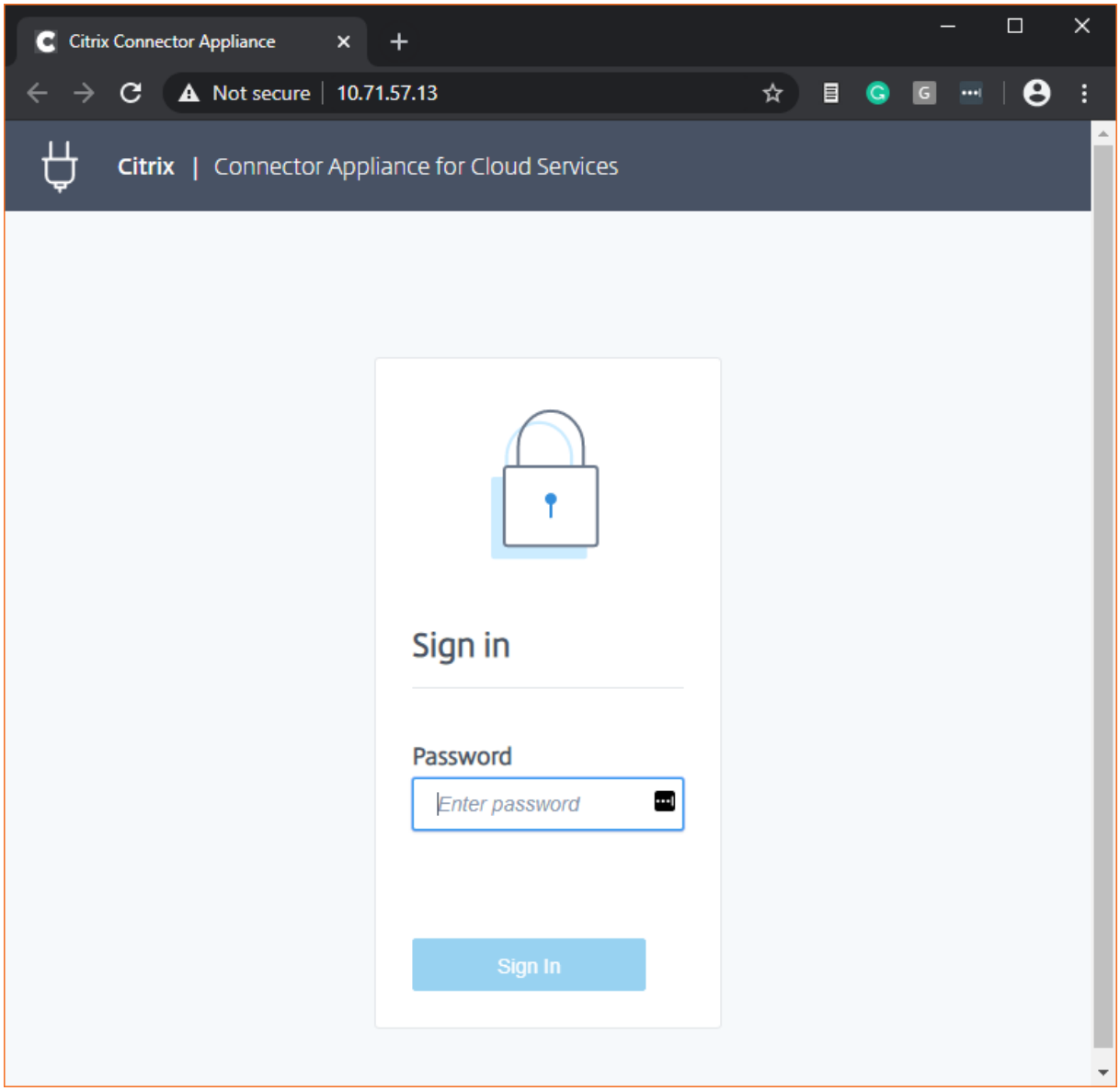
各リソースの場所で、2 つ以上のコネクタアプライアンスをインストールして登録することをお勧めします。この構成により、継続的な可用性が確保され、コネクタ間で負荷を分散できます。

コネクタアプライアンスを直接管理することはできません。

コネクタアプライアンスは自動的にアップデートされます。コネクタをアップデートするためにアクションを実行する必要はありません。コネクタアプライアンス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。詳しくは、「コネクタの更新」を参照してください。

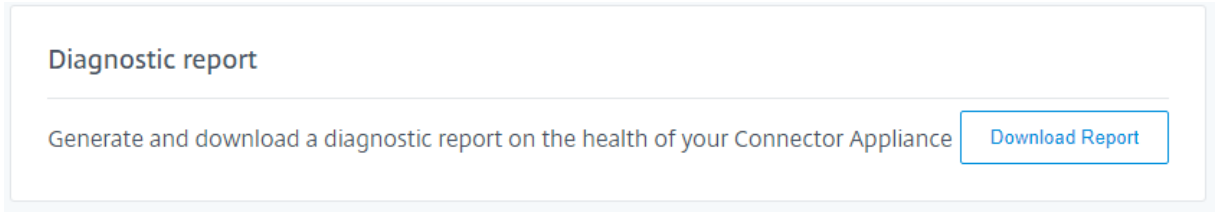
コネクタアプライアンス VM のスナップショットを複製、一時停止、作成しないでください。これらの操作はサポートされていません。

コネクタアプライアンス 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。その後の UI への接続では、コネクタアプライアンス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

［コネクタアプライアンス管理ページ］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コネクタアプライアンスコンソールから、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. コネクタアプライアンス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。

コネクタアプライアンスのネットワーク設定

デフォルトでは、コネクタアプライアンスの 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 を使用してコネクタアプライアンスを登録した後、［コネクタアプライアンス管理ページ］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 ［コネクタアプライアンス管理ページ］へのアクセス権限がない場合は、コネクタアプライアンスコンソールで直接ネットワーク構成を設定できます。

コネクタアプライアンス管理ページでのネットワーク設定の構成

DHCP を使用してコネクタアプライアンスを登録した後、［コネクタアプライアンス管理ページ］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、コネクタアプライアンスが再起動します。再起動中、コネクタアプライアンスは一時的に使用できなくなります。［コネクタアプライアンス管理ページ］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、コネクタアプライアンスコンソール内で、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、コネクタアプライアンスが再起動します。再起動中、コネクタアプライアンスは一時的に使用できなくなります。［コネクタアプライアンス管理ページ］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、コネクタアプライアンスコンソール内で、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。

コネクタアプライアンス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、コネクタアプライアンスの 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［コネクタアプライアンス管理ページ］へのアクセス権限がない場合は、コネクタアプライアンス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、コネクタアプライアンスを再起動します。
2. コネクタアプライアンスの起動中に、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、新しい構成でコネクタアプライアンスを起動します。

Connector の更新

September 17, 2021

Citrix では、Cloud Connector またはコネクタアプライアンスのパフォーマンス、セキュリティ、および信頼性を強化するためのアップデートを定期的にリリースしています。デフォルトでは、これらのアップデートが利用可能になるとすぐ、Citrix Cloud により各コネクタに対して 1 つずつインストールされます。ユーザーの Citrix Cloud エクスペリエンスに過度の影響を与えることなく、アップデートがタイムリーにインストールされるようにするため、希望する時刻と希望する曜日にこれらのアップデートをスケジュールできます。リソースの場所にある現在のコネクタのバージョンを Citrix Cloud の対象バージョンと比較することで、コネクタが最新であることを確認することもできます。

希望する時刻

希望する時刻を指定すると、Citrix Cloud は、アップデートが利用可能になってから 24 時間後の希望する時刻に更新をインストールします。たとえば、希望の時刻を午前 2:00（米国太平洋時間）に設定してあり、火曜日にアップデートが利用可能になった場合、Citrix Cloud は 24 時間待機してから、翌日の午前 2:00 にアップデートをインストールします。

希望する曜日

希望する曜日を指定すると、Citrix Cloud は 7 日間待機してから、希望する曜日にアップデートをインストールします。この 7 日間の待機期間により、アップデートをオンデマンドでインストールするか、Citrix Cloud が希望の曜日にインストールするのを待つかを選択する十分な時間が与えられます。選択した曜日とアップデートが利用可能になる曜日によっては、Citrix Cloud はアップデートのインストールを最大 13 日間待機する場合があります。

待機期間が **8** 日間になる場合の例

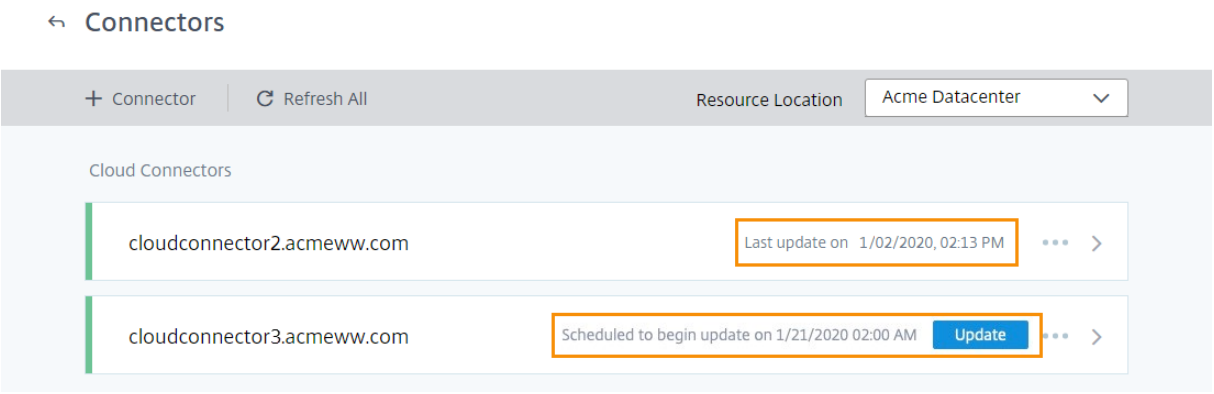
月曜日に、アップデートの希望日時を火曜日の午後 6:00 に設定しました。その日遅く、Citrix Cloud は利用可能なアップデートがあることを通知し、［アップデート］ボタンを表示します。そこでアップデートをしない場合、Citrix Cloud は 7 日間待機し、翌火曜日にアップデートをインストールします。

待機期間が **13** 日間になる場合の例

アップデートの希望日時を月曜日の午後 6:00 に設定しました。火曜日に、Citrix Cloud は利用可能なアップデートがあることを通知し、［アップデート］ボタンを表示します。そこでアップデートをしない場合、Citrix Cloud は 7 日間待機してから、6 日後の月曜日の午後 6:00 にアップデートをインストールします。

アップデートの通知とオンデマンドアップデート

アップデートが利用可能になると、Citrix Cloud は「通知」に記載された設定で通知します。また、各コネクタには、アップデートのインストール日時が表示されます。

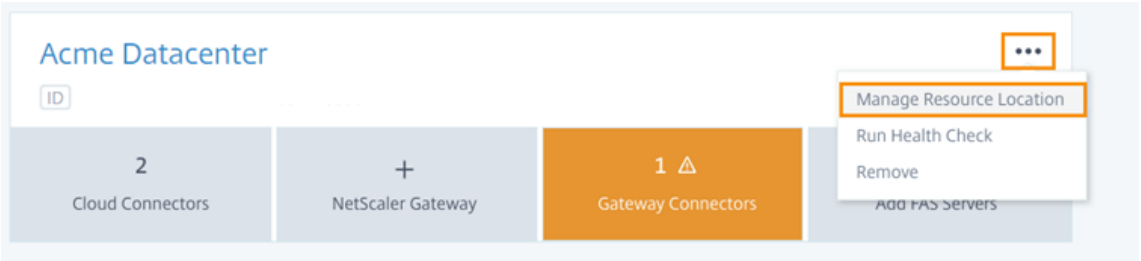


Citrix Cloud からアップデートが利用可能になったという通知が出されると、各コネクタに ［アップデート］ボタンが表示されるため、希望する日時よりも早くアップデートをインストールできます。コネクタごとの ［アップデート］を選択すると、Citrix Cloud はそれらのアップデートをキューに入れ、一度に 1 つずつインストールしていきます。アップデートを開始した後は、アップデートをキャンセルできません。

アップデートが完了すると、Citrix Cloud は最後にアップデートした日付を表示します。一部のアップデートが完了できない場合は、通知が送信されます。

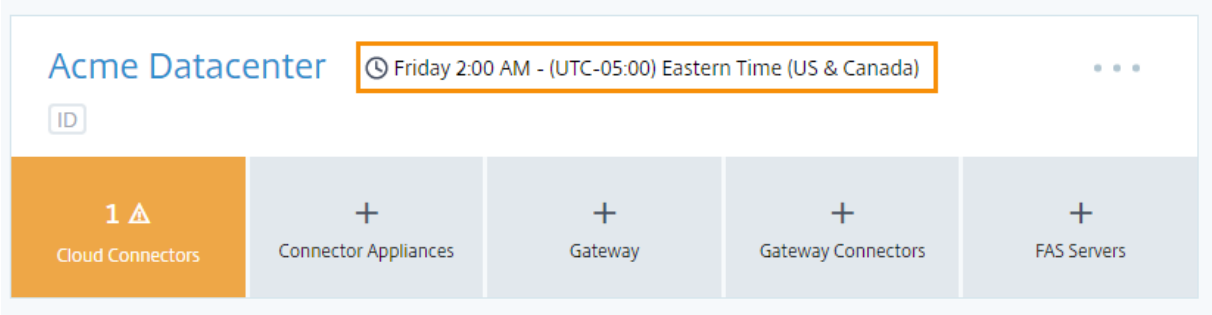
アップデートスケジュールの選択

1. Citrix Cloud メニューから ［リソースの場所］を選択します。
2. 変更するリソースの場所を見つけ、省略記号メニューから ［リソースの場所の管理］を選択します。



3. ［更新方法を選択します］から ［保守開始時刻を設定］を選択し、アップデートをインストールする希望の曜日、時刻、タイムゾーンを選択します。
   - 希望の時刻のみを指定するには、アップデートをインストールする時間とタイムゾーンを選択します。Citrix Cloud は、アップデートが利用可能になってから 24 時間後の希望する時刻に更新をインストールします。
   - 希望する曜日を指定するには、時刻、曜日、タイムゾーンを選択します。Citrix Cloud は、アップデートが利用可能になってから 7 日間待機した後、希望の曜日にインストールします。

アップデートスケジュールを構成すると、Citrix Cloud はリソースの場所の名前の横にアップデートスケジュールを表示します。



選択した開始時刻は、適用されるタイムゾーンに関係なく、すべてのコネクタに適用されます。コネクタが複数のタイムゾーンに存在する場合、Citrix Cloud により選択した時刻とタイムゾーンでアップデートがインストールされます。たとえば、アップデートを米国太平洋時間の午前 2 時にスケジュールし、コネクタがロンドンにある場合、Citrix Cloud ではこれらのコネクタに対するアップデートのインストールを米国太平洋時間の午前 2 時に開始します。

> 注:
>
> アップデートのインストール中にコネクタで問題が発生した場合、問題が解決されるまでインストールが一時停止します。アップデートは各コネクタに一度に 1 つずつインストールされるため、1 つのコネクタでアップデートを一時停止すると、Citrix Cloud アカウントに残っているすべてのコネクタのアップデートが妨げられる可能性があります。

計画外アップデート

アップデートをインストールする希望の時刻または曜日を選択した場合でも、Citrix Cloud により利用可能になったアップデートが即時にインストールされる場合があります。計画外アップデートは、次のような状況で行われます:

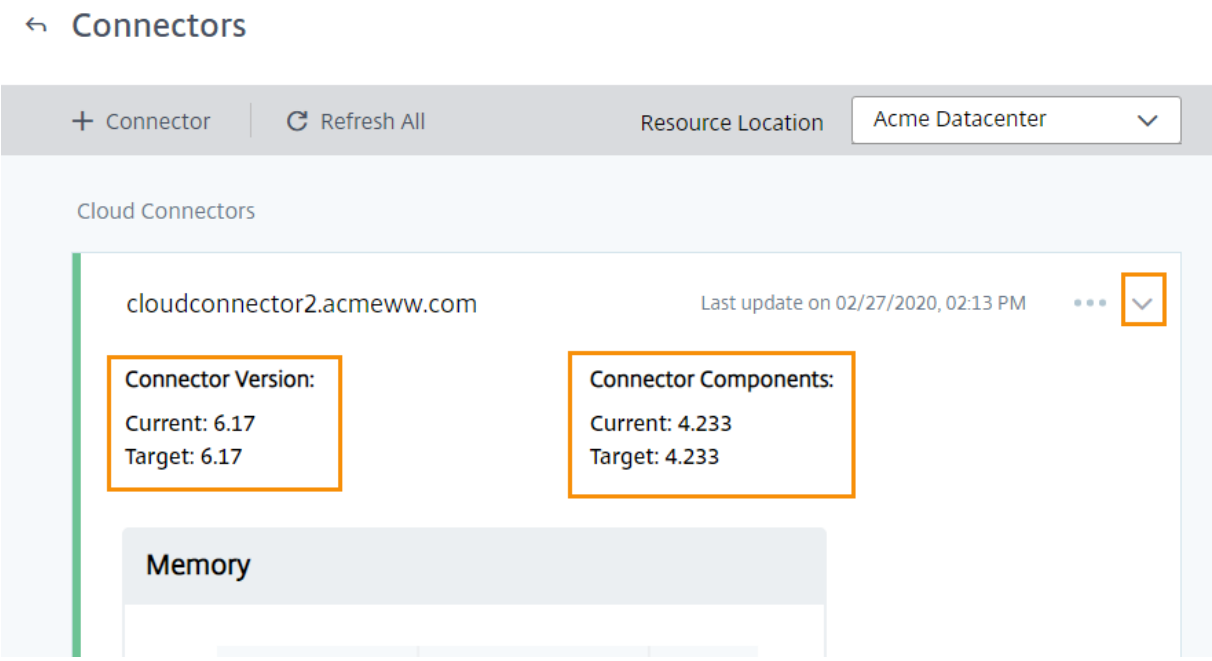
- アップデートを利用可能になってから 48 時間以内に希望の時刻でインストールできない。たとえば、希望時刻が午前 2 時で、コネクタがアップデートのリリース後 3 日間オフラインになった場合、コネクタがオンラインに戻ると Citrix Cloud によって即時にアップデートがインストールされます。
- アップデートには、セキュリティまたは機能に関する重大な問題に対する修正が含まれている。

Cloud Connector のバージョンの比較

リソースの場所で実行されている Cloud Connector のバージョンと、それが最新バージョンであるかどうかを確認できます。この情報は、Cloud Connector が正常に更新されていることを確認するのに役立ちます。

> 注:
>
> この内容は、コネクタアプライアンスでは利用できません。

[リソースの場所] ページから、管理するリソースの場所の [**Cloud Connectors**] タイルを選択します。次に、Cloud Connector のタイルを展開します。



［現在］のバージョン番号は、Cloud Connector マシンで現在実行されている Cloud Connector ソフトウェアのバージョンです。［ターゲット］のバージョン番号は、シトリックスがリリースした Cloud Connector ソフトウェアの最新バージョンです。マシンが正常に更新された場合、［現在］と［ターゲット］のバージョン番号は一致します。

更新エラーのトラブルシューティング

Cloud Connector マシンにインストールされているソフトウェアの競合、または保守中の予期しないエラーにより、Cloud Connector が更新に失敗してサービスが停止することがあります。Cloud Connector の保守後に更新に失敗した場合の対処方法については、「Cloud Connector の保守に失敗した際の解決方法」を参照してください。

Cloud Connector が正常に更新されない場合は、次の条件を確認して問題のトラブルシューティングを開始できます:

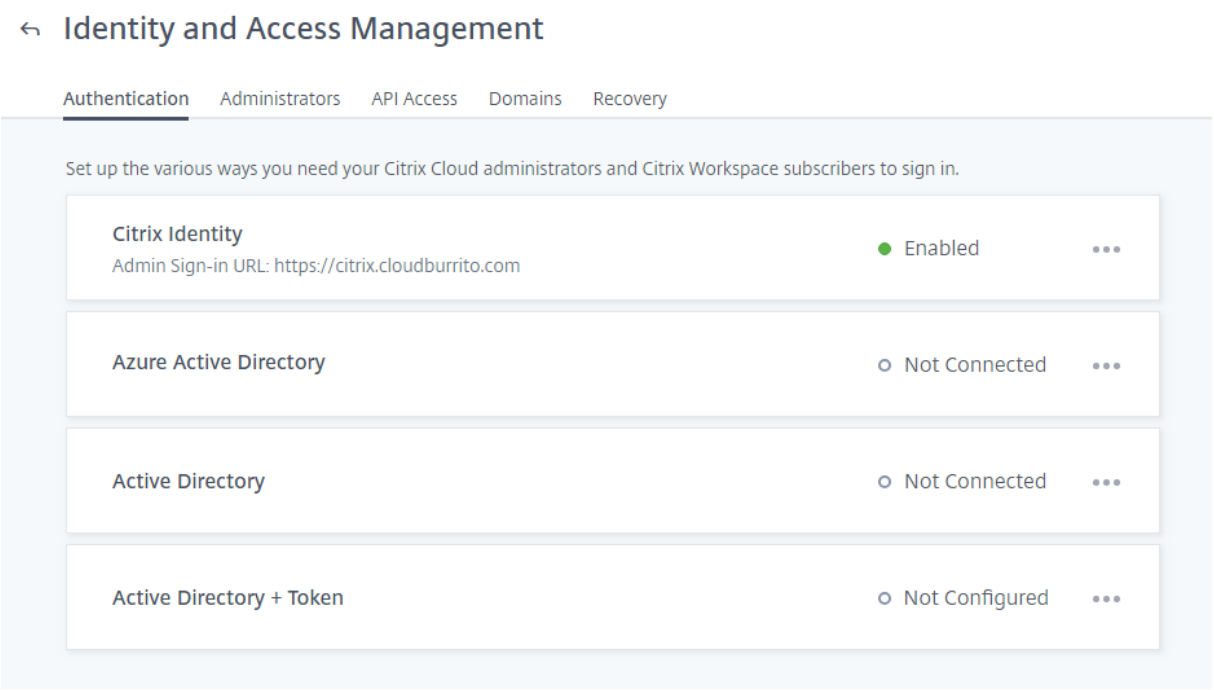
- Cloud Connector の電源がオンになっており、Cloud Connector 接続チェックユーティリティを使用して Citrix Cloud に接続されている。
- プロキシとファイアウォールが正しく構成されている。
- 必要な Windows サービスが［開始済み］の状態になっている。
- Cloud Connector で詳細ログが有効になっている。

Cloud Connector の更新エラーのトラブルシューティング手順については、シトリックスサポート Knowledge Center のCTX270718を参照してください。

Citrix Cloud Connector ログをシトリックスに送信して、トラブルシューティングのサポートを受けることができます。詳しくは、「Citrix Cloud Connector のログ収集」を参照してください。

ID およびアクセス管理

September 17, 2021



ID およびアクセス管理は、Citrix Cloud 管理者とワークスペース利用者が使用する、ID プロバイダーおよびアカウントを定義します。

ID プロバイダー

Citrix Cloud でサポートされている 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	利用者
Citrix ID プロバイダー	はい	いいえ
オンプレミス Active Directory	いいえ	はい
Active Directory+ トークン	いいえ	はい
Azure Active Directory	はい	はい
Citrix Gateway	いいえ	はい
Okta	いいえ	はい
SAML 2.0	いいえ	はい

デフォルトでは、Citrix Cloud は Citrix ID プロバイダーを使用して、Citrix Cloud アカウントを管理します。Citrix ID プロバイダーは、Citrix Cloud 管理者のみを認証します。

次の ID プロバイダーを Citrix Cloud アカウントに追加できます:

- オンプレミス Active Directory。ワークスペース利用者のみを認証する場合。
- Active Directory+ トークン。ワークスペース利用者のみを認証する場合。
- Azure Active Directory。Citrix Cloud 管理者とワークスペース利用者を認証する場合。
- Citrix Gateway。ワークスペース利用者のみを認証する場合。
- Okta。ワークスペース利用者のみを認証する場合。
- SAML 2.0。ワークスペース利用者のみを認証する場合。

Citrix Cloud では、Citrix フェデレーション認証サービス（FAS：Federated Authentication Service）を使用した、ワークスペース利用者のシングルサインオンアクセスがサポートされています。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。

> 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。各モジュールには、各 ID プロバイダーを Citrix Cloud 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。

管理者

管理者は、ID を使用して Citrix Cloud 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 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。最初の管理者は、Citrix Cloud 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 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。これらのアクセス権限の設定により、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 へのアクセスを定義する方法については、「Citrix Cloud 管理者を管理する」を参照してください。

パスワードをリセットする

パスワードを忘れた場合やリセットする場合は、Citrix Cloud サインインページに表示される［ユーザー名またはパスワードを忘れた場合］をクリックします。アカウントを見つけるためにメールアドレスまたはユーザー名を入力すると、パスワードをリセットするためのリンクが記載されたメールを受信します。

Citrix では、アカウントのパスワードを常に保護するために、特定の条件下ではパスワードをリセットする必要があります。これらの条件について詳しくは、「パスワードを変更する」を参照してください。

> 注:
>
> メールの許可リストに **customerservice@citrix.com** を追加して、Citrix Cloud のメールが迷惑メールやごみ箱のフォルダーに入らないようにしてください。

管理者を削除する

[管理者] タブで Citrix Cloud 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 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 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 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。
> - Citrix Cloud Connector は管理者アカウントに関連付けられていません。Cloud 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、Cloud 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 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。

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 Citrix Cloud Connector を 2 つ以上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 Citrix Cloud Connector のインストールをお勧めします。Active Directory での Cloud Connector の展開について詳しくは、「Active Directory での Cloud Connector 展開シナリオ」を参照してください。

> 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。
> - 各 Citrix 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 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、シトリックスの製品ドキュメント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 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。プライマリのリソースの場所については、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 Citrix Cloud Connector があるリソースの場所を選択します。このリソースの場所をプライマリのリソースの場所にすると、ユーザーは Citrix Cloud にすばやくログオンできます。

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。

Active Directory を Citrix Cloud に接続する

September 17, 2021

Citrix Cloud は、オンプレミスの Active Directory（AD）を使用したワークスペース利用者の認証をサポートしています。また、一部のワークスペース認証方法では、Active Directory と Citrix Cloud 間の接続が必要です。詳しくは、「ワークスペースへの認証の変更」を参照してください。

Citrix Cloud では、Active Directory を介して自分のワークスペースにサインインする利用者の認証の第 2 要素としてトークンを使用することをサポートしています。ワークスペースの利用者は、Citrix SSO などの時間ベースのワンタイムパスワード標準に従うアプリケーションを使用して、トークンを生成できます。

Active Directory とトークンを使用してワークスペースの利用者を認証する方法について詳しくは、「Active Directory+ トークン」を参照してください。

> 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 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。

Active Directory 認証

Active Directory を Citrix Cloud 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 つ以上インストールすることをお勧めします。詳しくは、次の記事を参照してください：

- Cloud Connector の技術詳細：システム要件と展開の推奨事項。

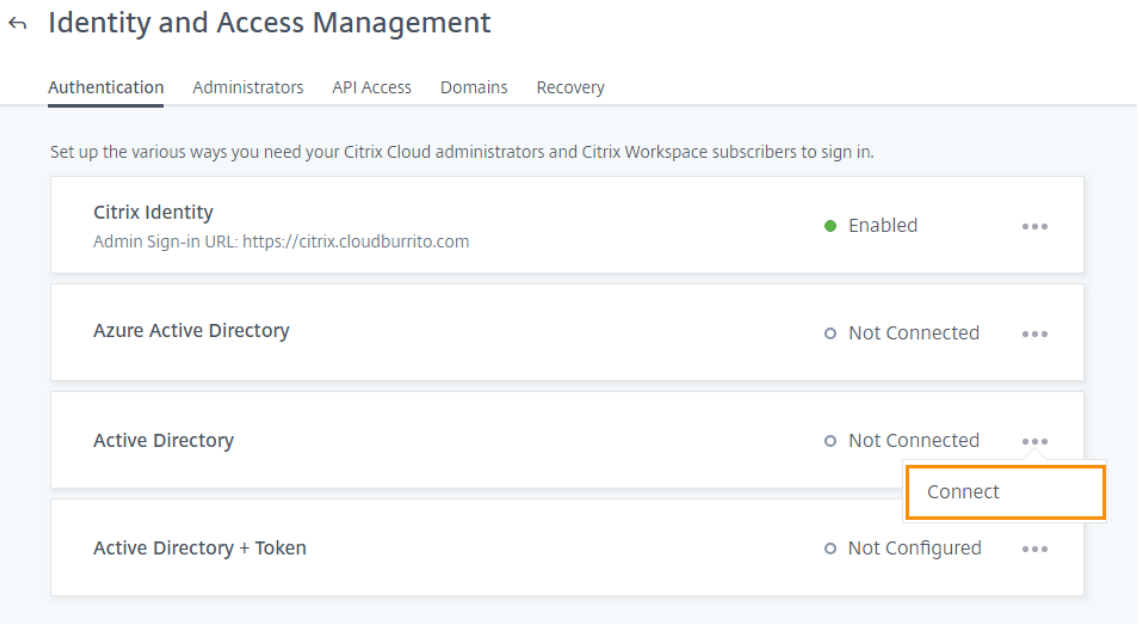
- Cloud Connector のインストール：グラフィカルインターフェイスまたはコマンドラインを使用したインストール手順。

Active Directory を Citrix Cloud に接続するには、次の作業が必要です：

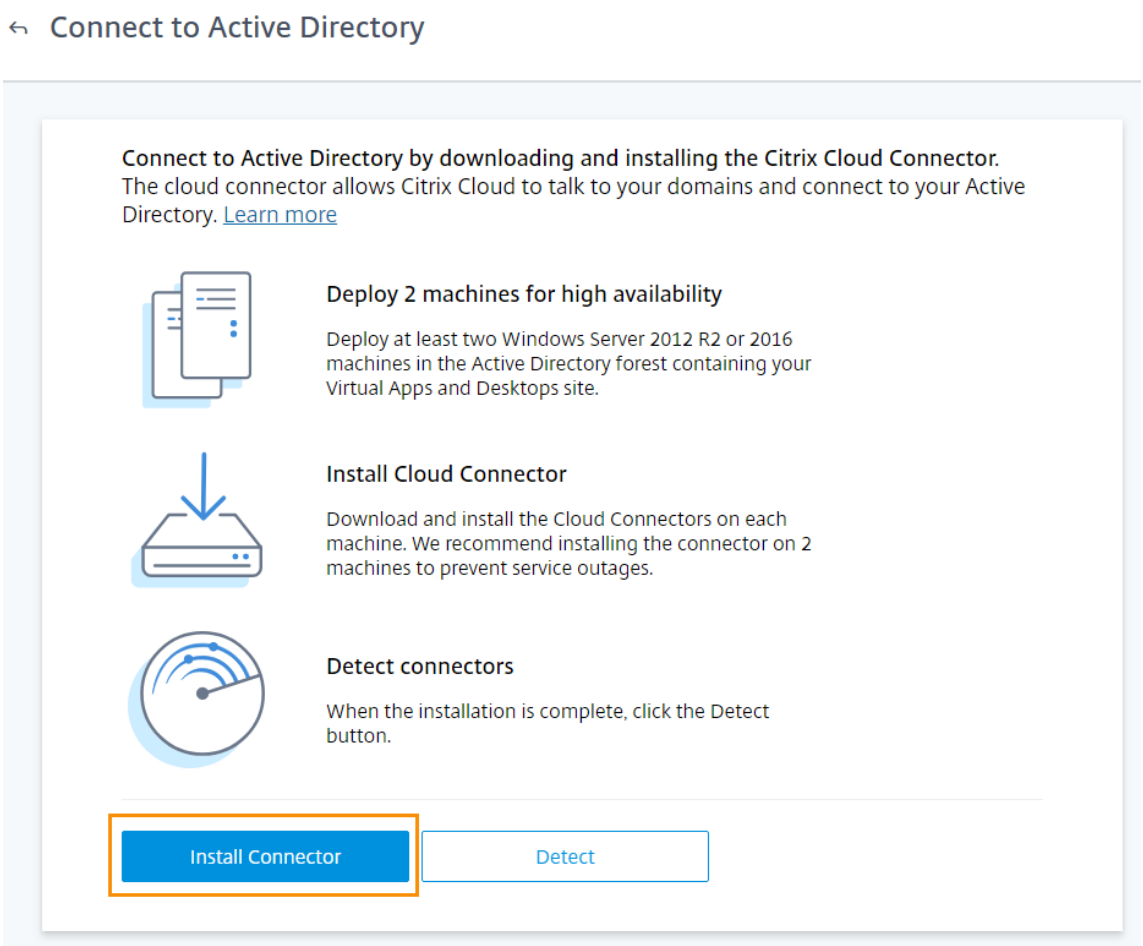
1. ドメインにCloud Connector をインストールします。可用性を高めるため、Cloud Connector を 2 つインストールすることを Citrix ではお勧めします。
2. 該当する場合は、ユーザーデバイスのトークンを有効にします。利用者は、一度に 1 つのデバイスしか登録できません。

Active Directory を **Citrix Cloud** 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。



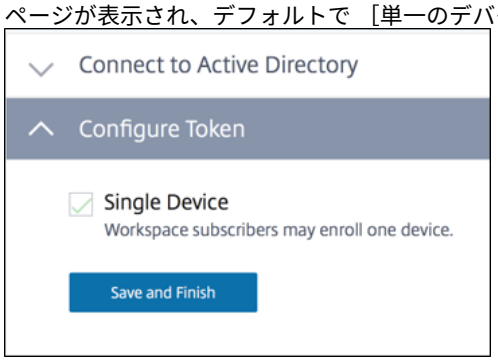
3. [コネクタのインストール] をクリックして、Cloud Connector ソフトウェアをダウンロードします。



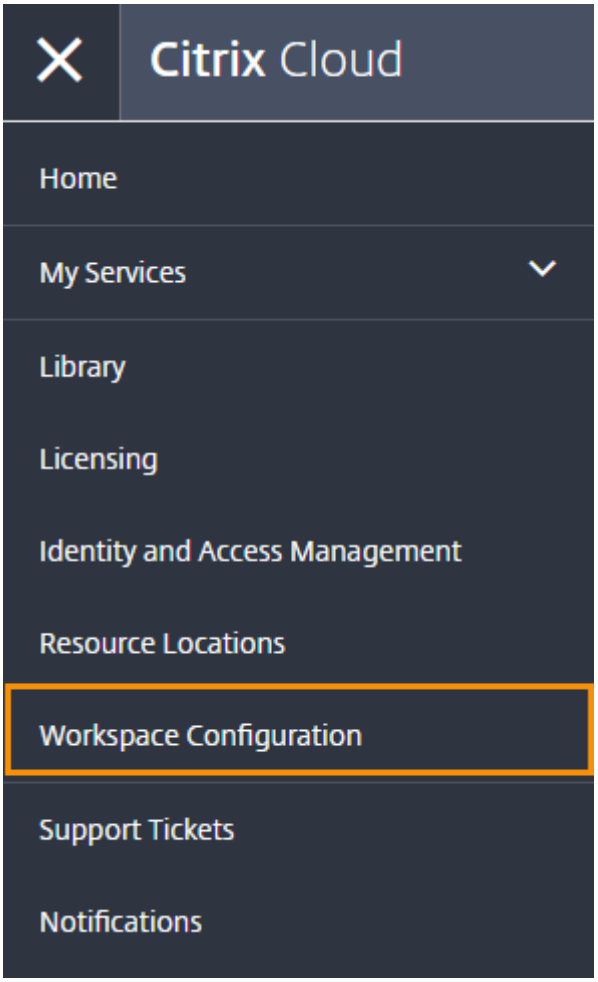
4. Cloud Connector インストーラーを起動し、インストールウィザードの指示に従って操作します。
5. [**Active Directory** に接続する] ページで、[検出] をクリックします。確認後、Citrix Cloud は Active Directory が接続されているというメッセージを表示します。
6. [認証に戻る] をクリックします。**Active Directory** エントリは、[認証] タブで [有効] とマークされます。

Active Directory+ トークン認証を有効にするには

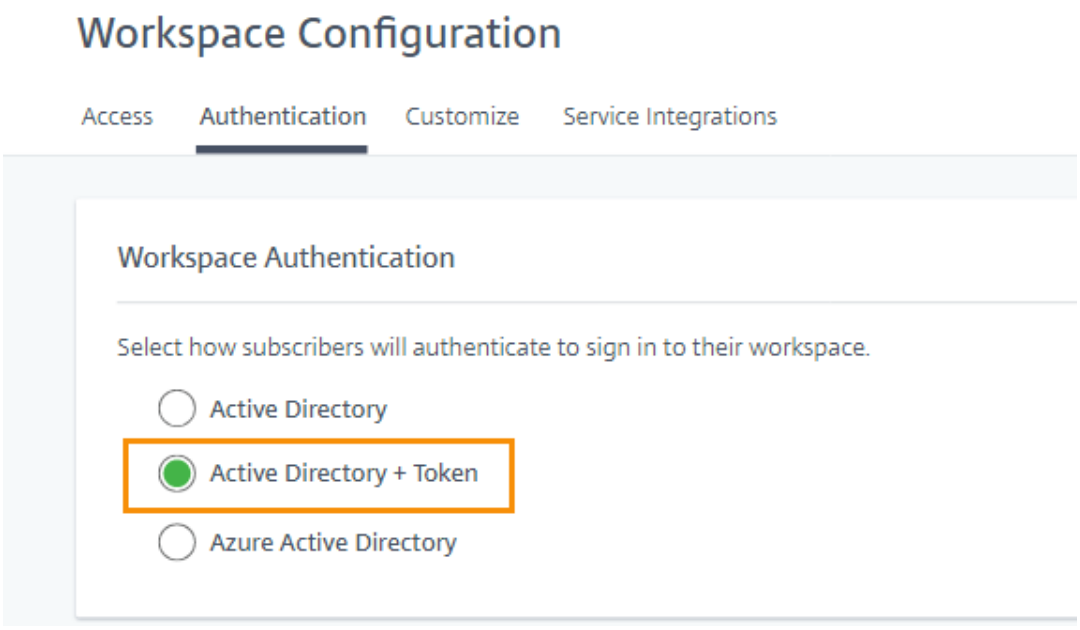
1. 「Active Directory を Citrix Cloud に接続するには」に記載されている手順 1～5 を実行します。
2. Citrix Cloud が Active Directory との接続を確認したあとに、[次へ] をクリックします。[トークンの構成] ページが表示され、デフォルトで [単一のデバイス] オプションが選択されています。



3. ［保存して終了］をクリックして、構成を完了します。［認証］タブで、［**Active Directory +** トークン］エントリが ［有効］になっています。
4. ワークスペースのトークン認証を有効にします：
   a) Citrix Cloud メニューから、［ワークスペース構成］を選択します。



   b)［認証］タブで、［**Active Directory +** トークン］を選択します。



Active Directory とトークン認証を有効にしたあと、ワークスペースの利用者は自分のデバイスを登録し、認証アプリケーションを使用してトークンを生成できます。利用者は、一度に 1 つのデバイスしか登録できません。利用者のデバイスを登録する手順については、「2 要素認証に対するデバイスの登録」を参照してください。

利用者のデバイスを再登録するオプションについては、「デバイスを再登録するには」を参照してください。

Azure Active Directory を Citrix Cloud に接続する

September 17, 2021

Citrix Cloud は、Azure Active Directory（AD）を使用した Citrix Cloud 管理者およびワークスペース利用者の認証をサポートしています。

Citrix Cloud 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 を活用して、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 アプリと権限

Citrix Cloud には Azure AD 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。2018 年 8 月現在、このアプリはアップグレードによってパフォーマンスが向上しており、今後のリリースにも対応できます。2018 年 8 月以前に Azure AD を Citrix Cloud に接続していた場合は、Citrix Cloud で Azure AD 接続を更新してください。詳しくは、この記事の「アプリのアップグレードに対応するため Azure AD に再接続する」を参照してください。

Citrix Cloud 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 用の Azure Active Directory の権限」を参照してください。

> 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 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。

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 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 では、Azure AD から追加された管理者には、シトリックスがホストする 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。詳しい手順については、Microsoft Azure Web サイトの「簡単設定を使用した Azure AD Connect の開始」を参照してください。

Citrix Cloud を **Azure AD** に接続する

Citrix Cloud 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のほか、ユーザープロファイル（またはサインイン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。Citrix Cloud が要求するアプリケーション権限について詳しくは、「Citrix Cloud 用の Azure Active Directory の権限」を参照してください。

> 重要:
>
> この作業を完了するには、Azure AD のグローバル管理者である必要があります。

1. https://citrix.cloud.comで Citrix Cloud にサインインします。
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、［接続］をクリックします。この識別子は、Citrix Cloud 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 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。これらの読み取り専用権限により、Citrix Cloud は Microsoft Graph からグループやユーザープロファイルなどの基本情報を収集できます。Citrix Endpoint Management または XenMobile Server を Microsoft Intune と統合した場合、Microsoft Intune 関連の読み取り/書き込み権限を付与する必要があります。詳しくは、「委任権限の要求に同意する」を参照してください。
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** に管理者を追加する

1. Citrix Croud の ［**ID** およびアクセス管理］ページで ［管理者］をクリックします。
2. ［追加する管理者の場所］メニューから、［Azure AD］オプションを選択します。
3. 検索ボックスで、追加するユーザーの名前を入力して、「Citrix Cloud 管理者を管理する」の説明どおりにアカウントに招待します。Citrix Cloud は招待を承諾するためのリンクが記載されたメールをユーザーに送信します。

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 間の接続が完了します。

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

Azure AD ユーザーアカウントの接続後、ユーザーは次のいずれかの方法で Citrix Cloud 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.cloud.com/go/mycompany`
- Citrix Cloud 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 を接続した時に作成した識別子（「mycompany」など）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 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、ワークスペースで 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. Citrix Cloud 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、［**Azure 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。

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 が自動的に活用できるようになります。

Azure AD サービスレベルの機能と価格を比較するには、https://azure.microsoft.com/ja-jp/pricing/details/active-directory/を参照してください。

アプリのアップグレードに対応するため **Azure AD** に再接続する

2019 年 5 月以前に Azure AD を Citrix Cloud に接続していた場合は、Citrix Cloud が Azure AD への接続で最新のアプリケーションを使用していない可能性があります。その結果、Citrix Cloud が Azure AD に再接続し、追加の読み取り専用権限を付与するよう求める場合があります。Azure AD グループをライブラリオファリングに追加し、ログオンパフォーマンスを向上させ、その他の利点を実現するには、Azure AD のグローバル管理者ロールを通じて Citrix Cloud に追加のアクセス権限を付与する必要があります。これを行うには、Azure AD のグローバル管理者である必要があります。Azure AD に再接続することにより、アプリケーションレベルの読み取り専用権限が Citrix Cloud に付与され、Citrix Cloud が Azure AD に再接続できるようになります。

> 重要:
>
> Azure AD を Citrix Cloud に再接続するには、Citrix ID プロバイダーの Citrix Cloud 管理者アカウントを使用して、Citrix Cloud にサインインする必要があります。Azure AD の資格情報を使用して Citrix Cloud にサインインしている場合、再接続は失敗します。Citrix Cloud で Azure AD 管理者アカウントを使用していて、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この再接続を実行し、後で削除することができます。

再接続を実行するには、Citrix Cloud 管理者資格情報を使用して Citrix Cloud にサインインします。再接続を求められたときは、グローバル管理者の資格情報を使用して Azure にサインインできます。

Citrix Cloud 用の Azure Active Directory の権限

September 17, 2021

この記事では、Azure Active Directory（AD）を接続して使用するときに Citrix Cloud が要求する権限について説明します。Citrix Cloud 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 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。

エンタープライズアプリケーション

名前	アプリケーション ID	用途
Citrix Cloud	e95c4605-aeab-48d9-9c36-1a262ef8048e	ワークスペース利用者のログイン
Citrix Cloud	f9c0e999-22e7-409f-bb5e-956986abdf02	Azure AD と Citrix Cloud 間のデフォルトの接続
Citrix Cloud	1b32f261-b20c-4399-8368-c8f0092b4470	管理者の招待、管理者のログイン
Citrix Cloud	5c913119-2257-4316-9994-5e8f3832265b	Citrix Endpoint Management を使用した Azure AD と Citrix Cloud 間のデフォルトの接続
Citrix Cloud	e067934c-b52d-4e92-b1ca-70700bd1124e	Citrix Endpoint Management を使用した Azure AD と Citrix Cloud 間の従来の接続

ワークスペース利用者のログイン

Citrix Cloud アプリケーション（ID：e95c4605-aeab-48d9-9c36-1a262ef8048e）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	Delegated
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	Delegated

Azure AD と **Citrix Cloud** 間のデフォルトの接続

Citrix Cloud アプリケーション（ID：f9c0e999-22e7-409f-bb5e-956986abdf02）は、次の権限を使用します：

API 名	要求値	権限	種類
Microsoft Graph	Group.Read.All	すべてのグループの読み取り	Delegated
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	Delegated
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	Delegated
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	Delegated
Microsoft Graph	Group.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	Directory.Read.All	ディレクトリデータの読み取り	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
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	アプリケーション
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	Delegated
Windows Azure Active Directory	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	Delegated
Windows Azure Active Directory	Group.Read.All	すべてのグループの読み取り	Delegated
Windows Azure Active Directory	Directory.Read.All	ディレクトリデータの読み取り	アプリケーション

管理者の招待とログイン

Citrix Cloud アプリケーション（ID：1b32f261-b20c-4399-8368-c8f0092b4470）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	Delegated
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	Delegated
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	Delegated
Windows Azure Active Directory	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	Delegated

Endpoint Management を使用した **Azure AD** と **Citrix Cloud** 間のデフォルトの接続

Citrix Cloud アプリケーション（ID：5c913119-2257-4316-9994-5e8f3832265b）は、次の権限を使用します：

API 名	要求値	権限名	種類
Microsoft Graph	Group.Read.All	すべてのグループの読み取り	Delegated
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	Delegated
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	Delegated
Microsoft Graph	Directory.Read.All	ディレクトリデータの読み取り	アプリケーション
Microsoft Graph	Directory.Read.All	ディレクトリデータの読み取り	Delegated
Microsoft Graph	DeviceManagementApps.ReadWrite.All	Microsoft Intune アプリの読み取りと書き込み	Delegated
Microsoft Graph	Directory.AccessAsUser	ディレクトリに対するサインインしたユーザーと同じアクセス	Delegated

Endpoint Management を使用した **Azure AD** と **Citrix Cloud** 間の従来の接続

Citrix Cloud アプリケーション（ID：e067934c-b52d-4e92-b1ca-70700bd1124e）は、次の権限を使用します：

API 名	要求値	権限名	種類
Microsoft Graph	Group.Read.All	すべてのグループの読み取り	Delegated
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	Delegated
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	Delegated
Microsoft Graph	DeviceManagementApps.ReadWrite.All	Microsoft Intune アプリの読み取りと書き込み	Delegated
Microsoft Graph	Directory.AccessAsUser	ディレクトリに対するサインインしたユーザーと同じアクセス	Delegated

権限

API 名

Citrix Cloud が権限を要求する 2 つのリソースアプリケーションがあります: [**API** 名] の下に表示される Microsoft Graph と Windows Azure Active Directory です。Citrix Cloud は、両方のリソースアプリケーションに同じ権限を要求します。

種類

Citrix Cloud が権限を要求できるアクセスには 2 つのレベルがあります: [種類] の下に表示される [委任] と [アプリケーション] です。

- 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 は、[要求値] の下に表示される権限の文字列値を割り当てます。次の表に、特定の要求値の説明を示します:

名前	説明
User.Read	Citrix Cloud 管理者が、接続された Azure AD のユーザーを Citrix Cloud 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 が、https://docs.microsoft.com/ja-jp/graph/api/user-list?view=graph-rest-1.0&tabs=httpに示す API 呼び出しにより、顧客の接続 Azure AD からユーザーを閲覧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 Virtual Apps and Desktops リソースへのアクセス権限を付与できます。Citrix Cloud 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。
Group.Read.All	Citrix Cloud が、https://docs.microsoft.com/ja-jp/graph/api/group-list?view=graph-rest-1.0&tabs=httpに示す API 呼び出しにより、顧客の接続 Azure AD からグループを閲覧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、Virtual Apps and Desktops 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。
Directory.Read.All	Citrix Cloud は、https://docs.microsoft.com/ja-jp/graph/api/user-list-memberof?view=graph-rest-1.0&tabs=httpに示す API 呼び出しにより、ユーザーのグループメンバーシップを取得します (Groups.Read.All では不十分な場合)。
DeviceManagementApps.ReadWrite.All	Microsoft Intune によって管理されるプロパティ、グループ割り当て、アプリの状態、アプリの設定、およびアプリ保護ポリシーの読み取りと書き込みを、Citrix Cloud が行えるようにします。
Directory.AccessAsUser.All	サインインユーザーと同じように、Citrix Cloud がディレクトリ内の情報にアクセスできるようにします。

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

September 17, 2021

Citrix Cloud 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 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 の技術詳細」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、「システムおよび接続要件」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 台用意することをお勧めします。インストール後、Citrix Cloud 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 のインストール手順について詳しくは、「Cloud Connector のインストール」を参照してください。

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 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 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 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 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 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 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 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 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 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 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。

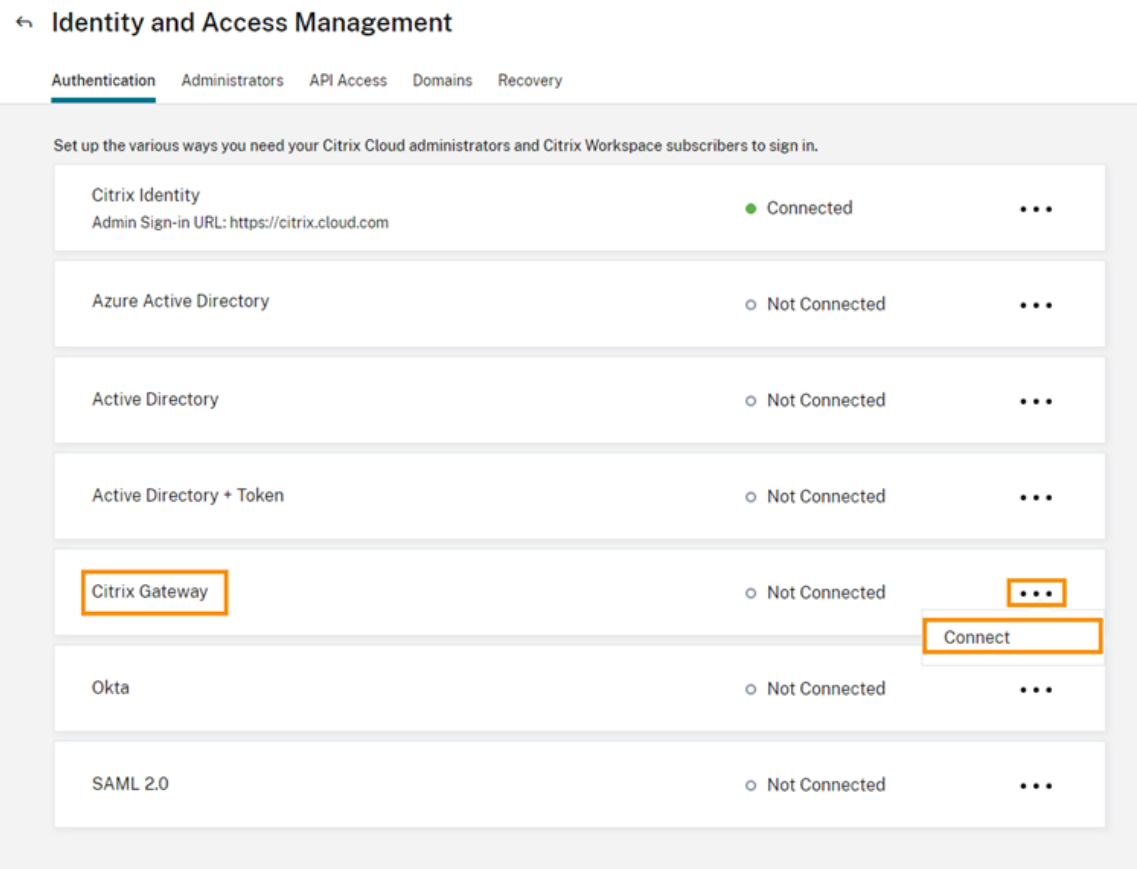
タスクの概要

Citrix Gateway 認証を設定するには、次のタスクを実行します:

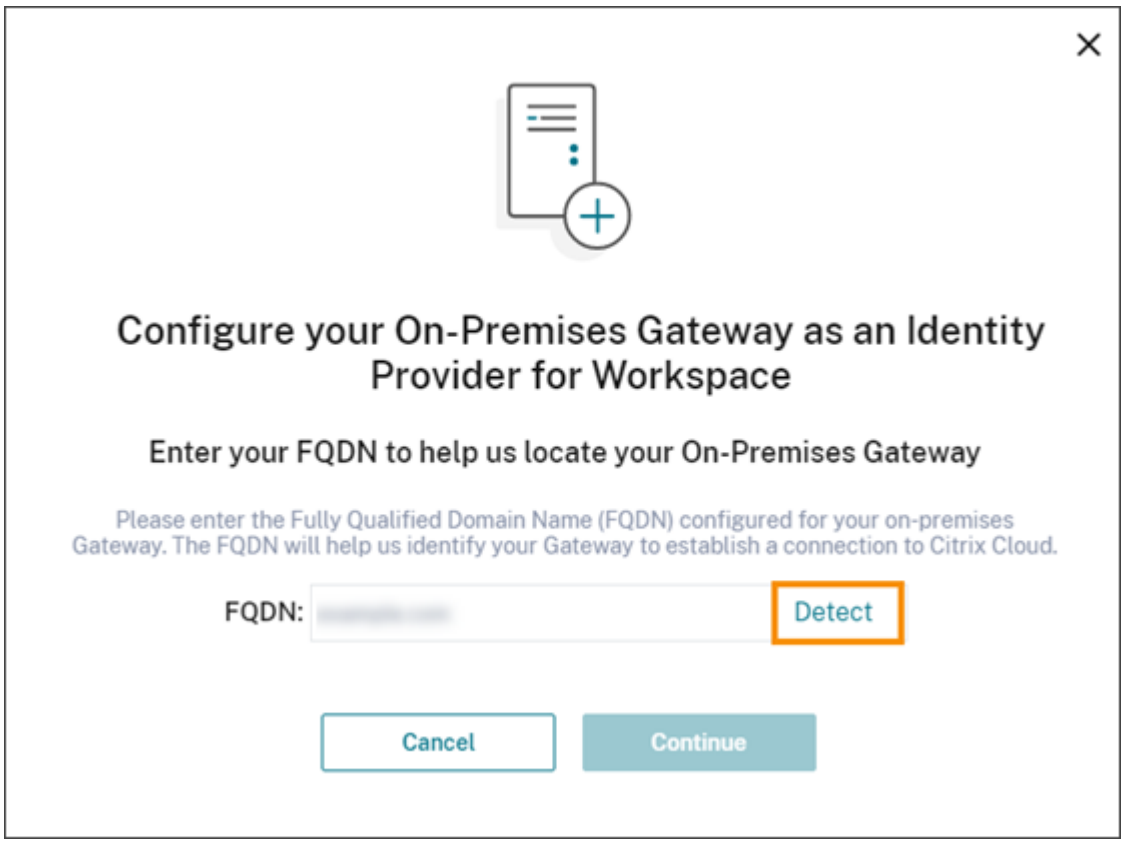
1. ［**ID** およびアクセス管理］で Gateway への接続を構成します。この手順では、Gateway のクライアント ID、シークレット、リダイレクト URL を生成します。
2. Gateway で、Citrix Cloud から生成された情報を使用して OAuth ID プロバイダー拡張ポリシーを作成します。これにより Citrix Cloud がオンプレミス Gateway に接続できるようになります。手順については、以下の記事を参照してください。
   - Citrix Gateway 12.1：オンプレミス Citrix Gateway を ID プロバイダーとして Citrix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

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

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 ［**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。

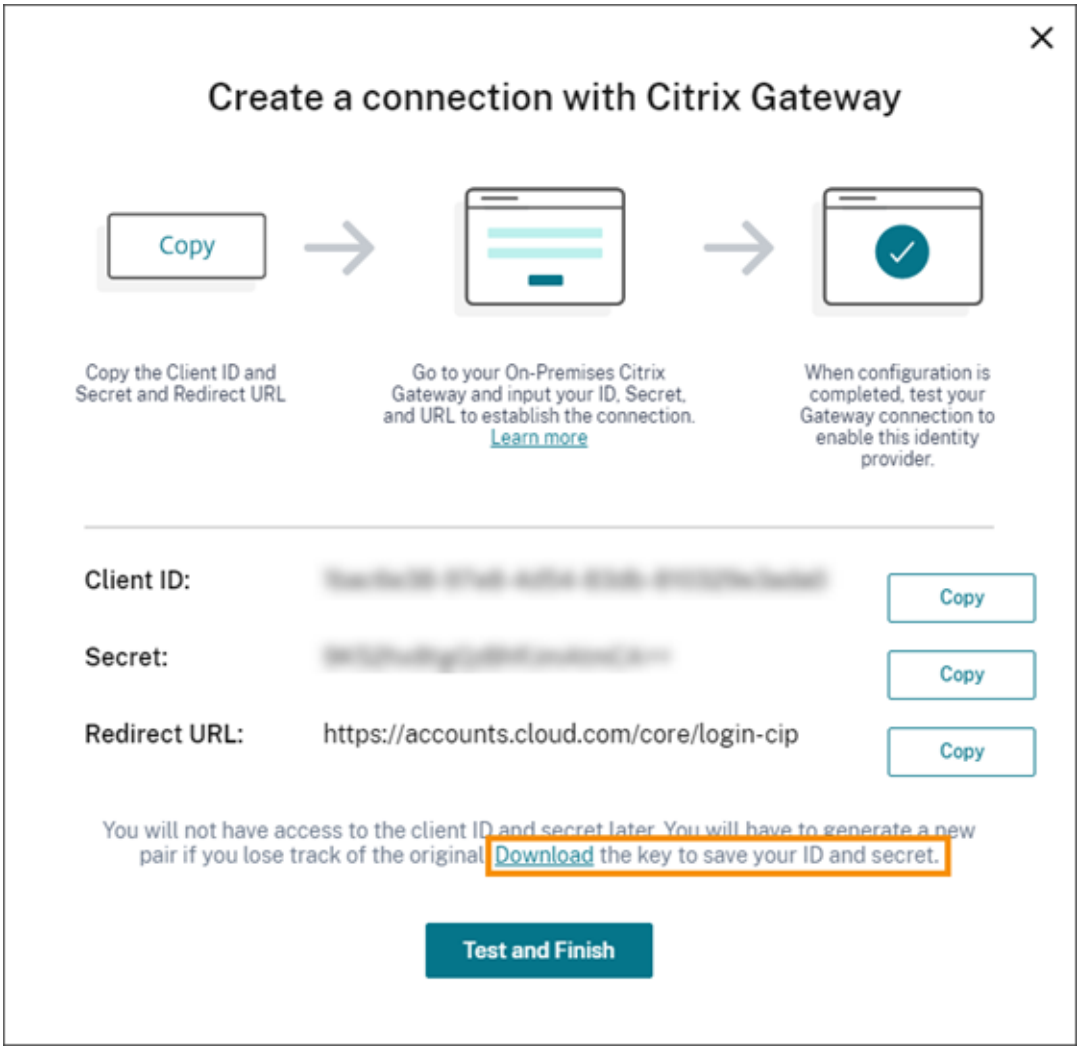


3. オンプレミス Gateway の完全修飾ドメイン名を入力して ［検出］をクリックします。



Citrix Cloud 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 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 で表示することはできなくなります。

b) Gateway で、Citrix Cloud 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 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。

5. ワークスペースの Citrix Gateway 認証を有効にするには：

a) Citrix Cloud メニューから、［ワークスペース構成］を選択します。

b) ［認証］タブで ［**Citrix Gateway**］を選択します。

c) ［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 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 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 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 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 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 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 Citrix Cloud に接続する

July 29, 2021

Citrix Cloud 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 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 Virtual Apps and Desktops サービス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 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 Cloud に Citrix フェデレーション認証サービスを接続する」を参照してください。

> 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 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。

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 とリソースの場所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:

- 「Cloud Connector の技術詳細」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、「システムおよび接続要件」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、「Cloud Connector のインストール」を参照してください。

Okta ドメイン

Okta を Citrix Cloud 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。シトリックスは、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 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 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 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 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 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ログオフ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 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 を Okta 組織に接続」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 SID、UPN、および OID の値を含めます。

> 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 アプリケーションの作成

1. Okta 管理コンソールの［**Applications**］から［**Applications**］を選択します。
2. ［**Add Application**］をクリックしてから、［**Create New App**］をクリックします。
3. ［**Sign in method**］で［**OpenID Connect**］を選択し、［**Create**］をクリックします。［**Platform**］のデフォルト値（**Web**）は変更されません。
4. アプリケーション名を入力します。
5. ［**Login redirect URIs**］に「`https://accounts.cloud.com/core/login-okta`」を入力します。
6. ［**Logout redirect URIs**］に、Citrix Cloud からのワークスペース URL を入力します。
7. ［保存］をクリックします。

Okta OIDC Web アプリケーションの構成

この手順では、Citrix Cloud に必要な設定によって Okta OIDC Web アプリケーションを構成します。Citrix Cloud 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. 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。
2. ［**Allowed grant types**］で、以下のオプションを選択します：
   - Authorization Code
   - Refresh Token
   - Implicit (Hybrid)
   - Allow ID Token with implicit grant type
   - Allow Access Token with implicit grant type
3. ［保存］をクリックします。
4. アプリケーションへのユーザーまたはグループアクセスの許可：
   a) ［**Assignments**］タブから［**Assign**］を選択してから、［**Assign to People**］または［**Assign to Groups**］を選択します。
   b) ワークスペースへのアクセスを許可するユーザーまたはグループを選択します。すべてのユーザーにアクセスを許可するには、［**Assign to Groups**］を選択してから［**Everyone**］を選択します。
5. ［完了］をクリックします。
6. 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 ユーザープロファイルを見つけ、[**Profile**] を選択します。[**Attributes**] で、[**Add attribute**] を選択します。
c) 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
- Attribute Required: Yes

d) [**Save and Add Another**] をクリックします。
e) 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
- Attribute Required: Yes

f) [**Save and Add Another**] をクリックします。
g) 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
- Attribute Required: Yes

h) [保存] をクリックします。

7. 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**] > [**Directory Integrations**] の順に選択します。
b) 以前に統合した AD を選択します。詳しくは、「Okta AD エージェントでアカウントを同期」を参照してください。
c) [**Settings**] タブで、[**Edit Mappings**] を選択します。
d) 次の属性をマップします:
- `appuser.objectSid`を選択し、`cip_sid`属性にマップします。
- `appuser.userName`を選択し、`cip_upn`属性にマップします。
- `appuser.externalId`を選択し、`cip_oid`属性にマップします。

e) [**Save Mappings**] をクリックします。
f) [**Apply updates now**] をクリックします。

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**] をクリックします。
6. トークン値をコピーします。Okta 組織の Citrix Cloud への接続時に、この値を入力します。

Citrix Cloud を **Okta** 組織に接続

1. Citrix Cloud（https://citrix.cloud.com）にサインインします。
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. [**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、Okta アプリケーションの資格情報を入力します。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 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 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** に接続する（**Technical Preview**）

June 15, 2021

Citrix Cloud 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、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 SAML 2.0 をサポートしている場合は、選択した SAML プロバイダーを使用できます。

> 注:
>
> - この機能は、現在 Technical Preview 段階です。Technical Preview 機能は、Citrix ではテスト環境でのみ使用することをお勧めします。
> - この記事では、Active Directory のみを使用した Citrix Cloud での SAML 2.0 の設定について説明します。SAML 2.0 でシングルサインオン（SSO）を使用する予定の場合は、How to Integrate Azure AD with SAML 2.0 Tech Preview（CTX312150）を参照してください。

前提条件

Citrix Cloud 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 Active Directory 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 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 台用意することをお勧めします。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:

- 「Cloud Connector の技術詳細」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。
- 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、「システムおよび接続要件」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、「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 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

- オンプレミスの Active Directory（AD）に Cloud Connector を展開して、AD を Citrix Cloud アカウントに接続します。
- AD ユーザーを SAML プロバイダーに同期します。Citrix Cloud 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 に渡すことができます:

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

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. 上記の AD ユーザー属性にマップするカスタム属性がまだない場合は、カスタム属性を作成して AD にマップします。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:
>
> 前述の必要な AD ユーザー属性にマップするカスタム属性を既に作成済みの場合は、さらにカスタム属性を作成してマップする必要はありません。代わりに、Citrix Cloud 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。

タスクの概要

ワークスペース利用者の 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 に接続するの説明に従って、オンプレミスの AD を Citrix Cloud に接続します。
2. この記事の「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 のSAML 認証の構成を実行します。このタスクには、SAML プロバイダーで Citrix Cloud からの SAML メタデータを構成してから、Citrix Cloud で SAML プロバイダーからのメタデータを構成して SAML 接続を作成することが含まれます。
4. [ワークスペース構成］で、SAML 認証方法の選択を実行します。

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 で既存のカスタム 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 プロバイダーが対応するコマンドについて詳しくは、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 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。

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 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 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 プロバイダーが対応するコマンドについて詳しくは、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. Citrix Cloud（https://citrix.cloud.com）にサインインします。
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。[**SAML** の構成］画面が表示されます。
4. 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。
5. 必要に応じて、表示名を入力してアプリを保存します。
6. Citrix Cloud 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。
7. 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.cloud.com`と入力します。
   - **Recipient** フィールドに、`https://saml.cloud.com/saml/acs`を入力します。
   - ACS URL 検証のフィールドに、`https://saml.cloud.com/saml/acs`を入力します。
   - ACS URL のフィールドに、`https://saml.cloud.com/saml/acs`を入力します。
   - 単一のログアウト URL のフィールドに、`https://saml.cloud.com/saml/logout/callback`を入力します。
8. 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

9. 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** に追加

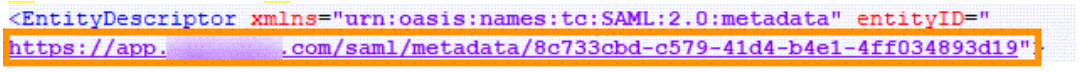
1. SAML プロバイダーから SAML メタデータを取得します。次の画像は、このファイルのイメージ例です:

```
<?xml version="1.0"?>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="
https://app.          .com/saml/metadata/8c733cbd-c579-41d4-b4e1-4ff034893d19">
  <IDPSSODescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#" protocolSupportEnumeration=
  "urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIID2DCCA
                                                                    +w3PpA==</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="
    https://citrixidentity-dev.          .com/trust/saml2/http-redirect/slo/1097253"/>

      <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>

    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="
    https://citrixidentity-dev.          .com/trust/saml2/http-redirect/sso/8c733cbd-c579-41d4-b4e1-4ff034893d19"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="
    https://citrixidentity-dev.          .com/trust/saml2/http-post/sso/8c733cbd-c579-41d4-b4e1-4ff034893d19"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location=
    "https://citrixidentity-dev.          .com/trust/saml2/soap/sso/8c733cbd-c579-41d4-b4e1-4ff034893d19"/>
  </IDPSSODescriptor>
</EntityDescriptor>
```

2. Citrix Cloud 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。

     ```
     <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="
     https://app.          .com/saml/metadata/8c733cbd-c579-41d4-b4e1-4ff034893d19">
     ```

   - ［認証要求に署名する］で ［はい］を選択して Citrix Cloud が認証要求に署名できるようにして、Citrix Cloud 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。

     ```
     <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="
     https://citrixidentity-dev.          /trust/saml2/http-redirect/sso/8c733cbd-c579-41d4-b4e1-4ff034893d19"/>
     <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="
     https://citrixidentity-dev.          .com/trust/saml2/http-post/sso/8c733cbd-c579-41d4-b4e1-4ff034893d19"/>
     ```

   - ［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 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 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 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。［最小］を選択した場合、選択したコンテキスト、およびより厳格なコンテキストで認証を実施します。［完全一致］を選択した場合、選択したコンテキストでのみ認証を実施します。たとえば、［**Transport Layer Security**（**TLS**）］コンテキストと ［最小］レベルを選択した場合、Citrix Cloud は、TLS、X.509 証明書、統合 Windows 認証、および Kerberos のコンテキストで SAML 応答を受け入れます。［ユーザー名とパスワード］および［パスワード保護転送］コンテキストを使用した応答は拒否されます。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。
8. Citrix Cloud 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 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 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。

ワークスペースの **SAML** 認証を有効にする

1. Citrix Cloud 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。

プライマリのリソースの場所の選択

September 4, 2019

ドメイン内に複数のリソースの場所がある場合は、Citrix Cloud の「プライマリの」、つまり「最も優先される」場所を選択できます。プライマリのリソースの場所は、Citrix Cloud とドメイン間で最高のパフォーマンスと接続性を提供するため、ユーザーはすぐにサインインできるようになります。

プライマリのリソースの場所を選択すると、そのリソースの場所にある Cloud Connector がユーザーのログオンとプロビジョニング操作に使用されます。プライマリのリソースの場所の Cloud Connector が利用できない場合、これらの操作はドメイン内の別の Cloud Connector を使用して実行されます。

> 注:
>
> 任意のリソースの場所で常に Cloud Connector を使用できるようにするには、少なくとも 2 つの Cloud Connector をインストールすることをお勧めします。

プライマリのリソースの場所に使用するリソースの場所を決定するには、次の点を考慮してください。

- ドメインとの接続に優れたリソースの場所である。
- Citrix Cloud 管理コンソールを使用している地理的地域に最も近いリソースの場所である。例えば、Citrix Cloud コンソールがhttps://us.cloud.comにある場合は、米国地域に最も近い場所をリソースの場所に選択します。

プライマリのリソースの場所を選択するには

1. Citrix Cloud 管理コンソールで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。
2. [ドメイン] をクリックし、使用するリソースの場所を含むドメインを展開します。
3. [プライマリのリソースの場所を設定する] をクリックし、プライマリとして指定するリソースの場所を選択します。
4. [保存] をクリックします。選択したリソースの場所の横に「プライマリ」と表示されます。

> 注:
>
> 別のドメインを展開する前に、選択内容をドメインに保存してください。ドメインを展開してから別のドメインを展開すると、最初に展開されたドメインが折りたたまれ、保存されていない選択が破棄されます。

別のプライマリのリソースの場所を選択する

1. Citrix Cloud 管理コンソールで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。
2. [ドメイン] をクリックし、変更するプライマリのリソースの場所を含むドメインを展開します。

3. ［プライマリのリソースの場所を変更する］をクリックし、使用するリソースの場所を選択します。
4. ［保存］をクリックします。

プライマリのリソースの場所をリセットする

プライマリのリソースの場所をリセットすると、別の場所を選択せずにリソースの場所から「プライマリ」の指定を削除できます。「プライマリ」の指定を削除すると、ドメイン内のどの Cloud Connector でもユーザーログオン操作を処理できるようになります。その結果、一部のユーザーのログオンが遅くなる可能性があります。

1. Citrix Cloud 管理コンソールで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。
2. ［ドメイン］を選択し、変更するプライマリのリソースの場所を含むドメインを展開します。
3. ［プライマリのリソースの場所を変更する］を選択し、［リセット］を選択します。ログオンのパフォーマンスが影響を受ける可能性があることを警告する通知が表示されます。
4. ［利用者に影響を与える可能性があることを了承します。］を選択し、［リセットの確認］をクリックします。

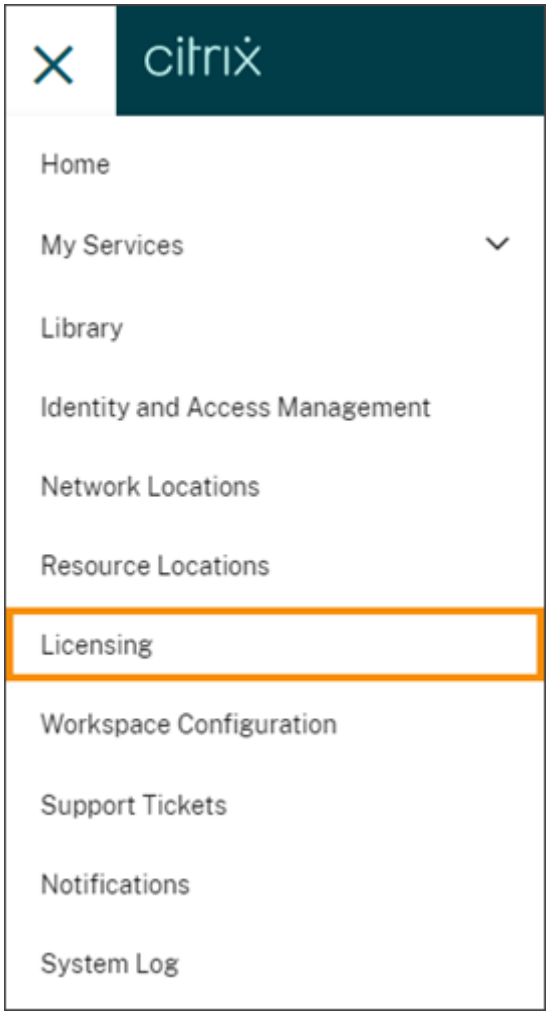
Citrix Cloud 用のライセンス

September 17, 2021

Citrix Cloud 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 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。

法人顧客用のライセンス

法人顧客は、Citrix Cloud 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。



クラウドサービスの企業ライセンスと使用状況の監視について詳しくは、「クラウドサービスのライセンスおよびアクティブな使用状況の監視」を参照してください。

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 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 に登録することにより、顧客は Citrix Cloud の ［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、「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（CSP）用のライセンス

Citrix Service Provider 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 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、サポートされている Virtual Apps and Desktops 製品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、次の記事を参照してください:
  - Citrix Virtual Apps and Desktops サービスの顧客のライセンスと使用状況の監視
  - Citrix Virtual Apps and Desktops Standard for Azure の顧客のライセンスと使用状況の監視

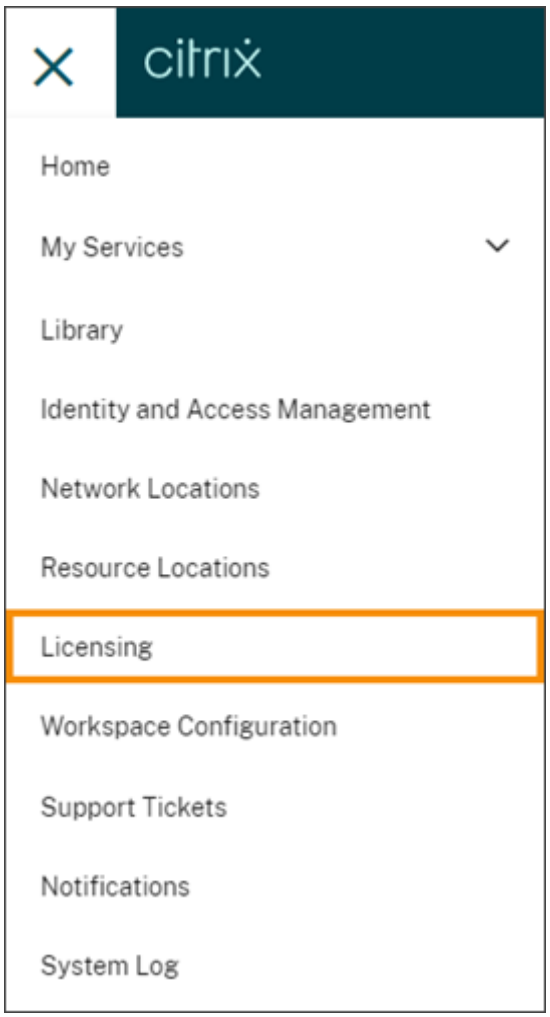
クラウドサービスのライセンスおよびアクティブな使用状況の監視

September 17, 2021

Citrix Cloud のライセンス機能により、購入したクラウドサービスのライセンス消費を常に把握できます。概要レポートと詳細レポートを使用すると、次のことが実行できます:

- ライセンスの可用性と割り当てを一目で把握する
- 関連するクラウドサービスの日次および月次のアクティブな使用状況の傾向を表示する
- 個別のライセンス割り当ての詳細と使用傾向をドリルダウンして確認する
- ライセンス使用状況データを CSV にエクスポートする

クラウドサービスのライセンスデータを表示するには、コンソールメニューで ［ライセンス］を選択します。



> 注:
>
> この記事では、サポートされているすべての Citrix Cloud サービスに共通のライセンス機能について説明します。ライセンスのいくつかの要素は、サービスによって異なる場合があります（ライセンスの割り当てなど）。各サービスのライセンスと使用状況について詳しくは、以下の記事を参照してください:
>
> - Virtual Apps and Desktops サービス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）
> - Virtual Apps and Desktops サービスのライセンスとピーク時の使用状況の監視（同時使用）
> - Virtual Apps and Desktops Standard for Azure のライセンスとアクティブな使用状況の監視
> - Endpoint Management サービスのライセンスとアクティブな使用状況の監視

サポートされている地域とクラウドサービス

ライセンス機能は、米国、EU、南アジア太平洋地域のサポートされているサービスでのみ利用できます。

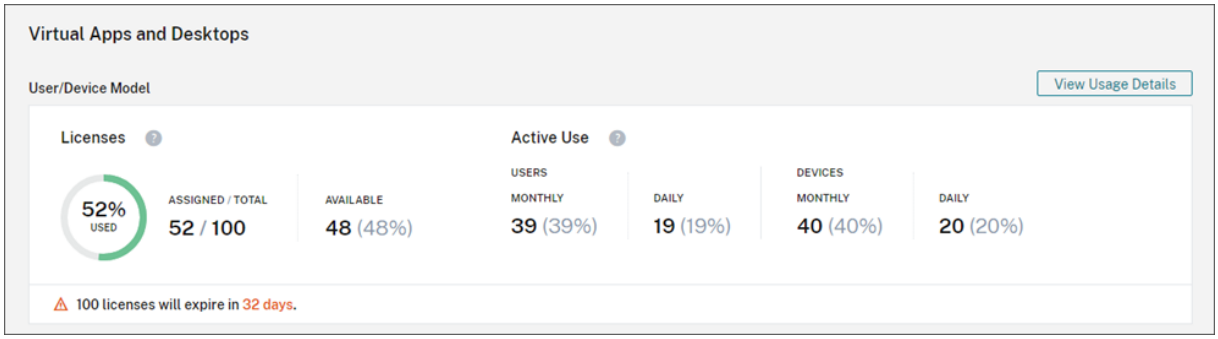
ライセンス機能は次のクラウドサービスでサポートされています:

- Virtual Apps and Desktops（ユーザー/デバイスおよび同時使用のライセンスモデル）
- Virtual Apps and Desktops Standard for Azure（ユーザー/デバイスライセンスモデル）
- Endpoint Management
- Gateway

ライセンス割り当て

一般に、ユーザーには、クラウドサービスの最初の使用時にライセンスが割り当てられます。一部のサービスでは、使用するライセンスモデルに基づいて異なる方法でライセンスを割り当てる場合があります。各サービスのライセンスの割り当て方法について詳しくは、この記事の上部で参照されているライセンスの記事を参照してください。

ライセンスの概要と詳細



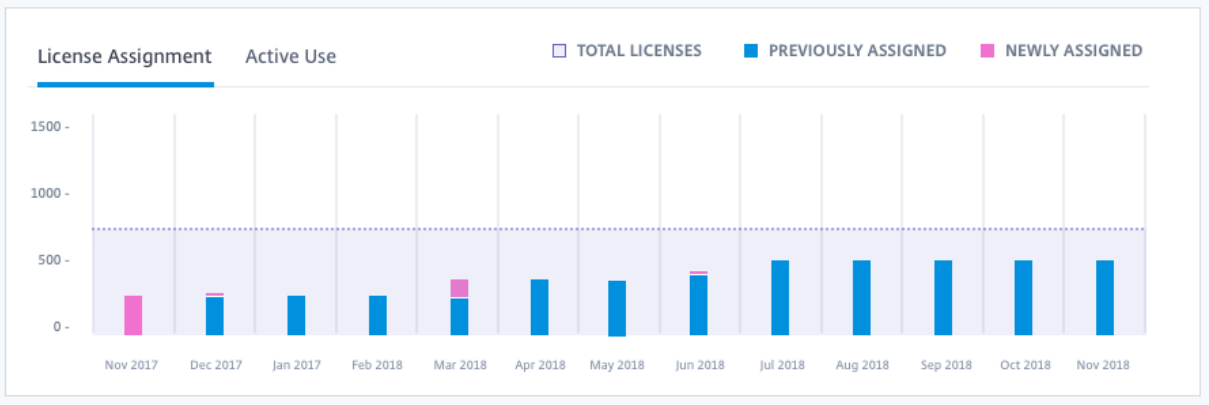
ライセンスの概要では、サポートされている各サービスに関する次の情報を一目で確認できます：

- 購入済みライセンス合計に対する割り当て済みライセンスの割合。割合が 100% に近づくにつれて、表示は緑色から黄色に変わります。割合が 100% を超えると、表示が赤になります。
- 購入したライセンスに対する割り当てられたライセンスの比率、および使用可能なライセンスの残りの数。
- クラウドサービスのサブスクリプションが期限切れになるまでの残り時間。サブスクリプションが 90 日以内に期限切れになる場合、警告メッセージが表示されます。

一部のサービスでは、この概要にアクティブな使用などの追加情報が含まれる場合があります。サービス固有の詳細について詳しくは、この記事の上部で参照されているライセンスの記事を参照してください。

使用状況の傾向とライセンスアクティビティ

クラウドサービスライセンスの詳細を表示するには、［使用状況の詳細の表示］をクリックします。使用状況の傾向と、クラウドサービスライセンスを使用しているユーザーの内訳を確認できます。



この内訳には、クラウドサービスに応じてさまざまな情報が含まれます。使用状況の傾向とライセンスアクティビティについて詳しくは、この記事の上部で参照されているライセンスの記事を参照してください。

割り当て済みライセンスを解放する

一般に、割り当て済みライセンスは、ユーザーがクラウドサービスを 30 日間連続して使用していない場合、解放対象となります。ライセンスが解放されると、それに応じて残りのライセンス数が増加し、割り当て済みライセンス数が減少します。

一部のサービスでは、使用するライセンスモデルによって、ライセンスの解放が異なる場合があります。各サービスのライセンスの解放について詳しくは、この記事の上部で参照されているライセンスの記事を参照してください。

よくある質問

- 割り当てられたライセンス数が購入したライセンス数を超えた場合、クラウドサービスの使用が停止されますか**?** いいえ。購入済みクラウドライセンスの使用数を超過した場合でも、サービスは停止されません。［ライセンス使用状況］ではクラウドライセンスの使用数を把握するための情報が提供されるため、お客様はライセンスの割り当てを監視し、購入したライセンス数内でサービスを使用されることを期待されます。ライセンス数を超えてサービスを使用することが判明した場合、営業担当者にご連絡いただき、ライセンス要件の見直しについてご相談いただくようお願いします。
- どのようなライセンス情報がキャプチャされていますか**?** 現在、ユーザーログインに関連するライセンス情報のみがキャプチャされます。
- マルチタイプのライセンスは **Virtual Apps and Desktops** サービスでサポートされていますか**?**（ユーザー**/**デバイスモデルおよび同時使用モデル両方の使用など）両方のライセンスモデルが単一の Citrix Cloud アカウントに導入されている場合は、Virtual Apps and Desktops のタイルが Citrix Cloud のライセンスコンソールページに表示されなくなります。このように Virtual Apps and Desktops サービスのライセンスが表示されなくなるため、マルチタイプのライセンスの使用はお勧めしません。
- マルチエディションのライセンスは **Virtual Apps and Desktops** サービスでサポートされていますか? たとえば、同一の **Citrix Cloud** アカウントで **Premium** エディションと **Advanced** エディションの両方を使用できますか**?** いいえ、そのユースケースはサポートされていません。1 つの Virtual Apps and Desktops

サイトには、1 つのエディションのライセンスのみが付与されます。同じ Citrix Cloud アカウントで複数の Virtual Apps and Desktops サービス（たとえば、Virtual Apps と Virtual Apps and Desktops）を使用する場合は、それらが同じエディションである必要があります。

- 監視レポート（**Director** 内）と同時使用ライセンスの分析情報の違いは何ですか**?** 監視レポートと同時使用セッションの説明では、使用中の同時ライセンスの測定値とは異なる解釈と測定基準が提供されます。ほとんどの場合、Director 内の同時使用セッション数を、使用中のピーク時の同時使用ライセンスの表現または予測として使用すると、必要な同時使用ライセンスの数が多くなりすぎてしまいます。同時使用ライセンスの使用状況レポートの代わりに、Director の監視レポートを使用しないでください。レポートツールの主な違いは次の 2 つです：
  - サンプリング時間の長さ：ライセンスには 5 分のサンプリング時間があります。Citrix Cloud は 5 分ごとに、現在サービスに接続されている固有のデバイスをカウントします。5 分のすべてのサンプリング期間が集計され、24 時間、毎月、および契約期間のピーク時の使用量が割り出されます。Director の監視レポートでは、レポートの実行方法に応じて、最大 2 時間の間隔を表示できます。
  - 一意性：ライセンスは、セッションが開始されたときにデバイス間の一意性を確認します。監視レポートでは、一意のデバイスかどうかは考慮されません。
- ユーザーをクラウドサービスの新しいインスタンスに移行した後（たとえば、自分が所属する組織のドメイン名を変更した場合）、使用中の自分のライセンスが同じユーザーに対して **2** 回カウントされるのはなぜですか? Citrix Cloud は、ユーザープリンシパル名（UPN）を使用して一意のユーザーをカウントします。移行が発生する前後にユーザーがクラウドサービスにアクセスした場合、Citrix Cloud は、異なるドメイン名を持つ各ユーザーの一意の UPN を 2 つキャプチャします。そのため、Citrix Cloud は同じユーザーを 2 回カウントします。ユーザーが古いドメイン名でサービスにアクセスしなければ、その古いライセンス割り当てを 30 日後に解放できます。購入済みクラウドライセンスの使用数を超過した場合でも、サービスは停止されません。

Endpoint Management のライセンスとアクティブな使用状況の監視

May 27, 2020

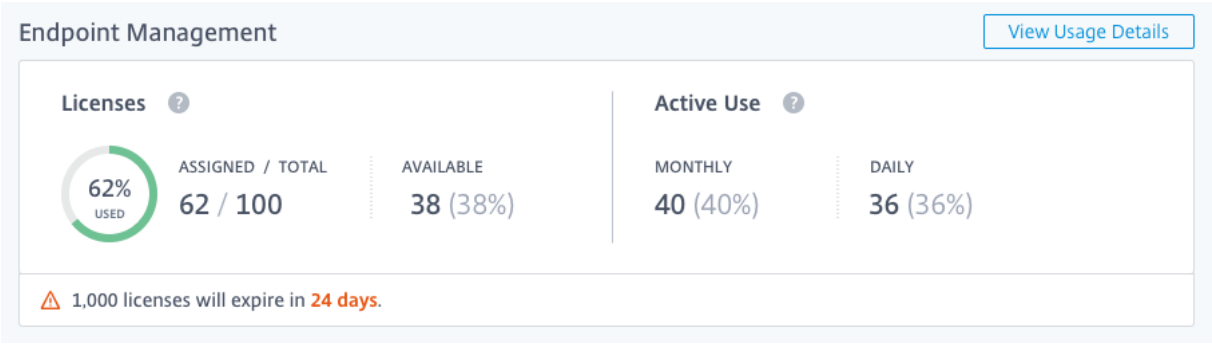
ライセンス割り当て

一般に、ユーザーには、クラウドサービスの最初の使用時にライセンスが割り当てられます。Endpoint Management では、ユーザーがデバイスを登録するときにライセンスが割り当てられます。デバイスが登録されると、デバイスは定期的に Citrix Cloud にチェックインします。Citrix Cloud は、この「チェックインパルス」を使用して毎月の使用量を計算し、管理者がユーザーの最新のサービス使用状況を把握できるようにします。

初回使用は、ユーザーがデバイスを初めて登録したとき、またはデバイスに対して「チェックインパルス」が初めて発生したときに発生します。

ライセンスは、ユーザーごとに割り当てられます。したがって、2 人のユーザーが同じデバイスを登録して使用すると、2 つのライセンスが割り当てられます。

ライセンスの概要と詳細

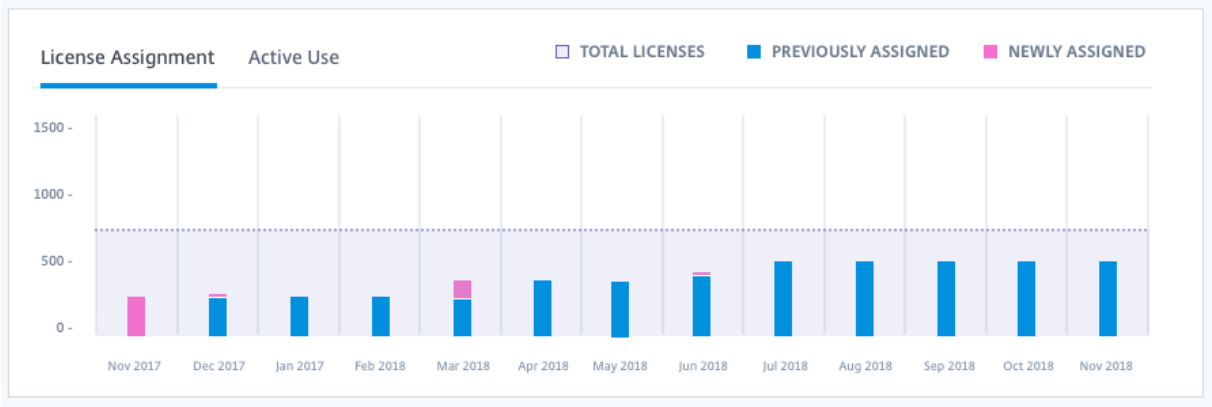


ライセンスの概要では、サポートされている各サービスに関する次の情報を一目で確認できます:

- 購入済みライセンス合計に対する割り当て済みライセンスの割合。割合が 100% に近づくにつれて、表示は緑色から黄色に変わります。割合が 100% を超えると、表示が赤になります。
- 購入したライセンスに対する割り当てられたライセンスの比率、および使用可能なライセンスの残りの数。
- 月次および日次のアクティブな使用状況の統計:
  - 月次のアクティブな使用状況とは、過去 30 日間にサービスを使用した一意のユーザー数を指します。
  - 日次のアクティブな使用状況とは、過去 24 時間以内にサービスを使用した一意のユーザー数を指します。
- クラウドサービスのサブスクリプションが期限切れになるまでの残り時間。サブスクリプションが 90 日以内に期限切れになる場合、警告メッセージが表示されます。

使用状況の傾向とライセンスアクティビティ

ライセンスの詳細を表示するには、[使用状況の詳細の表示] をクリックします。使用傾向と、クラウドサービスライセンスを使用している個々のユーザーおよびデバイスの内訳を確認できます。



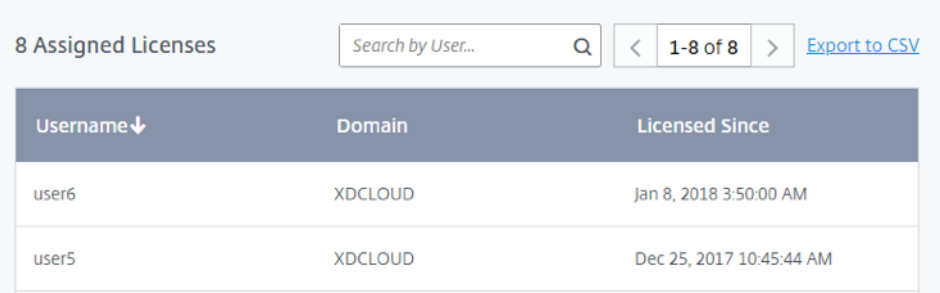
この内訳では、次の情報を表示します:

- ライセンス合計: 合計したクラウドサービス使用権のために購入済みのライセンス合計数。
- 事前割り当て済み: 月ごとの初めに既に割り当てられているクラウドサービスライセンス。例えば、7 月にユーザーにライセンスが割り当てられた場合、その割り当ては 8 月の事前割り当て済み数に含まれます。

- 新しく割り当て済み：月ごとに割り当てられたクラウドサービスライセンス数。例えば、7 月にクラウドサービスに初めてアクセスするユーザーには、ライセンスが割り当てられます。このライセンスは、7 月の新しく割り当て済みの合計に含まれます。
- アクティブな使用状況：前の暦月および暦年の日次および月次のアクティブな使用状況の傾向。

［ライセンスアクティビティ］セクションには、次の情報も表示されます：

- ライセンスを割り当てた個々のユーザーのリスト
- ライセンスが割り当てられた日付
- 登録されたデバイスの数と各ユーザーの最終チェックイン日



特定のユーザーの登録済みデバイスの数を表示するには、省略記号ボタンをクリックして ［デバイスを表示］を選択します。Citrix Cloud には、ユーザーに登録されているデバイスの一覧と、各デバイスの最終チェックイン日が表示されます。

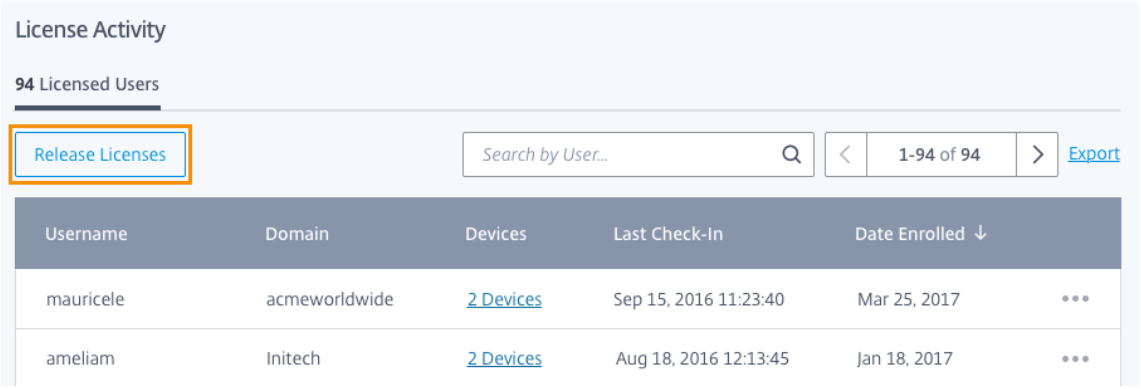
割り当て済みライセンスを解放する

新しいデバイスを登録しておらず、既存のデバイスが過去 30 日間に Citrix Cloud でチェックインしていないユーザーのライセンスを解放できます。ライセンスは複数を一括で解放するか、個別に解放できます。

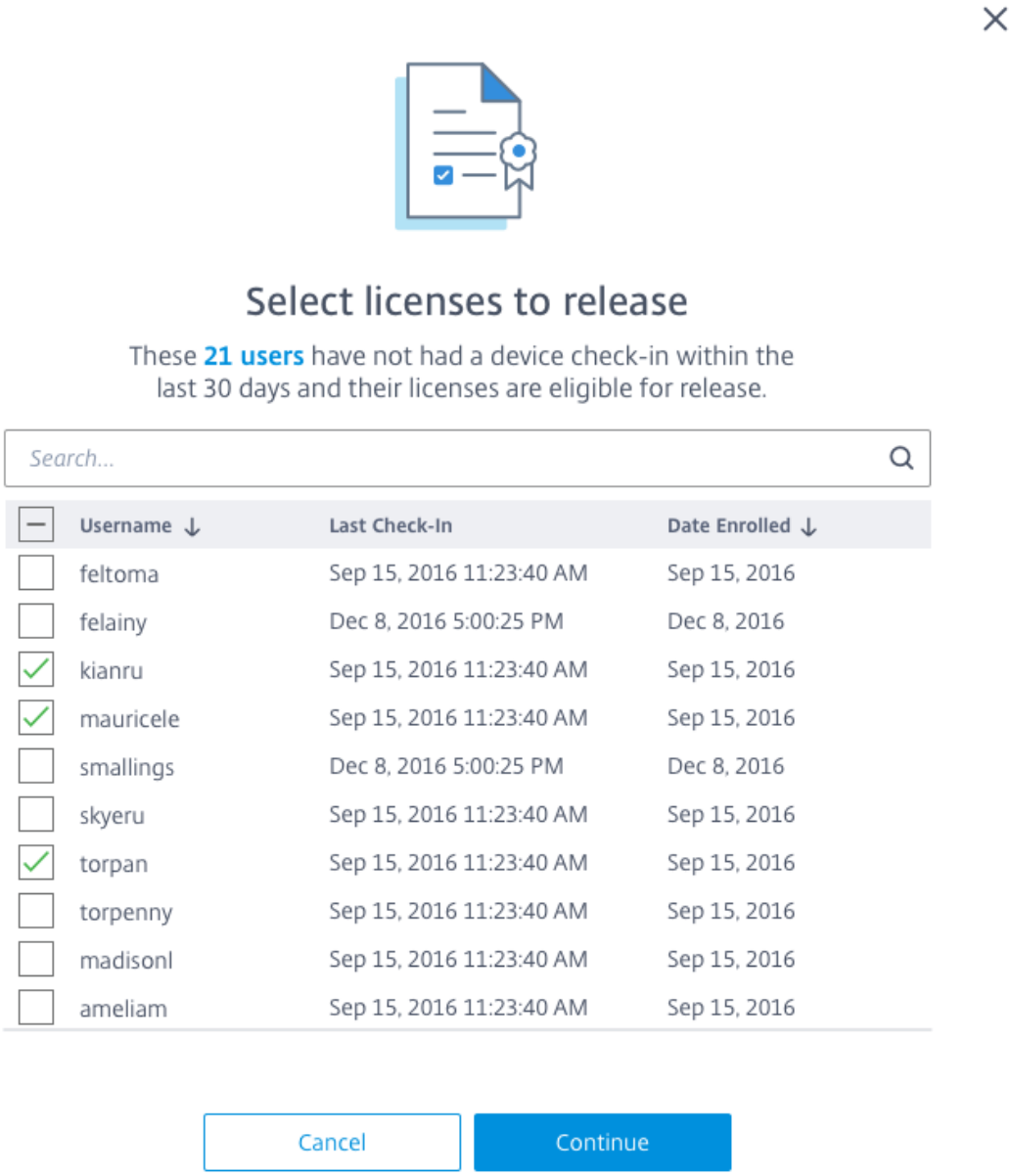
ライセンスが解放されると、それに応じて残りのライセンス数が増加し、割り当て済みライセンス数が減少します。ユーザーのライセンスが解放された後、ユーザーはデバイスを登録することで別のライセンスを取得できます。

複数の割り当て済みライセンスを解放するには

1. ［ライセンスアクティビティ］で、［ライセンスを解放］を選択します。



2. リストから、管理するユーザーを選択し、［続行］を選択します。

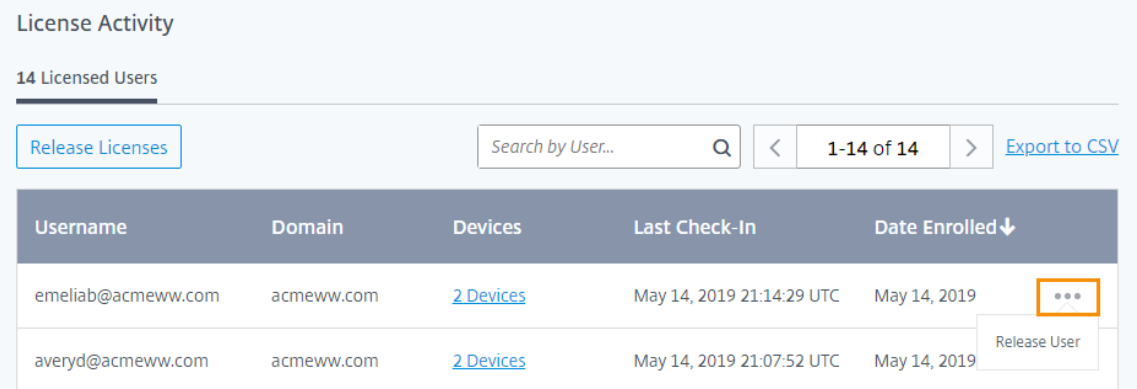


3. 解放を確認するメッセージが表示されたら、［解放］をクリックします。

1 つの割り当て済みライセンスを解放するには

［ライセンス使用ユーザー］リストから、個別のライセンスを解放できます。このリストには、解放対象のライセンスがあるユーザーのみに省略ボタンが表示され、クリックできます。省略ボタンは、新しいデバイスを登録し、既存のデバイスが過去 30 日間に Citrix Cloud でチェックインしているユーザーに対してはアクティブになりません。

1. ［ライセンスアクティビティ］で、［ライセンス使用ユーザー］タブを選択します。
2. 管理するユーザーを見つけます。
3. 省略記号ボタンをクリックして、［ユーザーを解放］を選択します。



4. 選択したユーザーを確認して ［続行］ を選択します。
5. 解放を確認するメッセージが表示されたら、［解放］ をクリックします。

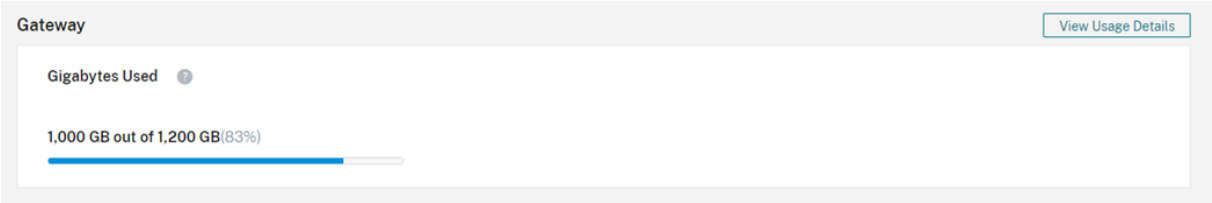
Gateway サービスの帯域幅の使用状況の監視（Technical Preview）

September 17, 2021

> 注:
>
> 「Gateway サービスの帯域幅の使用状況の監視」は、Technical Preview 段階にあります。この機能は、顧客が Gateway サービスでの実際の帯域幅の使用状況をよりよく理解できるようにすることを目的としています。シトリックスが、顧客の環境で帯域幅の使用状況の割り当てを強制したり、実稼働のワークロードに干渉したりすることはありません。シトリックスが顧客の使用権と使用状況ポリシーの強制方法を変更する場合、これらの変更が有効になる前に早い段階でお客様に通知します。

この記事では、Citrix Virtual Apps and Desktops サービスと Citrix Workspace を使用する場合の Gateway サービスについて説明しています。Virtual Apps Essentials サービスに含まれる Gateway サービスの帯域幅消費量は、Citrix Cloud 管理コンソールの ［ライセンス］ ページに表示されません。

ライセンスの概要



Gateway サービスのライセンスの概要では、次の情報を一目で確認できます:

- すべてのサブスクリプションの帯域幅の合計量のうち、消費された帯域幅の量。
- クラウドサービスのサブスクリプションが期限切れになるまでの残り時間。サブスクリプションが 90 日以内に期限切れになる場合、警告メッセージが表示されます。

使用されるライセンスと帯域幅

Gateway サービスのサブスクリプションの場合、各ユーザーは 1 か月あたり 1GB の帯域幅にアクセスできます（ユーザーあたり 12GB/年）。この帯域幅は、複数のライセンスにまたがって、サブスクリプション期間中、プールされます。たとえば、3 年間で 100 ライセンスを購入した場合、合計帯域幅は 3600GB（年間 1200GB）になります。この帯域幅は、3 年間、すべてのライセンスユーザーに分散されます。さらにサブスクリプションを購入すると、Citrix Cloud ではすべてのサブスクリプションのライセンスの総数と帯域幅が表示されます。

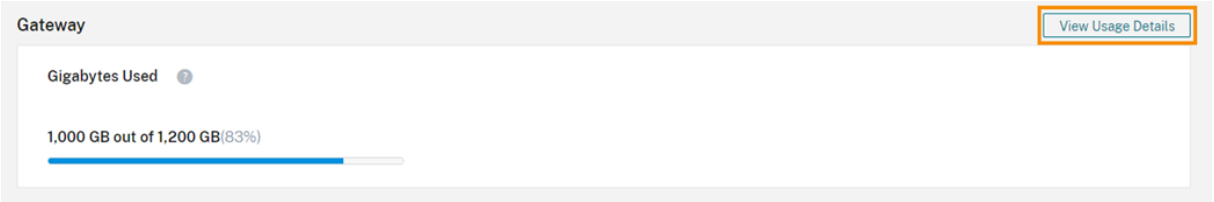
Gateway サービスのトライアル版の場合、60 日間のトライアル期間中、25 人のユーザー全体に 50GB の帯域幅がプールされます。

サブスクリプション期間中に帯域幅の全量を使用しなかった場合、Citrix Cloud では更新時に未使用の帯域幅が引き継がれません。

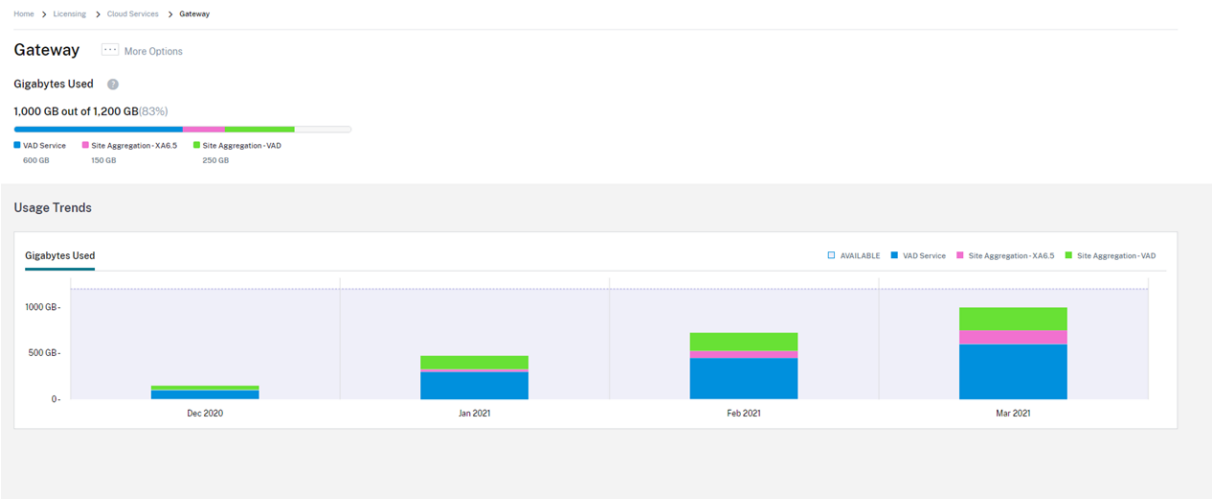
期間が重複する複数のサブスクリプションがある場合、Citrix Cloud は有効期限が切れていないサブスクリプションに関連付けられた帯域幅のみを表示します。たとえば、2 つのサブスクリプションを購入した場合、Citrix Cloud では両方のサブスクリプションの合計ライセンス数と合計帯域幅が表示されます。最初のサブスクリプションの有効期限が切れると、Citrix Cloud では有効期限が切れていないサブスクリプションに関連付けられた帯域幅のみが表示されます。最後のサブスクリプションの有効期限が切れると、Citrix Cloud では現在消費されている帯域幅と合計帯域幅 0 が表示されます。これは、「Citrix Cloud サービスのサブスクリプション延長」に記載されているサービスの猶予期間とデータ保有期間の間、表示されます。

使用状況の傾向

ライセンスの詳細を表示するには、［使用状況の詳細の表示］をクリックします。



使用状況の傾向、およびクラウドサービスのライセンスと帯域幅を使用している個々のユーザーの内訳を確認できます。



［使用状況の傾向］セクションの ［使用帯域幅（**GB**）］タブには、使用可能な合計帯域幅のうち消費された帯域幅の量が表示されます。消費された帯域幅の量は、アクセスに基づいて次の方式で分類されます：

- VAD サービス：Virtual Apps and Desktops ユーザーが外部接続に使用した帯域幅の量。
- サイトアグリゲーション：サイトアグリゲーションで、Workspace を介したオンプレミスのアプリとデスクトップの起動に使用した帯域幅の量。

> 注：
>
> 使用状況の傾向は、現在のサブスクリプション期間中、累積されます。

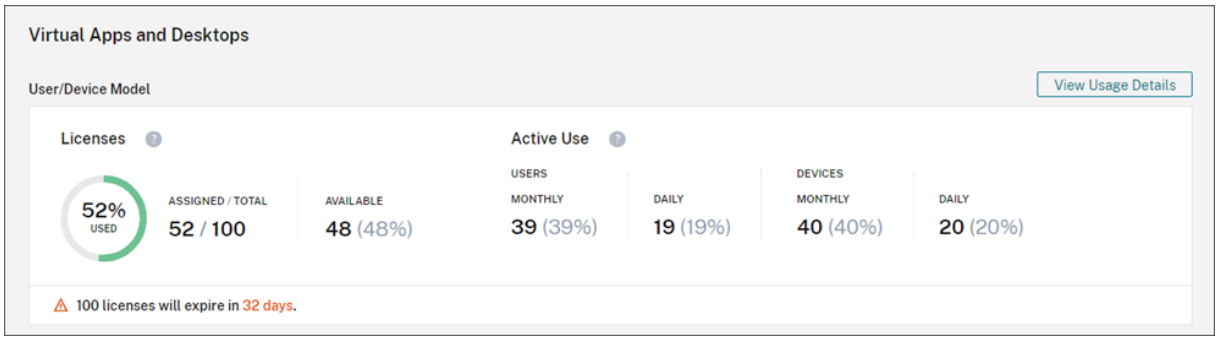
Citrix Virtual Apps and Desktops サービスのライセンスとアクティブな使用状況の監視（ユーザー/デバイス）

September 17, 2021

ライセンス割り当て

Citrix Cloud では、一意のユーザーまたはデバイスによるアプリまたはデスクトップの初回起動時にライセンスが割り当てられます。

ライセンスの概要



ライセンスの概要では、次の情報を一目で確認できます:

- 割り当てられた購入済みライセンスの合計パーセンテージ。割合が 100% に近づくにつれて、表示は緑色から黄色に変わります。割合が 100% を超えると、表示が赤になります。

  購入したライセンスの総数は、ユーザー/デバイスライセンスモデルを使用する Virtual Apps、Virtual Desktops、および Virtual Apps and Desktops サービスの使用のために購入したライセンスの合計です。

- 購入したライセンスに対する割り当てられたライセンスの比率、および使用可能なライセンスの残りの数。
- 月次および日次のアクティブな使用状況の統計:
  - 月次のアクティブな使用状況とは、過去 30 日間にサービスを使用した一意のユーザーまたはデバイスの数を指します。
  - 日次のアクティブな使用状況とは、過去 24 時間以内にサービスを使用した一意のユーザーまたはデバイスの数を指します。
- クラウドサービスのサブスクリプションが期限切れになるまでの残り時間。サブスクリプションが 90 日以内に期限切れになる場合、警告メッセージが表示されます。

割り当てられたライセンスとアクティブな使用状況の計算

Virtual Apps and Desktops サービスのユーザー/デバイスライセンスモデルが正確に反映されるよう、Citrix Cloud ではサービスを使用した一意のユーザー数とデバイス数がカウントされます。Citrix Cloud は、割り当て済みライセンスを計算するために、これらのうち少ない方の数を使用します。Citrix Cloud は、アクティブな使用状況を計算するために、特定の期間のアクティブなユーザーとアクティブなデバイスの数として、各カウントを使用します。

割り当て済みライセンスの計算例

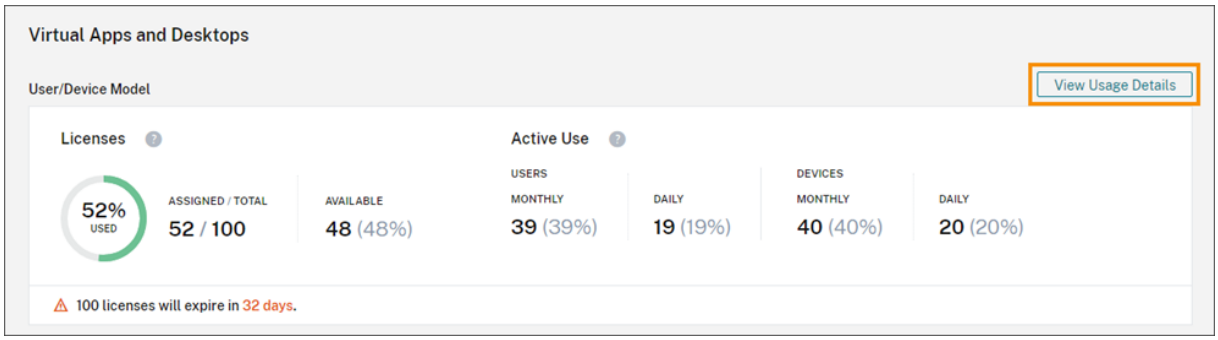
サービスを使用している一意のユーザー数が 100、一意のデバイス数が 50 の場合、Citrix Cloud では少ない方の数（50）を使用して割り当て済みライセンスの数を判断します。使用されているライセンスの割合と使用可能なライセンスの数は、割り当てられた 50 のライセンスに基づきます。

アクティブな使用状況の計算例

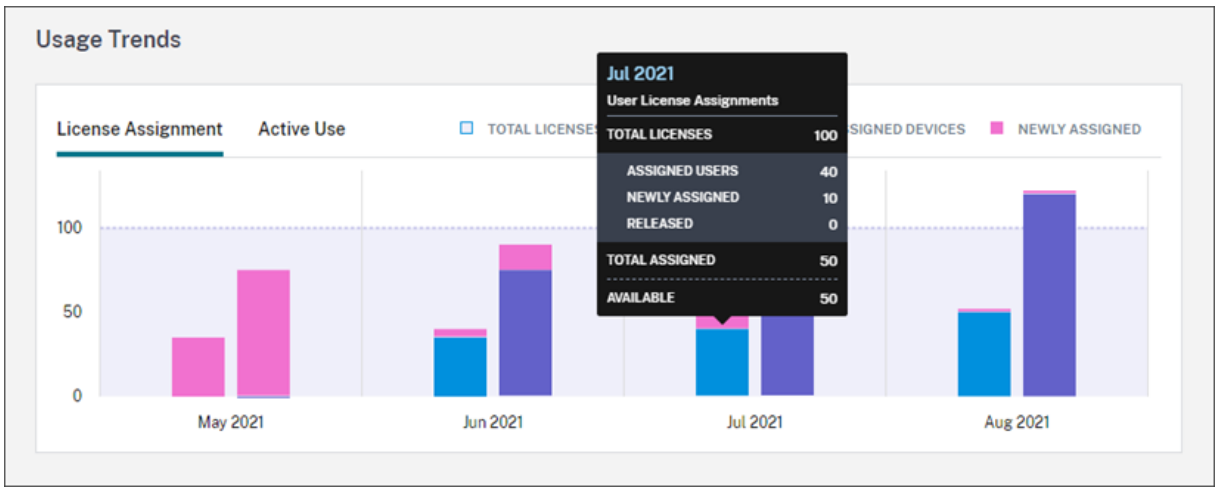
過去 30 日間に 10 人の一意のユーザーと 20 人の一意のデバイスがサービスを使用した場合、Citrix Cloud は、月次のアクティブな使用状況が 10 人のアクティブなユーザーと 20 人のアクティブなデバイスで構成されていると判断します。同様に、過去 24 時間以内に 30 人の一意のユーザーと 15 人の一意のデバイスがカウントされた場合、Citrix Cloud は、日次のアクティブな使用状況が 30 人のアクティブなユーザーと 15 人のアクティブなデバイスで構成されていると判断します。

使用状況の傾向とライセンスアクティビティ

ライセンスの詳細を表示するには、概要の右端にある ［使用状況の詳細の表示］をクリックします。使用傾向と、クラウドサービスライセンスを使用している個々のユーザーおよびデバイスの内訳を確認できます。



［使用状況の傾向］セクションでは、この内訳がグラフで表示されます。

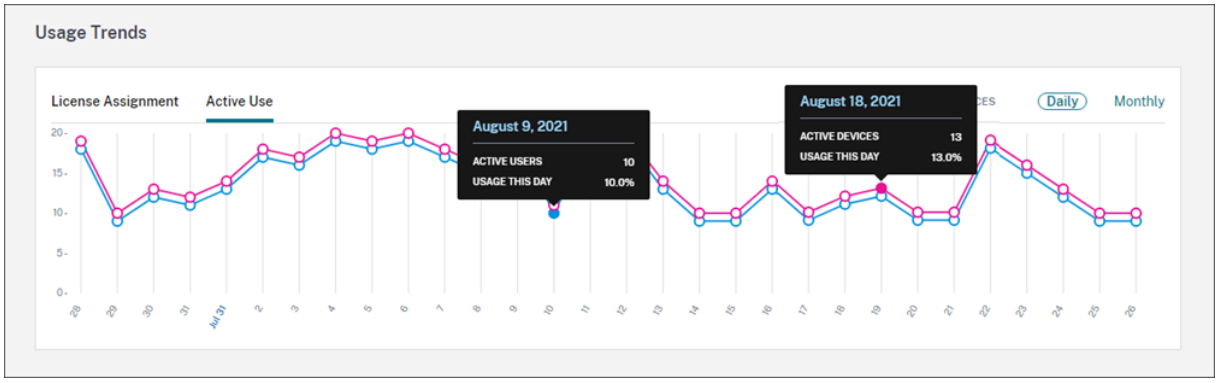


［ライセンス割り当て］グラフで、特定の月または日のバーをポイントすると、次の情報が表示されます：

- ライセンス合計：合計したクラウドサービス使用権のために購入済みのライセンス合計数。
- 割り当てられたユーザー：今月までにユーザーに割り当てられたライセンスの累積数。
- 割り当てられたデバイス：今月までにデバイスに割り当てられたライセンスの累積数。特定の月にこの数が特に多いと思われる場合、アプリまたはデスクトップが Web ブラウザーを介して起動していることが原因である可能性があります。この数を減らすには、ローカルにインストールされた Workspace アプリを使用することをお勧めします。

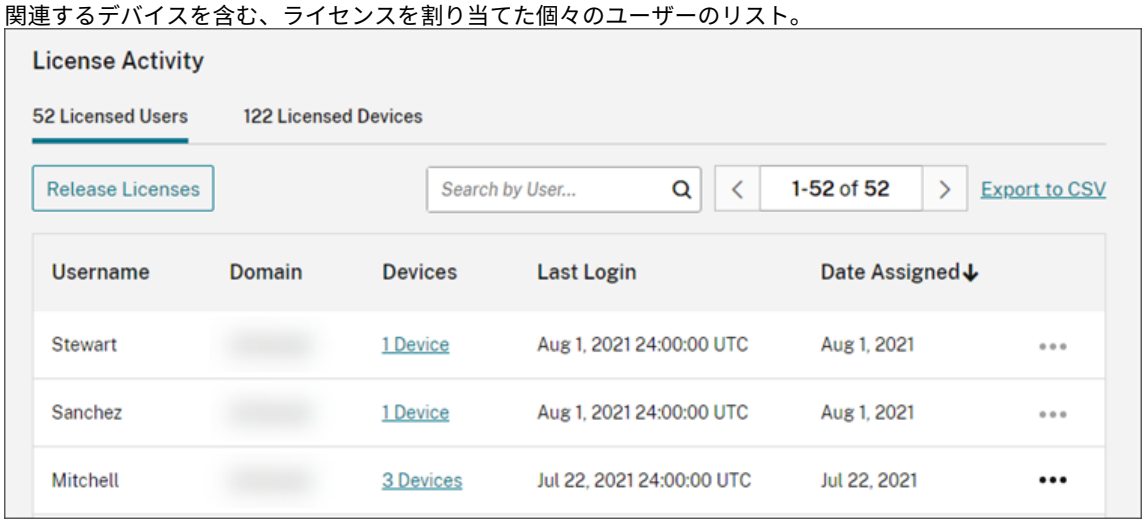
- 新しく割り当て済み：各月に割り当てられた新しいライセンスの数。たとえば、7 月にクラウドサービスに初めてアクセスするユーザーにライセンスが割り当てられたとします。このライセンスは、7 月に［新しく割り当て済み］としてカウントされます。
- リリース済み：各月にリリースされた対象ライセンスの数。たとえば、20 個のライセンスがリリースの対象であり、7 月に 10 個をリリースした場合、7 月に表示されるリリース済みライセンスの数は 10 個です。

［アクティブな使用］を選択して、前の暦月と暦年の、アクティブなユーザーとデバイスのグラフをそれぞれ表示します。グラフ上の特定の場所をポイントすると、アクティブなユーザーまたはデバイスの数と使用率が表示されます。



［ライセンスアクティビティ］セクションには、次の情報も表示されます：

- 関連するデバイスを含む、ライセンスを割り当てた個々のユーザーのリスト。



- 関連するユーザーを含む、ライセンスを割り当てたデバイスのリスト。

- ライセンスがユーザーまたはデバイスに割り当てられた日付。

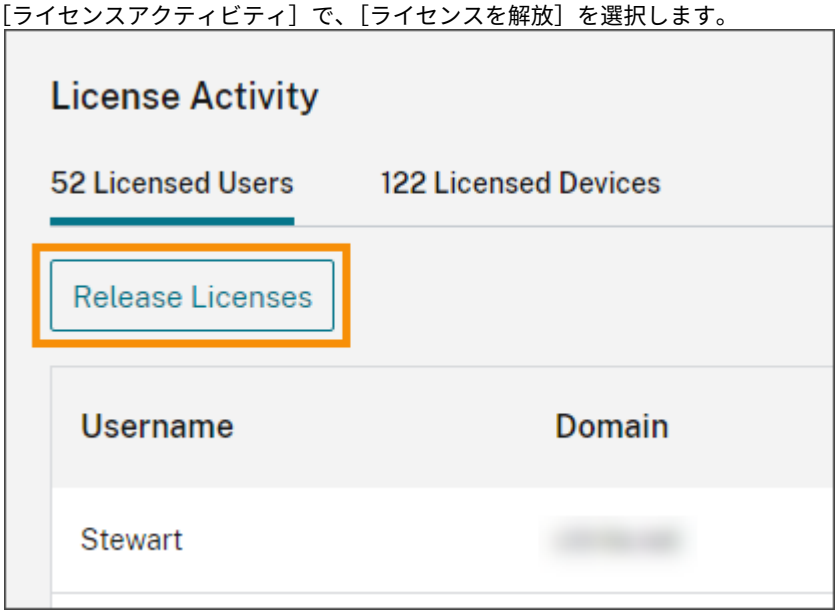
割り当て済みライセンスを解放する

過去 30 日間にアプリまたはデスクトップを起動していないユーザーのライセンスを解放できます。過去 30 日間にデバイスからアプリやデスクトップが起動されていない場合は、デバイスのライセンスを解放できます。ライセンスは複数を一括で解放するか、個別に解放できます。（これは、非アクティブなライセンスが 90 日後に自動的に解放されるオンプレミスの Citrix Virtual Apps and Desktops 展開とは異なります。）

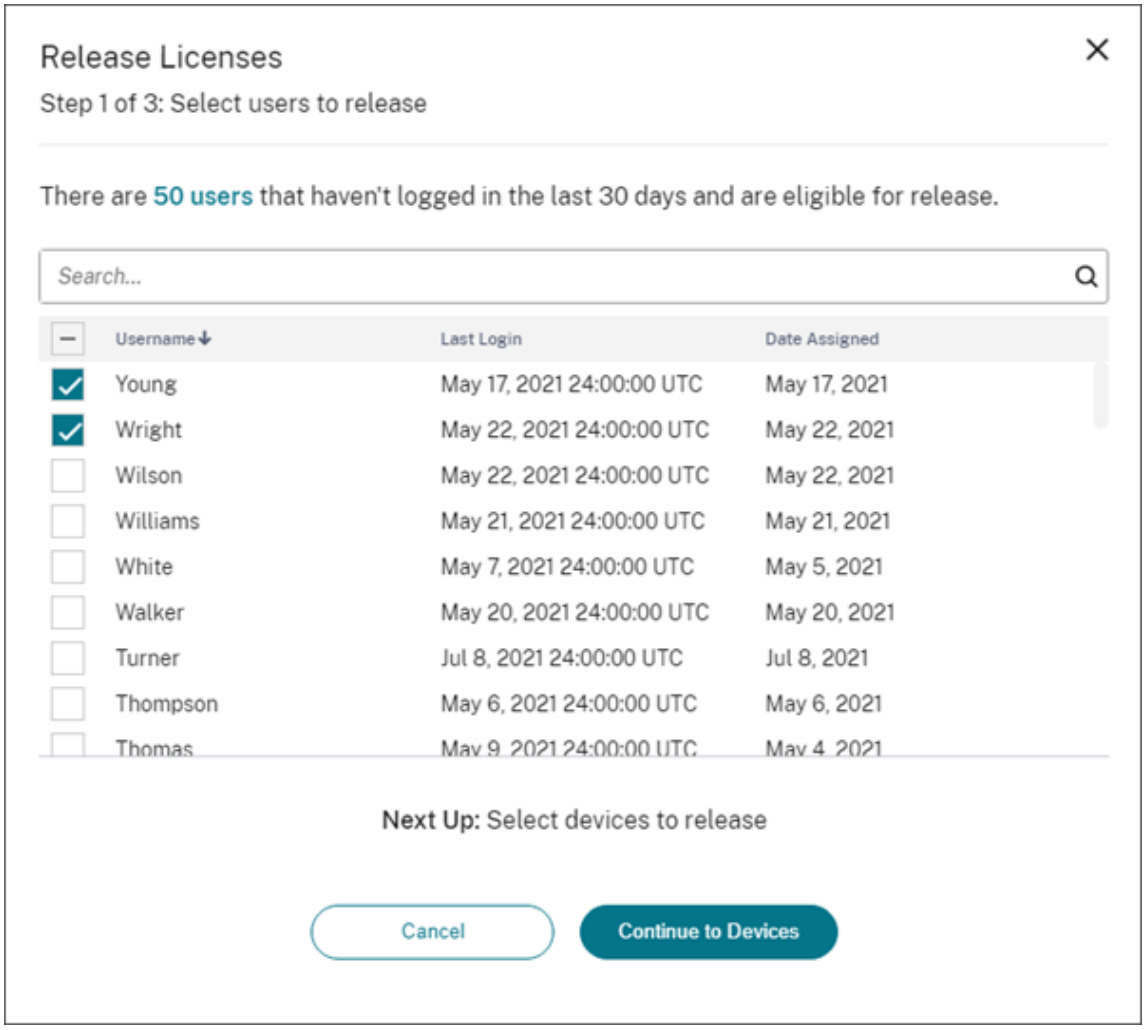
ライセンスが解放されると、それに応じて残りのライセンス数が増加し、割り当て済みライセンス数が減少します。ライセンスが解放された後、ユーザーはクラウドサービスにログインして使用することによって、別のライセンスを取得できます。

複数の割り当て済みライセンスを解放するには

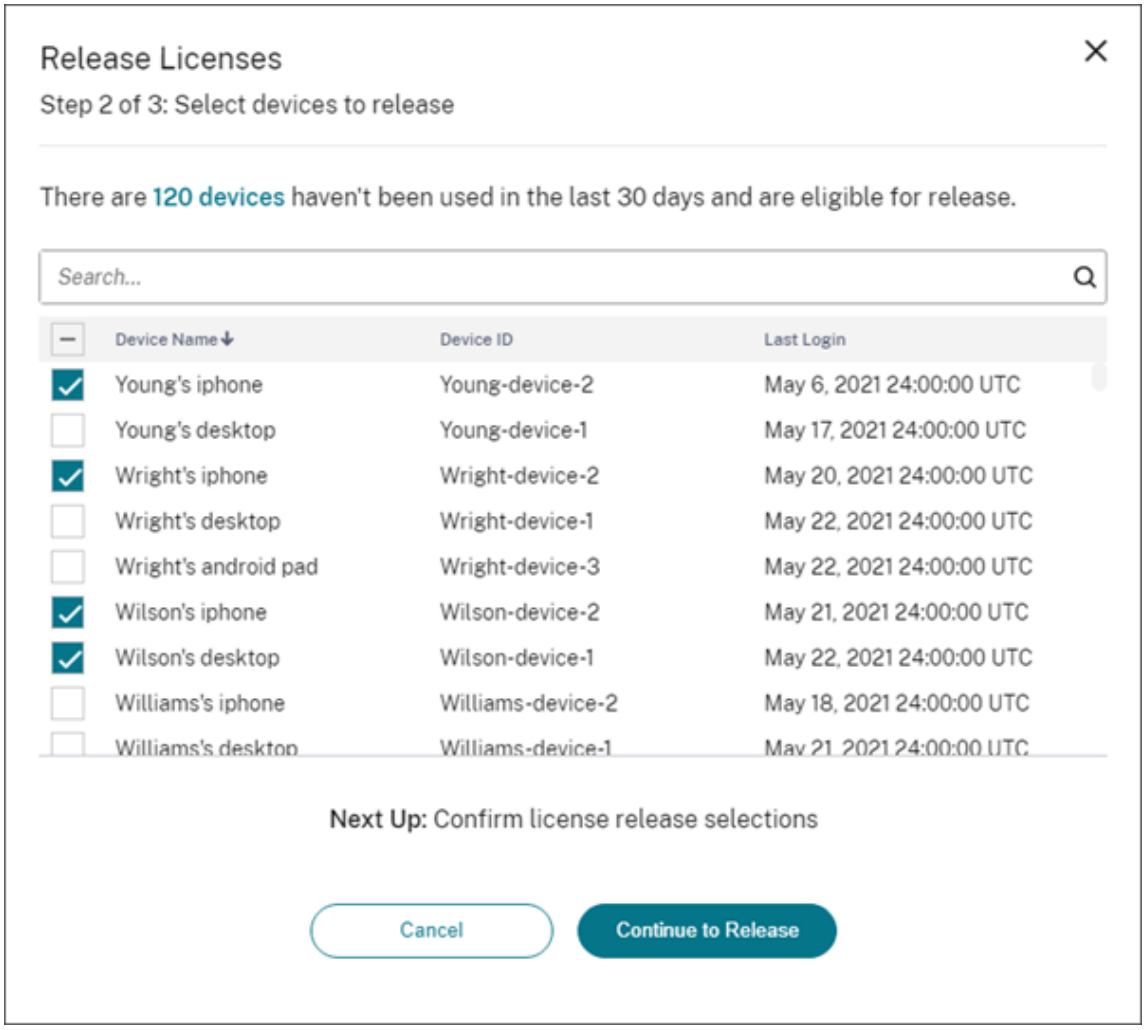
1. ［ライセンスアクティビティ］で、［ライセンスを解放］を選択します。



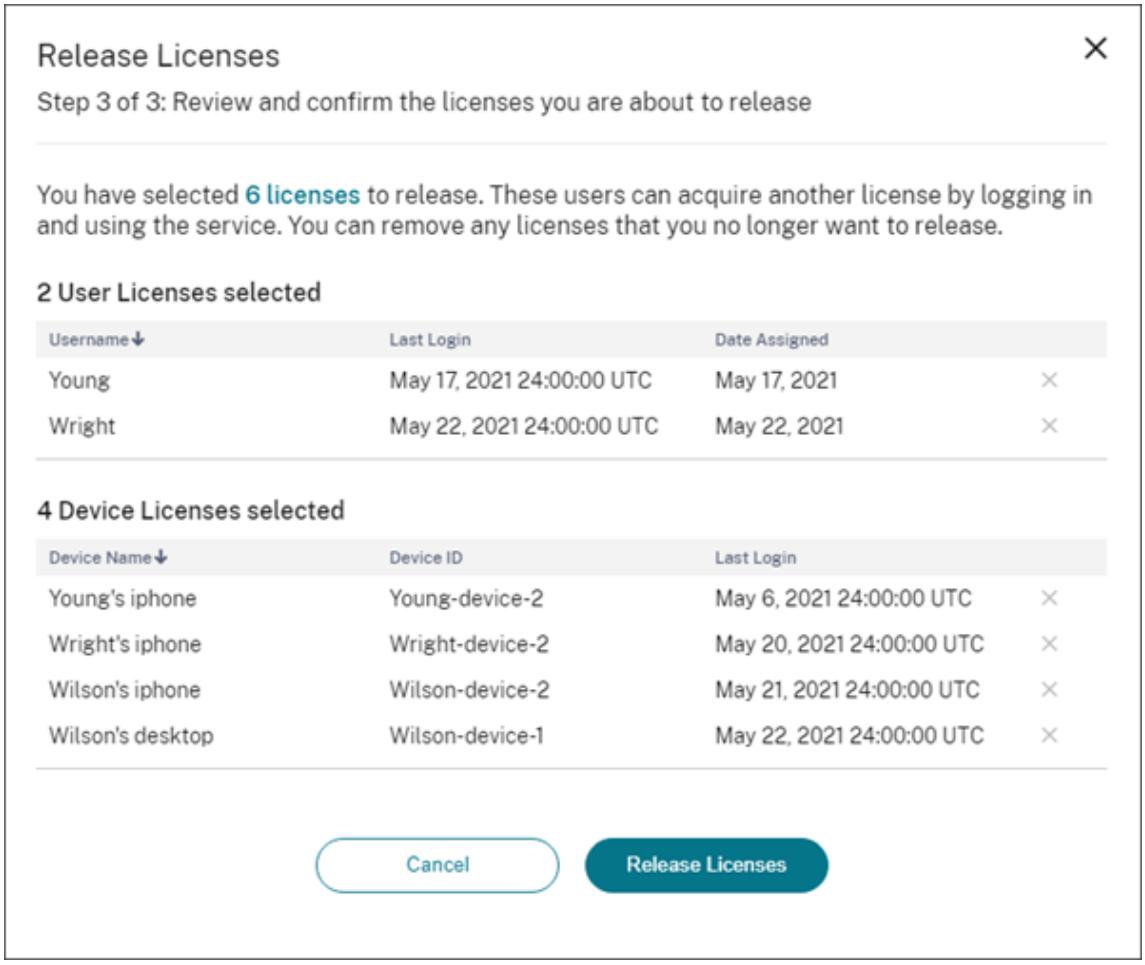
2. リストから、管理するユーザーを選択し、［**[**デバイス**]** に進む］を選択します。



3. 管理するデバイスを選択して ［**[**解放**]** に進む］を選択します。



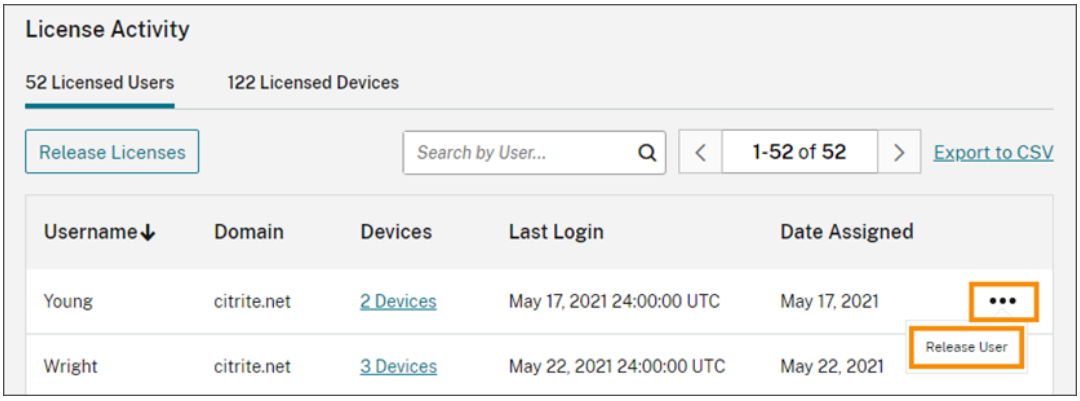
4. 選択したライセンスを確認して ［ライセンスを解放］を選択します。



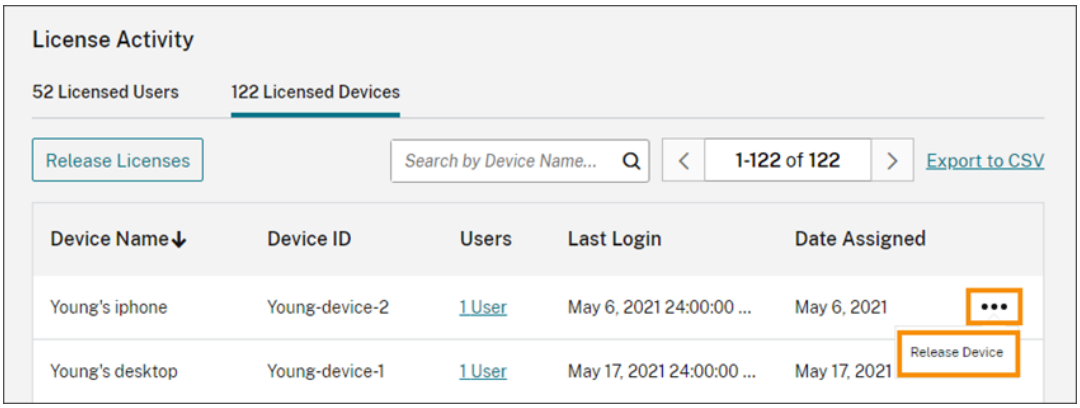
1 つの割り当て済みライセンスを解放するには

［ライセンス使用ユーザー］または ［ライセンス使用デバイス］リストから、個別のライセンスを解放できます。これらのリストには、解放対象のライセンスがあるユーザーまたはデバイスのみに省略ボタンが表示され、クリックできます。省略ボタンは、過去 30 日間にアプリやデスクトップを起動した個々のユーザーおよび個々のデバイスに対してはアクティブになりません。

1. ［ライセンスアクティビティ］で、［ライセンス使用ユーザー］または ［ライセンス使用デバイス］タブを選択します。
2. 管理するユーザーまたはデバイスを見つけて、ライセンスを解放します:
   a) 単一ユーザーのライセンスを解放するには、省略記号ボタンをクリックして ［ユーザーを解放］を選択します。



b) 単一デバイスを解放するには、省略記号ボタンをクリックして ［デバイスの解放］を選択します。



3. 選択内容を確認してから ［続行］を選択します。
4. 解放を確認するメッセージが表示されたら、［解放］を選択します。

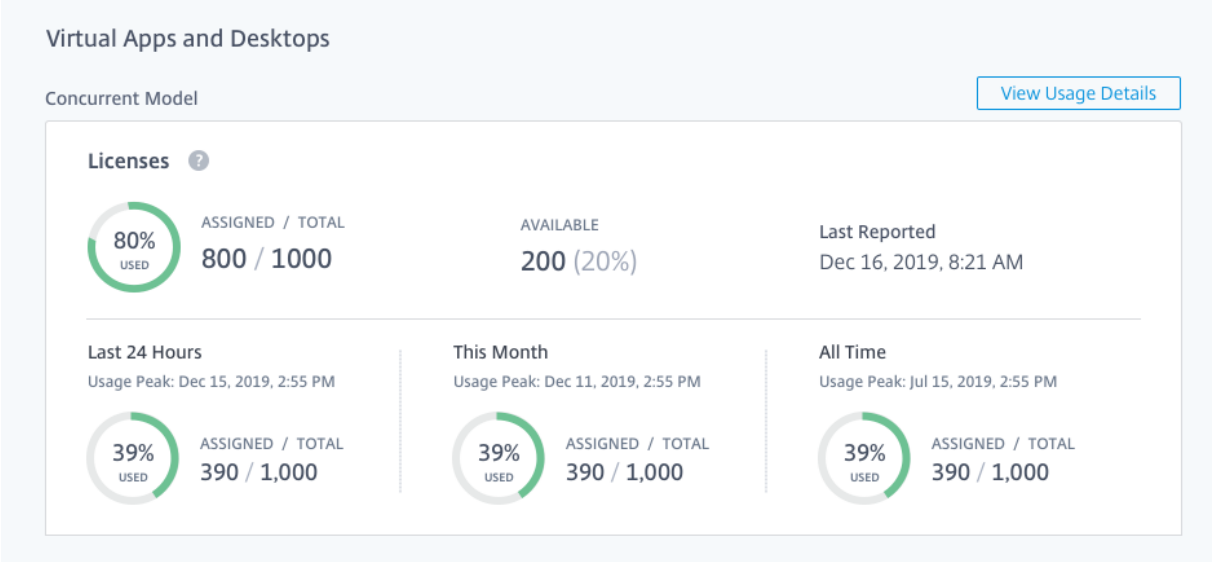
Citrix Virtual Apps and Desktops サービスのライセンスとピーク時の使用状況の監視（同時使用）

September 17, 2021

ライセンス割り当て

Citrix Cloud では、デバイスにあるアプリまたはデスクトップをユーザーが起動したときにライセンスが割り当てられます。ユーザーがログオフするか、セッションから切断すると、ライセンスは割り当てられなくなります。ライセンスの割り当ては、アプリまたはデスクトップにアクセスするデバイスの数に応じて変わる可能性が常にあるため、Citrix Cloud は 5 分ごとに使用中のライセンスの数を評価します。同時使用ライセンスモデルについて詳しくは、「同時使用ライセンス」を参照してください。

ライセンスの概要



ライセンスの概要では、次の情報を一目で確認できます:

- Citrix Cloud が使用中のライセンスを最後に評価したときに使用中だった購入済みライセンスの合計の割合。Citrix Cloud は、サービスへのアクティブな接続を持つ一意のデバイスに基づいて、5 分ごとにこの割合を計算します。

  購入したライセンスの総数は、同時使用ライセンスモデルを使用する Virtual Apps、Virtual Desktops、および Virtual Apps and Desktops サービスの使用のために購入したライセンスの合計です。

- 購入したライセンスの合計に対する現在割り当てられているライセンスの比率、および使用可能なライセンスの残りの数。この比率に示す［合計］の数値は、現在所有しているライセンスの合計数を表します（[最新レポート］の日時の時点での内容）。

- ピーク時使用状況の統計。ピーク時のライセンス使用を計算する場合、Citrix Cloud は、次の期間に使用されたライセンスの最大数を取得します:

  - 過去 **24** 時間: 過去 24 時間で同時使用されたライセンスの最大数。
  - 今月: 現在の暦月に入ってから同時使用されたライセンスの最大数。
  - 常時: サブスクリプションが開始してから同時使用されたライセンスの最大数。

  これらのピーク時使用状況期間に示される［合計］の数値は、その時点で所有していたライセンスの総数を表します。所有ライセンスの合計数が増加または減少し、それに伴って割り当てられたライセンスが増加した場合、［合計］の数値は、その時点における所有ライセンスの新しい数を反映して変更されます。ただし、対応する使用量のピークがない場合、［合計］の数値は変化しません。

ピーク時のライセンス使用の計算

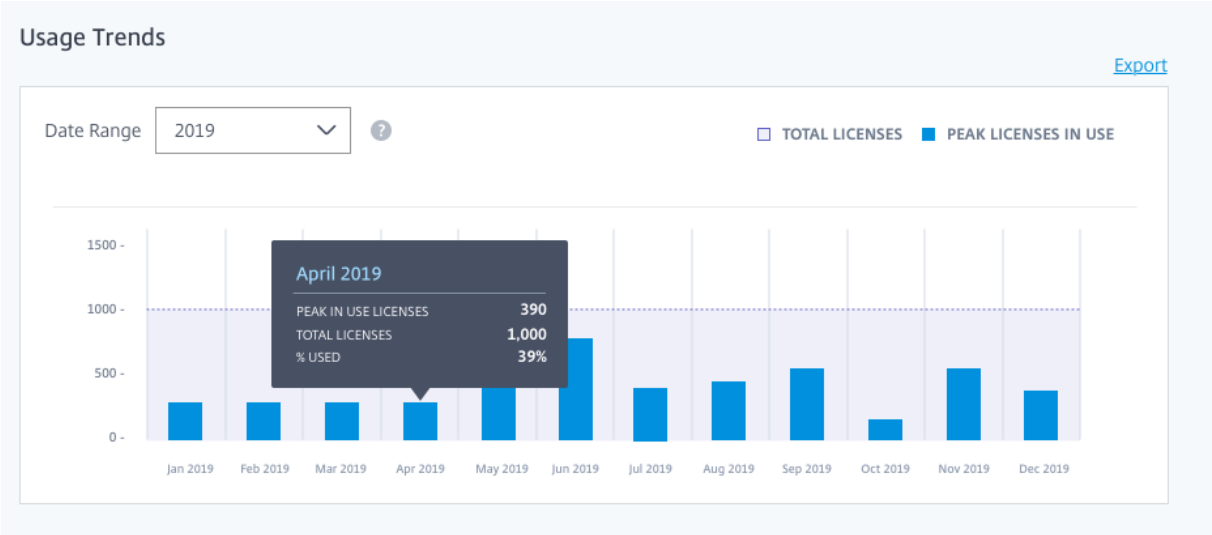
Virtual Apps and Desktops サービスの同時使用ライセンスモデルが正確に反映されるよう、Citrix Cloud ではサービスに同時にアクセスする一意のデバイスの数が 5 分ごとにカウントされます。このカウントで、表示されている

現在のピーク使用量よりも多くなった場合、Citrix Cloud では、新しいピーク使用量と、その使用量に達した日時が表示されます。カウントが現在のピーク使用量より少ない場合、現在のピーク使用量は変更されません。

> 重要:
>
> Director で［監視］を使用して同時セッションに関する情報を入手する場合、監視レポートで提供される同時セッションの解釈は異なり、使用中の同時ライセンスの数を正確に反映しないことに注意してください。監視レポートとライセンスレポートの違いについて詳しくは、「よくある質問」を参照してください。

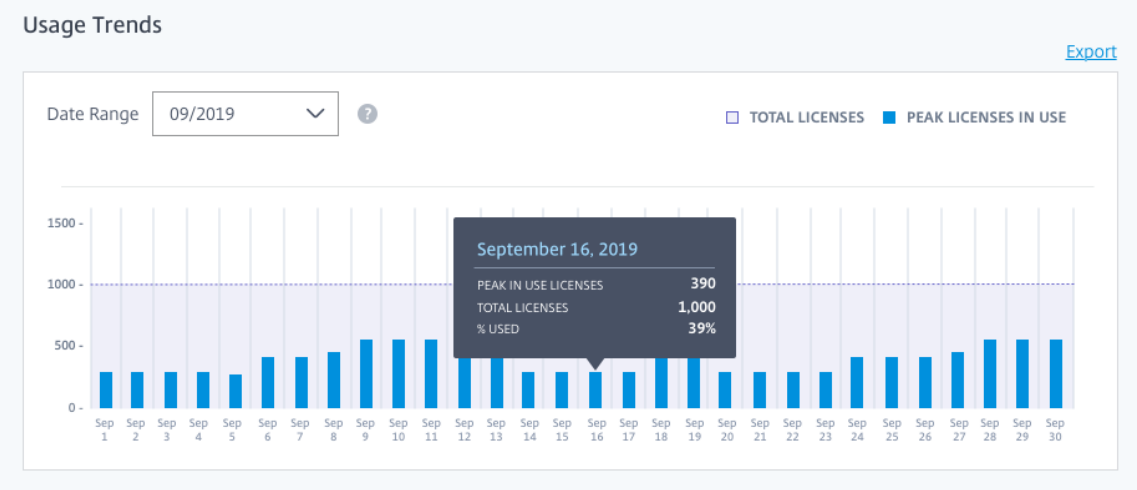
使用状況の傾向とライセンスアクティビティ

ライセンスの履歴を表示するには、［使用状況の詳細の表示］をクリックします。

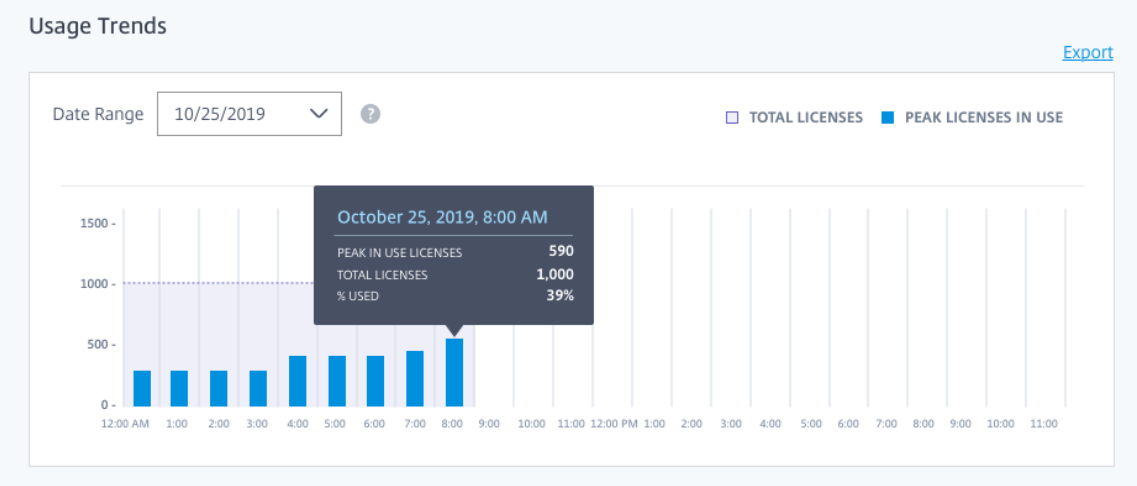


［使用状況の傾向］の詳細に次の情報が表示されます:

- ライセンス数合計: 購入した同時ライセンスの合計。
- ピーク時のライセンス使用: 選択した日付範囲に割り当てられたライセンスの最大数。デフォルトでは、Citrix Cloud は現在の暦年の各月のピーク使用量を表示します。月間または時間ごとのピーク使用量を確認するには、表示する暦月または暦日を ［日付範囲］ メニューから選択します。



選択した日付範囲がまだ終了していない場合、Citrix Cloud にはその時点において最新の時間間隔のピーク使用量が表示されます。たとえば、現在進行中の暦日を確認する場合、その瞬間までの 1 時間ごとの最大ライセンス数が表示されます。次の 5 分のカウント間隔でライセンスの最大数が増えると、Citrix Cloud ではその 1 時間のピーク使用量が更新されます。



Citrix Virtual Apps and Desktops Standard for Azure サービスのライセンスとアクティブな使用状況の監視

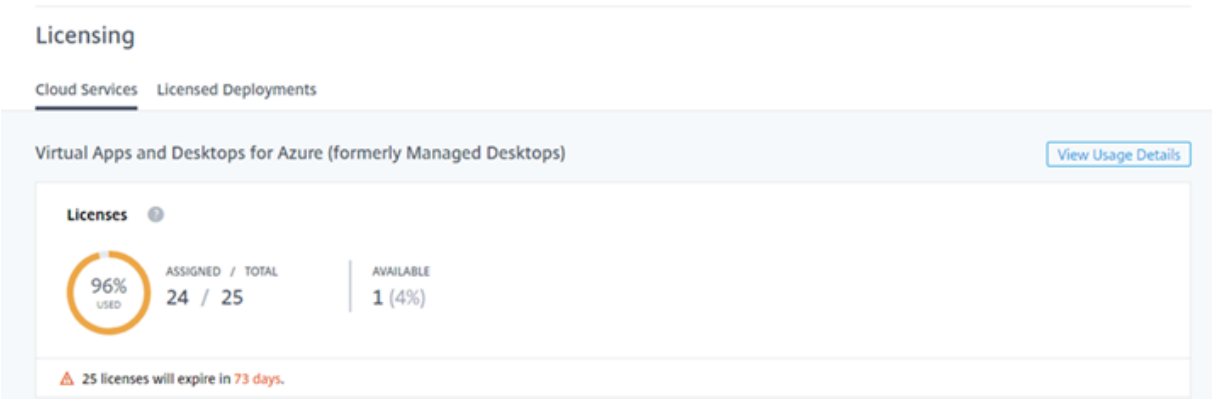
January 21, 2021

この記事では、ユーザー/デバイスライセンスモデルのクラウドライセンスレポート内容についてのみ説明します。

ライセンス割り当て

Citrix Cloud では、一意のユーザーまたはデバイスによるデスクトップの初回起動時にライセンスが割り当てられます。

ライセンスの概要



ライセンスの概要では、次の情報を一目で確認できます:

- 購入済みライセンス合計に対する割り当て済み（使用済み）ライセンスの割合。割合が 100% に近づくにつれて、表示は緑色から黄色に変わります。割合が 100% を超えると、表示が赤になります。
- 購入したライセンスに対する割り当てられたライセンスの比率、および使用可能なライセンスの残りの数。

[使用状況の詳細の表示] をクリックして、使用状況レポートおよび傾向の詳細と、Citrix Virtual Apps and Desktops Standard for Azure ライセンスを消費しているユーザー一覧を表示できます。

> 注:
>
> Citrix Virtual Apps and Desktops Standard for Azure は、以前は Citrix Managed Desktops と呼ばれていました。一部の表示には、旧名称が含まれている場合があります。

使用状況レポート

使用状況の情報を標準の間隔、または指定の間隔でダウンロードできます。

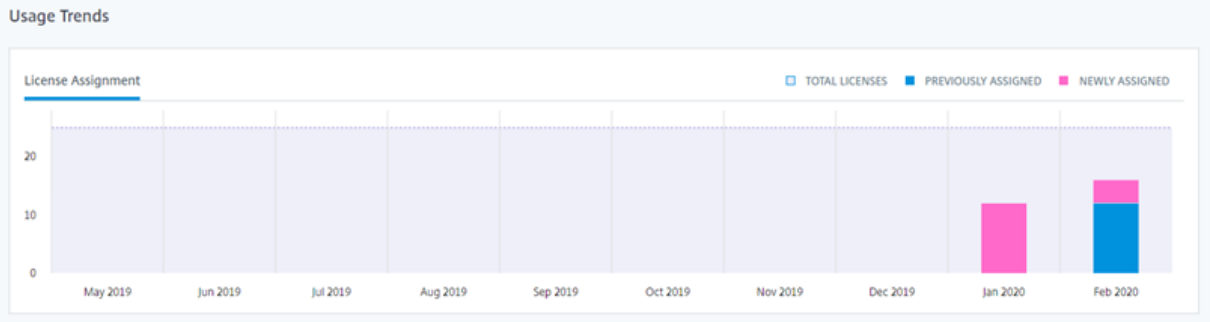
情報には、次の項目に関するメーターの使用量が含まれます:

- Azure 仮想マシン
- ネットワーク接続（VNet ピアリングなど）
- Managed Disks、ブロック BLOB、ページ BLOB のような Azure ストレージの項目

すべての使用状況がデータに反映されるまで 1 日または 1 月の終わりから最大 72 時間を要することがあります。

[**Download Data**] をクリックし、CSV ファイルを生成して、ローカルマシンにダウンロードします。

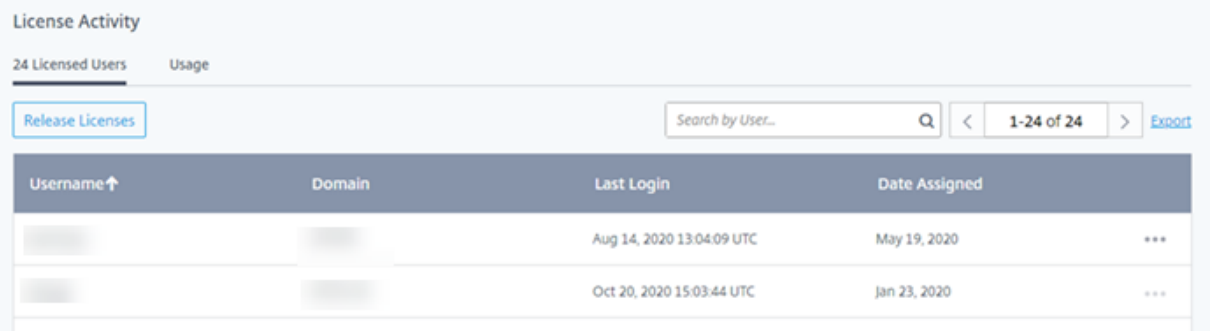
使用状況の傾向とライセンスアクティビティ



［使用状況の傾向］の詳細に次の情報が表示されます：

- ライセンス合計：合計したクラウドサービス使用権のために購入済みのライセンス合計数。
- 以前に割り当て済み：先月割り当てられたライセンスの数。たとえば、7 月にクラウドサービスに初めてアクセスするユーザーにライセンスが割り当てられたとします。このライセンスは、7 月に「新しく割り当て済み」としてカウントされます。8 月には、「以前に割り当て済み」としてカウントされます。
- 新しく割り当て済み：各月に割り当てられた新しいライセンスの数。たとえば、7 月にクラウドサービスに初めてアクセスするユーザーにライセンスが割り当てられたとします。このライセンスは、7 月に「新しく割り当て済み」としてカウントされます。

［ライセンスアクティビティ］セクションでは、ライセンスを割り当てた個々のユーザーの一覧とユーザーにライセンスが割り当てられた日付が表示されます。



割り当て済みライセンスを解放する

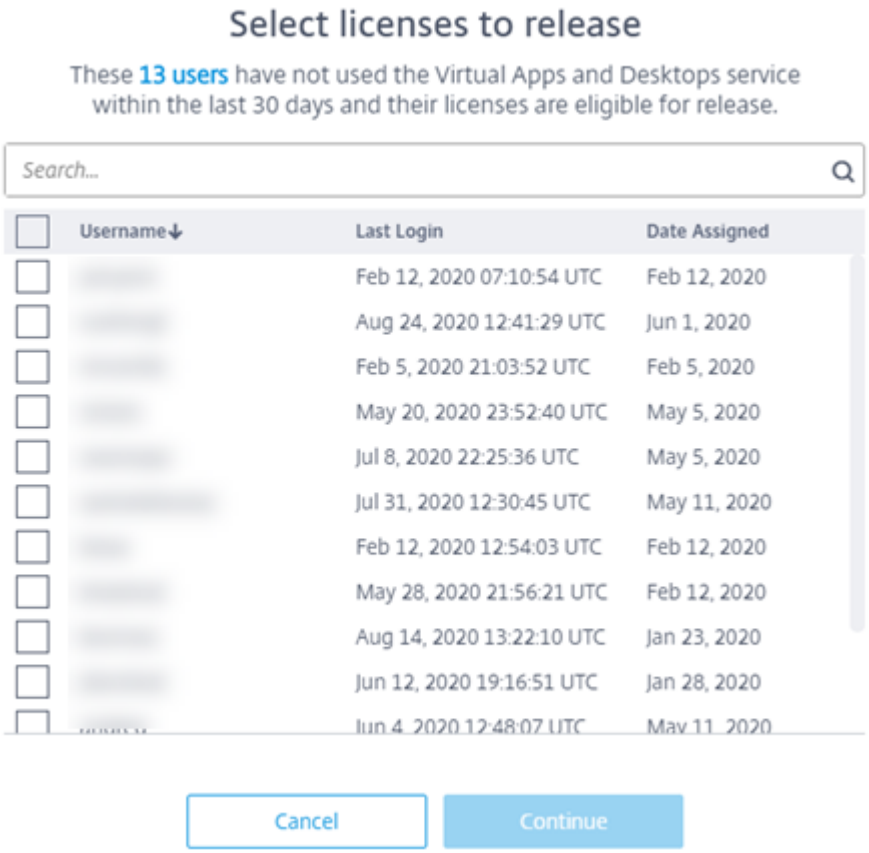
年単位サービスサブスクリプション：年単位サブスクリプションがある場合は、過去 30 日間にアプリまたはデスクトップを起動していないユーザーのライセンスを解放できます。ライセンスは複数を一括で解放するか、個別に解放できます。

月単位サービスサブスクリプション：月単位サブスクリプションがある場合は、非アクティブ期間に関係なく、各月の 1 日にライセンスを解放できます。

ライセンスが解放されると、それに応じて残りのライセンス数が増加し、割り当て済みライセンス数が減少します。ライセンスが解放された後、ユーザーはクラウドサービスにログインして使用することによって、別のライセンスを取得できます。

複数の割り当て済みライセンスを解放するには

1. ［ライセンスアクティビティ］で、［ライセンスを解放］を選択します。
2. リストから、管理するユーザーを選択し、［続行］を選択します。



3. 選択したライセンスを確認して ［ライセンスを解放］を選択します。

1 つの割り当て済みライセンスを解放するには

［ライセンスアクティビティ］リストから、個別のライセンスを解放できます。リストには、解放対象のライセンスがあるユーザーのみに省略ボタンが表示され、クリックできます。

1. ［ライセンスアクティビティ］で、管理するユーザーを見つけます。そのユーザーの省略記号メニューから、［ユーザーを解放］を選択します。
2. 選択内容を確認してから ［続行］を選択します。
3. 解放を確認するメッセージが表示されたら、［解放］を選択します。

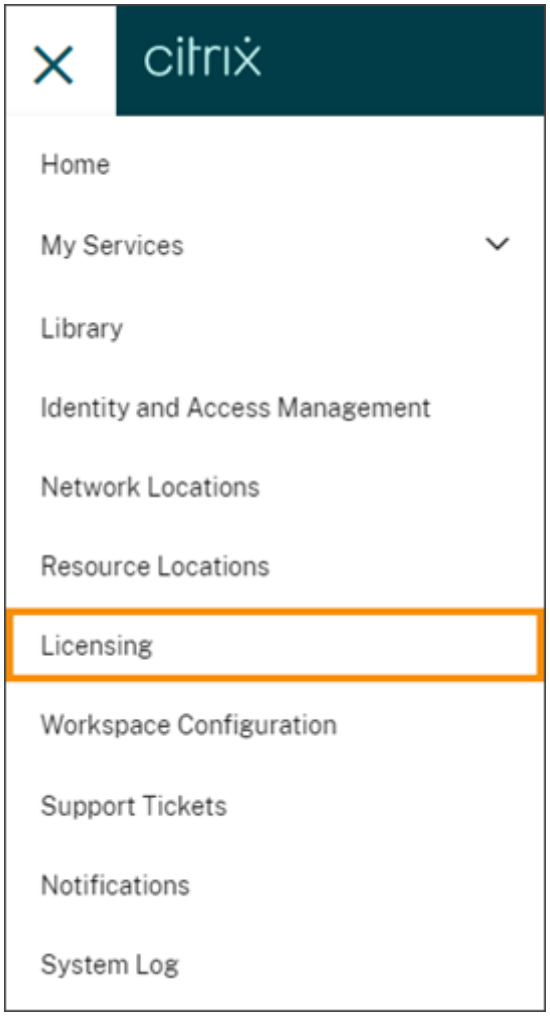
オンプレミス展開のライセンスと使用状況の監視

March 18, 2021

Citrix Cloud のライセンス割り当て済み展開画面には、次の機能があります:

- 製品登録: 既存の Citrix ライセンスサーバーを Citrix Cloud に登録して、展開に関する詳しい使用状況の識見とレポートを取得できます。ライセンスサーバーの登録について詳しくは、「Citrix Cloud を使用するオンプレミス製品の登録」を参照してください。
- ライセンスサーバーの状態: Citrix ライセンスサーバーの状態を表示して、使用状況を正常に報告しているサーバーと、Citrix Cloud に最後に使用状況を報告した日時を把握できます。
- 使用状況の識見: Citrix ライセンスサーバー全体でインストールされ、使用されているライセンスの数を表示して、ライセンス使用傾向の履歴を把握できます。

Citrix ライセンスサーバーの使用状況の識見を表示するには、コンソールメニューで［ライセンス］を選択し、［ライセンス割り当て済みの展開］を選択します。



前提条件

Citrix ライセンスサーバーの使用状況の識見を使用するには、次の要素が必要です:

- Citrix ライセンスサーバーバージョン 11.15.0.0 以降

- Citrix Cloud アカウント
- Citrix ライセンスサーバーから Citrix Cloud へのネットワークアクセス

サポートされている製品

Citrix ライセンスサーバーの使用状況の識見は、同時使用ライセンスモデルおよびユーザー/デバイスライセンスモデルで Virtual Apps and Desktops のすべてのエディションに関して利用できます。

オンプレミス製品ライセンスの使用状況の表示

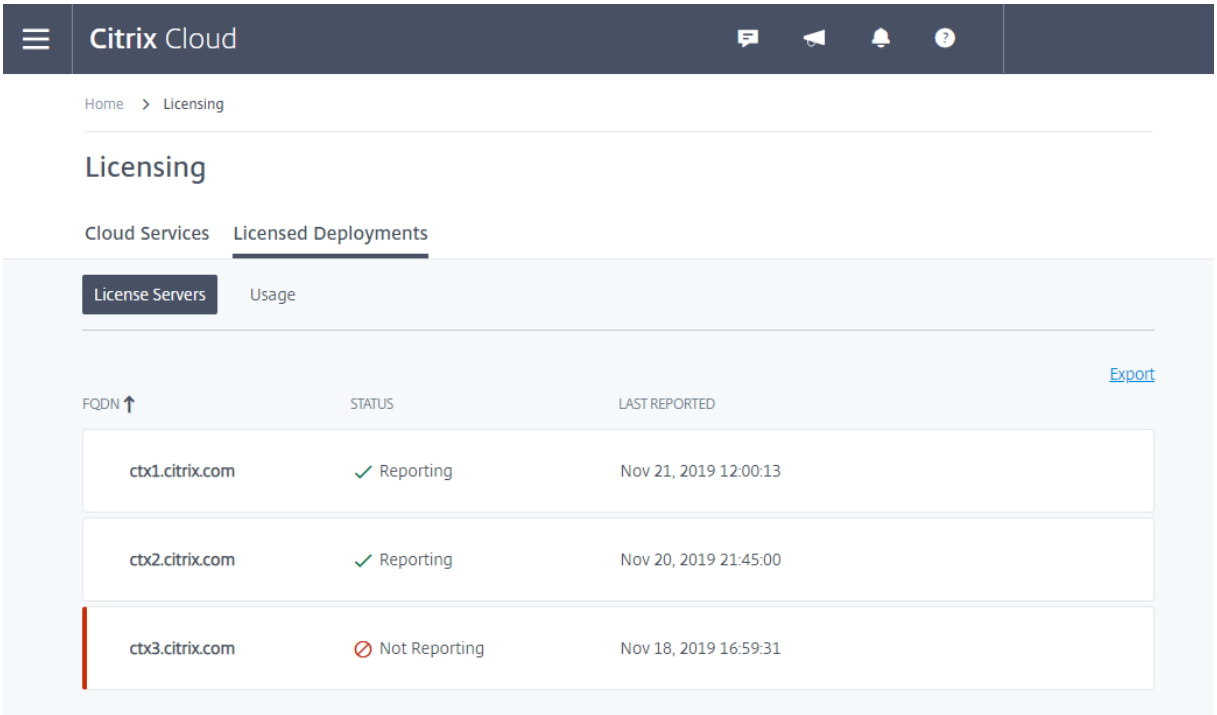
Citrix ライセンスサーバーの使用状況の識見により、シトリックス資産全体のライセンス使用状況を表示できます。ライセンスサーバーの使用状況の識見を有効にして Citrix Cloud に登録すると、次のような便利な使用状況レポートにアクセスできます:

- 展開および登録されているライセンスサーバーの数、およびこれらのサーバーが使用状況情報を Citrix Cloud に報告しているかどうかを把握できます。
- Virtual Apps and Desktops の同時使用ライセンスとユーザー/デバイスライセンス使用状況を表示できます。
- 複数展開の同時使用ライセンスとユーザー/デバイスライセンス使用状況が集約された識見を得ることができます。
- 過去のライセンス使用状況の傾向と毎月のライセンス使用状況の傾向を把握できます。
- 特定のユーザーの最終ログイン時間を表示できます。
- Citrix ライセンスサーバー全体でインストールされているライセンスに対する使用中のライセンスの数を比較できます。
- ライセンスの超過使用保護を監視できます。
- 同時使用ライセンスとユーザー/デバイスライセンスの使用状況の内訳を表示できます。

ライセンスサーバーの登録について詳しくは、「Citrix Cloud を使用するオンプレミス製品の登録」を参照してください。

ライセンスサーバーの状態の表示

ライセンスサーバーの状態には、Citrix Cloud に使用状況を報告する各ライセンスサーバーが表示されます。



ライセンスサーバーは、過去 3 日間に使用状況を Citrix Cloud に正常にアップロードしている場合、「レポート」状態を表示します。ライセンスサーバーは、過去 30 日間の使用状況を報告し、過去 3 日間は報告していない場合、「レポートを送信していません」状態を表示します。過去 30 日間に使用状況が報告されていないライセンスサーバーは、一覧から削除されます。

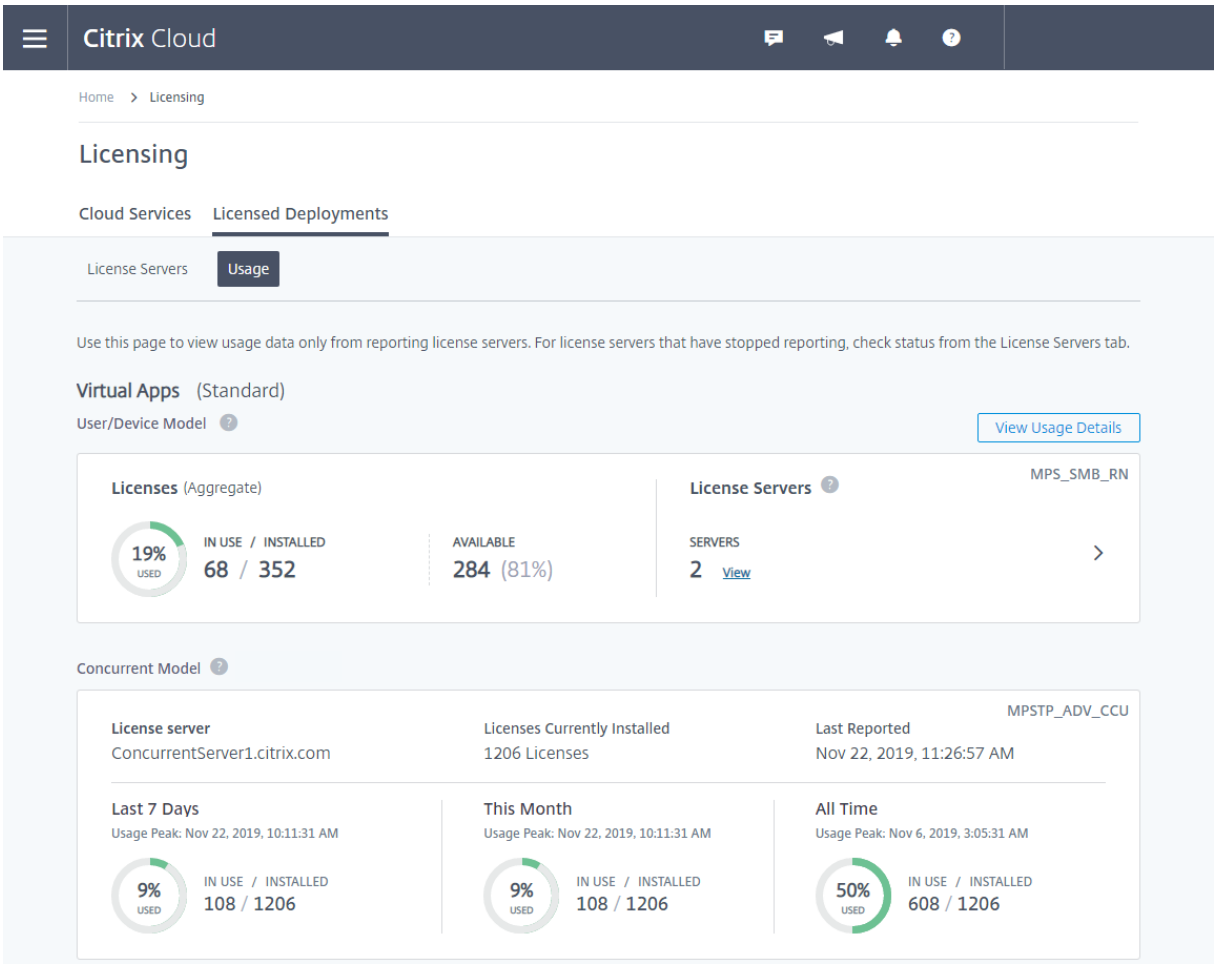
ライセンスサーバーの状態がライセンス使用状況表示に与える影響

ライセンスサーバーのレポートの状態と［最新レポート］の日付によって、使用状況の識見の表示およびレポートに特定のライセンスサーバーの使用状況が含まれるかどうかがわかります。

- 現在インストールされているライセンスおよび使用されているライセンスは、レポートライセンスサーバーからのデータのみに基づいて表示されます。ライセンスサーバーが「レポートを送信していません」として表示されている場合、このライセンスサーバーからインストールされているライセンスおよび使用されているライセンスは、使用状況の識見の画面に反映されません。
- 各ライセンスサーバーの［最新レポート］日によって、使用状況の識見の画面で表示されるライセンス使用状況の情報がどのくらい新しいかを判断できます。表示されるライセンス使用状況レポートは、各ライセンスサーバーの［最新レポート］時刻の時点での内容です。
- 使用状況の識見用に構成され、Citrix Cloud に登録された Citrix ライセンスサーバーは、1 日に 1 回使用状況を更新します。必要に応じて、ライセンスサーバー上の Citrix License Manager 管理コンソールから更新を強制できます。

ライセンス使用状況

［使用状況］タブは、Citrix 展開全体でのライセンス使用状況の統合ビューを提供します。各レポートライセンスサーバーからのライセンス情報は、シングルビューに結合されます。このビューを使用すると、さまざまな展開およびライセンスサーバー全体でのライセンスの概要を簡単に確認できます。



ライセンスの使用状況は、製品のエディションとライセンスモデルに基づいて、複数のライセンスサーバー間で整理および集約されます。すべてのレポートライセンスサーバーで検出された一意のライセンスエディションごとに、ライセンス使用状況の概要カードが表示されます。検出された製品エディションごとに概要カードが表示されます。

同時使用ライセンスモデルのピーク時のライセンス使用状況

同時使用ライセンスのレポート内容は、次のデータポイントを中心に構成されています：

- インストール済みライセンス：各ライセンスサーバーにインストールされているライセンスの数。
- ピーク時のライセンス使用：特定の期間に使用されたライセンスの最大数。

ピーク時のライセンス使用を計算する場合、Citrix Cloud は、次の期間に使用されたライセンスの最大数を取得します：

- 過去 7 日間：過去 7 日間に同時使用されたライセンスの最大数。
- 今月：現在のカレンダー月に同時使用されたライセンスの最大数。
- 常時：ライセンスサーバーが Citrix Cloud に登録されてから同時使用されたライセンスの最大数。

> 重要：
>
> これらの期間のデータは、ライセンスサーバー上の使用中のライセンス数と一致しないことがあります。ライセンスサーバーが報告するのは、任意の時点で使用中のライセンス数だけです。Citrix Cloud は、これらの個別データポイントを受信して、これらの期間のピークを計算します。

ライセンス使用状況の解釈に関する考慮事項

Citrix ライセンスは多くの使用シナリオに対応し、詳細な情報を含みます。使用状況を監視するときは、次の考慮事項に留意してください：

- 使用情報は、各レポートライセンスサーバーにインストールされているライセンスに基づいています。ライセンスサーバーで使用可能なライセンスが不足している場合は、ライセンスサーバーに追加のライセンスを割り当てて配置し、使用可能なライセンスの数を増やすことができます。
- Citrix ライセンスサーバーの使用状況の識見で利用可能な情報には、登録済みのアクティブなレポート用 Citrix ライセンスサーバーによって収集およびレポートされた情報のみが含まれます。ライセンス割り当て済みの展開環境は、実際に所有または購入したライセンスの総数ではないため、総数と一致しない場合があります。
- 使用可能なライセンスの割合は、レポートライセンスサーバーにインストールされているライセンスに対する使用中のライセンスの数に基づいて計算されます。

Citrix Cloud を使用するオンプレミス製品の登録

September 17, 2021

Citrix Cloud からの短いコードによるアクティブ化機能を使用して、オンプレミスの Citrix 製品を簡単に登録できます。製品によっては、製品のインストールプロセス中または製品の管理コンソールの実行中に、この 8 桁のコードが生成されます。製品がユーザーに登録を要求するとき、製品は Citrix Cloud からコードを要求して表示します。その後、Citrix Cloud でこのコードをコピーして貼り付けるか、手動で入力します。

オンプレミスライセンスサーバーの登録

製品登録は Citrix ライセンスサーバーでサポートされています。この機能を使用するには、次のタスクを行います：

- Call Homeを有効にします。
- Citrix Licensing Manager コンソールから Citrix Cloud を使用するライセンスサーバーを登録します。

オンプレミスライセンスサーバーを Citrix Cloud に登録する方法については、「Citrix ライセンスサーバーの登録と登録削除」を参照してください。

接続の要件

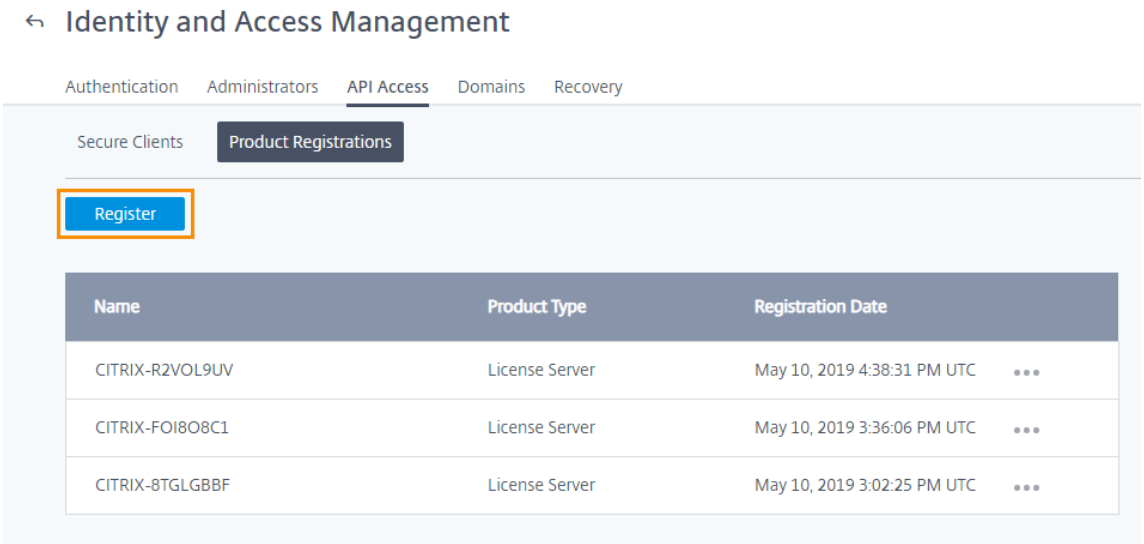
オンプレミス製品を正常に登録するには、次のアドレスに接続可能であることを確認してください:

- https://trust.citrixnetworkapi.net（コードを取得する場合）
- https://trust.citrixworkspacesapi.net/ （ライセンスサーバーが登録されていることを確認する場合）
- https://cis.citrix.com（データをアップロードする場合）
- https://core-eastus-release-a.citrixworkspacesapi.net
- https://core.citrixworkspacesapi.net（ライセンスサーバー証明書が取り消されていないことを確認する場合）
- ocsp.digicert.com port 80
- crl3.digicert.com port 80
- crl4.digicert.com port 80
- ocsp.entrust.net port 80
- crl.entrust.net port 80

Citrix ライセンスサーバーにプロキシサーバーを使用している場合、プロキシサーバーがライセンスサーバー製品ドキュメントの「プロキシサーバーの構成」の説明どおりに構成されていることを確認します。

製品の登録

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. [**API** アクセス] **>** [製品の登録] を選択して、[登録] を選択します。

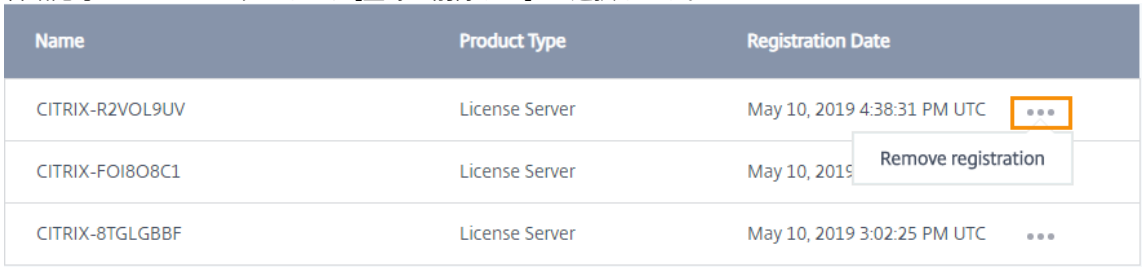


3. Citrix 製品の 8 桁の製品登録コードを入力して、[次へ] をクリックします。
4. 登録の詳細を確認してから、[登録] をクリックします。

製品登録の削除

環境から登録済みの Citrix 製品を実行しているサーバーを削除しても、製品登録ページにはこれらのサーバーが表示されます。サーバーを Citrix Cloud から削除するには、次の手順を実行します：必要に応じて後から製品を再度登録し、［製品登録］ページにサーバーを表示できます。

1. ［製品登録］ページで削除するサーバーを特定します。
2. 省略記号ボタンをクリックして、［登録を削除する］を選択します。



3. プロンプトが表示されたら、［削除］を選択します。

Citrix Service Provider 用のライセンス

September 17, 2021

Citrix Cloud の License Usage Insights サービスは、**Citrix Service Provider**（**CSP**）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。CSP パートナーのみが License Usage Insights にアクセスできます。

LUI サービスでは、次のことを実行できます：

- Citrix ライセンスサーバーから製品使用情報を自動的に収集して集計する
- シングルテナントおよびマルチテナントの顧客のクラウドライセンスの使用状況と消費量を自動的に集計する
- 毎月 Virtual Apps and Desktops 展開環境にアクセスしているユーザーを簡単に確認する
- ライセンス使用状況に関する顧客の内訳を作成する
- 無料ユーザーを特定して追跡することにより、ライセンスコストを最適化する
- シトリックスとの過去のビジネス実績を表示し理解する
- Virtual Apps and Desktops 製品とクラウドライセンスの使用状況、ADC VPX 割り当てデータ、および Virtual Apps and Desktops Standard for Azure のライセンスと消費データを CSV にエクスポートする

追加情報

要件とセットアップ手順については、「License Usage Insights サービスの使用開始」を参照してください。

シングルテナントの顧客とマルチテナントのパートナーの集計された使用状況データを表示する方法については、「Cloud サービスのライセンス使用状況とレポート（Citrix Service Providers 向け）」を参照してください。

ライセンスコンソールを使用して、サポートされているサービスの顧客の使用状況を表示するには、次の記事を参照してください:

- Citrix Virtual Apps and Desktops サービスの顧客のライセンスと使用状況の監視
- Citrix Virtual Apps and Desktops Standard for Azure の顧客のライセンスと使用状況の監視

License Usage Insights の使用開始

September 17, 2021

サポートされるシトリックス製品

License Usage Insights サービスは、以下のシトリックス製品の使用状況に関する情報を提供します:

- Virtual Apps and Desktops（オンプレミス）製品の使用状況
- Virtual Apps Premium および Virtual Apps and Desktops Premium サービス
- Virtual Apps and Desktops Standard for Azure
- Citrix ADC VPX の割り当て

要件

シトリックスのオンプレミス製品のライセンスおよび使用状況の情報を取得するには、Citrix ライセンスサーバー 11.16.3.0 以降が必要です。Windows ベースおよび VPX ベースのライセンスサーバーのみがサポートされています。

Citrix ライセンスサーバー 11.16.3.0 以降には、Citrix Service Provider（CSP）パートナーにとって重要な主要機能が含まれています:

- 最適化された使用状況収集機能：ライセンスサーバーには、ライセンスの動作と追跡を最適化する新しい機能が追加され、CSP をさらに適切にサポートできるようになりました。
- Call Home：ライセンスサーバーには、CSP パートナーの製品使用状況収集を自動化する Call Home 機能が含まれています。これらの機能は CSP パートナーに限定されており、ライセンスサーバーで CSP ライセンスが検出された場合にのみ有効になります。

手順 **1**：**Citrix** ライセンスサーバーを更新する

バージョン 11.16.3.0 より古いライセンスサーバーを実行している場合は、License Usage Insights を使用する前にライセンスサーバーをアップグレードする必要があります。インプレースアップグレードはシンプルかつ高速です。次の手順を実行します:

1. 最新のライセンスサーバーをダウンロードします。Citrix ライセンスサーバーの最新バージョンについて詳しくは、Citrix ライセンスサーバーのドキュメントを参照してください。

2. ライセンスサーバーをアップグレードします。
3. ライセンスサーバーごとにアップグレードプロセスを繰り返します。

手順 **2**：**My Citrix** の資格情報で **Citrix Cloud** にサインインする

サインインする前に、Citrix Cloud アカウントに登録する必要があります。「Citrix Cloud への登録」で説明されている手順に従ってください。

アカウントを作成する時は、Citrix.com で Citrix ライセンスを割り当ててダウンロードするために使用した My Citrix 認証情報と同じ情報を使用してください。Citrix Cloud は、My Citrix の資格情報に関連付けられたアドレス宛てに、アカウントを確認するためのメールを送信します。

Citrix Cloud アカウントを使用する準備ができたら、メールアドレスとパスワードを使用してhttps://citrix.cloud.comにサインインします。

手順 **3**：**Citrix** ライセンスサーバーを **Citrix Cloud** に登録する

License Usage Insights でさまざまな製品のライセンスの詳細を表示するには、ライセンスサーバーを Citrix Cloud に登録します。ライセンスサーバーを Citrix Cloud に登録する方法について詳しくは、「Citrix ライセンスサーバーの登録と登録削除」を参照してください。

手順 **4**（オプション）：ライセンスサーバーによりユーザー名を匿名化する

デフォルトでは、Virtual Apps and Desktops ライセンスのチェックアウトに関連付けられたユーザー名が、安全にシトリックスに送信されます。

ユーザー名の送信によって、CSP パートナーは License Usage Insights 機能、およびトライアル、テスト、管理用に製品を使用している無料ユーザーをサポートする CSP ライセンスプログラムをフルに活用できます。

ユーザー情報は、単一の「ユーザー @ ドメイン」エントリのみです。それ以外の個人が識別可能なデータは送信されません。また、シトリックスがこの情報を共有することはありません。

ユーザー名情報のアップロードに不安を覚えるパートナーは、ユーザー名の匿名化を有効にすることができます。有効にすると、ユーザー名の匿名化機能によって、アップロード前に安全で不可逆的なアルゴリズムを使用して、読み取り可能なユーザー名が一意の文字列に変換されます。

License Usage Insights サービスは、これらの一意の識別子を使用して、実際のユーザー名の代わりに製品の使用状況を追跡します。このアプローチにより、クラウドサービスのユーザーインターフェイスに実際のユーザー名が表示されることなく、サービスプロバイダーが月ごとの情報を活用できます。

ユーザー名の匿名化を構成するには

1. ライセンスサーバーの構成ファイルをテキストエディターで開きます。通常、構成ファイルは C:\ProgramFiles\Citrix\Licensing\WebServicesForLicensing\SimpleLicenseServiceConfig.xml

にあります。

2. ［構成］セクションで、次のように **UsageBasedBillingScramble** 設定を追加します：

```
<?xml version="1.0" encoding="utf-8"?>
<Configurations>
<EncoreConfiguration>
<SamplingPeriod>15</SamplingPeriod>
<RetentionTime>180</RetentionTime>
<Enabled>true</Enabled>
</EncoreConfiguration>
<SARenewalConfigOptions>Notify</SARenewalConfigOptions>
<UsageBasedBillingScramble>1</UsageBasedBillingScramble>
</Configurations>
<!--NeedCopy-->
```

3. ファイルを保存します。

手順 **5**：**License Usage Insights** サービスを使用する

Citrix Cloud コンソールで、License Usage Insights サービスを見つけて ［管理］をクリックします。サービスの主な機能の概要については、「製品の使用状況、ライセンスサーバー、および通知の管理」を参照してください。

追加の詳細

License Usage Insights とともに Citrix ライセンスサーバーを使用する場合は、次の点を考慮してください：

- 新しく更新されたライセンスサーバーが License Usage Insights 管理コンソールに表示されるまで、最大 24 時間かかる場合があります。
- 使用状況データがライセンスサーバーからアップロードされると、安全な方法で処理および保存され、後日 License Usage Insights がそのデータにアクセスできます。この処理が完了するまで最大 24 時間かかることがあります。
- デフォルトでは、Virtual Apps and Desktops ライセンスのチェックアウトに関連付けられたユーザー名が、安全にシトリックスに送信されます。
- ユーザー名の送信によって、CSP パートナーは License Usage Insights 機能、およびトライアル、テスト、管理用に製品を使用している無料ユーザーをサポートする CSP ライセンスプログラムをフルに活用できます。
- ユーザー情報は、単一の「ユーザー @ ドメイン」エントリのみです。それ以外の個人が識別可能なデータは送信されません。また、シトリックスがこの情報を共有することはありません。

ヘルプとサポート

License Usage Insights についてサポートが必要な場合は、My Supportポータルでサポートチケットを開いてください。Citrix Cloud から My Support にアクセスするには：

1. Citrix Cloud にサインインします。
2. 画面の右上にある ［ヘルプ］アイコンをクリックします。
3. ［チケットを開く］を選択します。
4. ［**My Support** に移動］を選択し、My Citrix 資格情報でサインインします。
5. フォームに記入して送信します。

シトリックステクニカルサポートのメンバーが対応、サポートします。

よくある質問

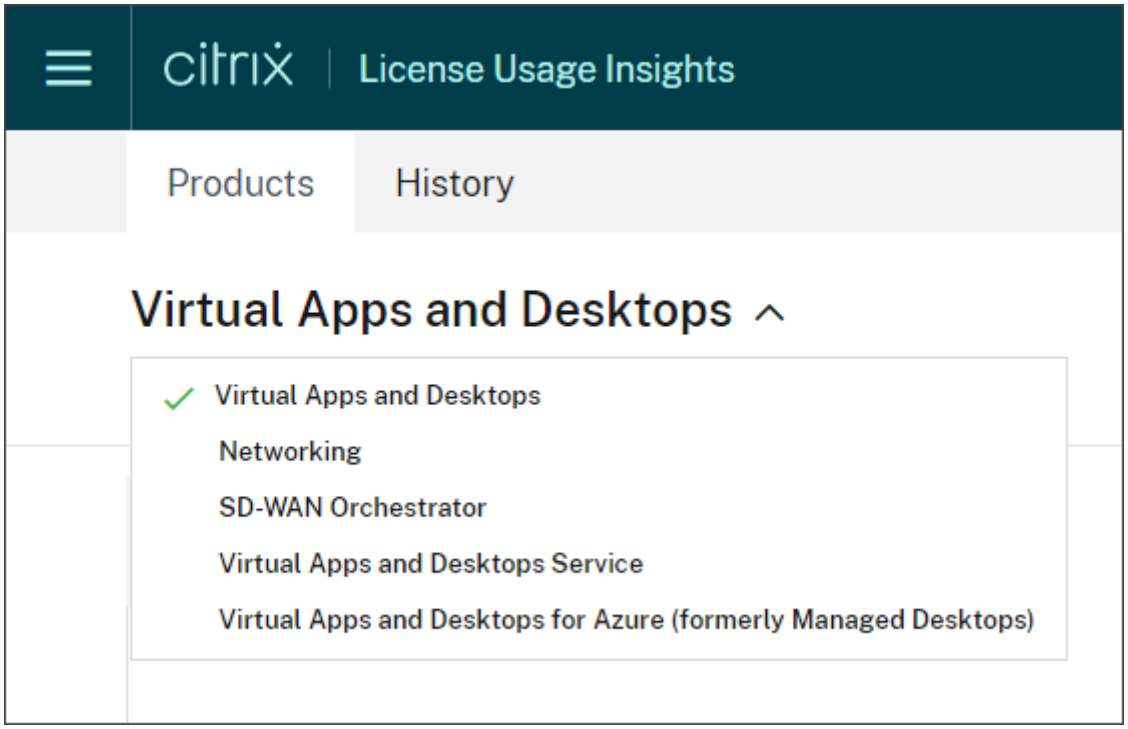
- どのような情報が送信されますか**?** ライセンスサーバーがシトリックスに送信している情報を表示できますか**?** はい。シトリックスに送信された情報のコピーを表示できます。詳しくは、「アップロードに含まれるライセンスサーバー情報」を参照してください。
- **Citrix Service Provider** ではないシトリックスの顧客やパートナーは、**License Usage Insights** を利用できますか? いいえ。License Usage Insights を利用できるのは、パートナー契約がアクティブな Citrix Service Provider パートナーのみです。
- ライセンスサーバーで **Call Home** を無効にできますか? いいえ。Citrix Service Provider のライセンス契約の下では、すべてのライセンスサーバーが製品使用状況に関する情報を送信する必要があります。情報送信機能の使用に不安を覚えるパートナーは、ユーザー名の匿名化機能を使用できます。詳しくは、「ライセンスサーバーによるユーザー名の匿名化」を参照してください。
- 請求は **License Usage Insights** に表示される製品の使用状況に基づくものですか? いいえ。License Usage Insights はパートナーが製品使用状況を把握し、シトリックスディストリビューターに迅速かつ正確に報告するための機能です。Citrix Service Provider（CSP）パートナーへの請求は、これまで同様パートナーからシトリックスディストリビューターに報告する製品使用状況に基づきます。シトリックスディストリビューターと CSP パートナーとの請求関係に変更はありません。

製品の使用状況、ライセンスサーバー、通知の管理

September 17, 2021

製品の選択

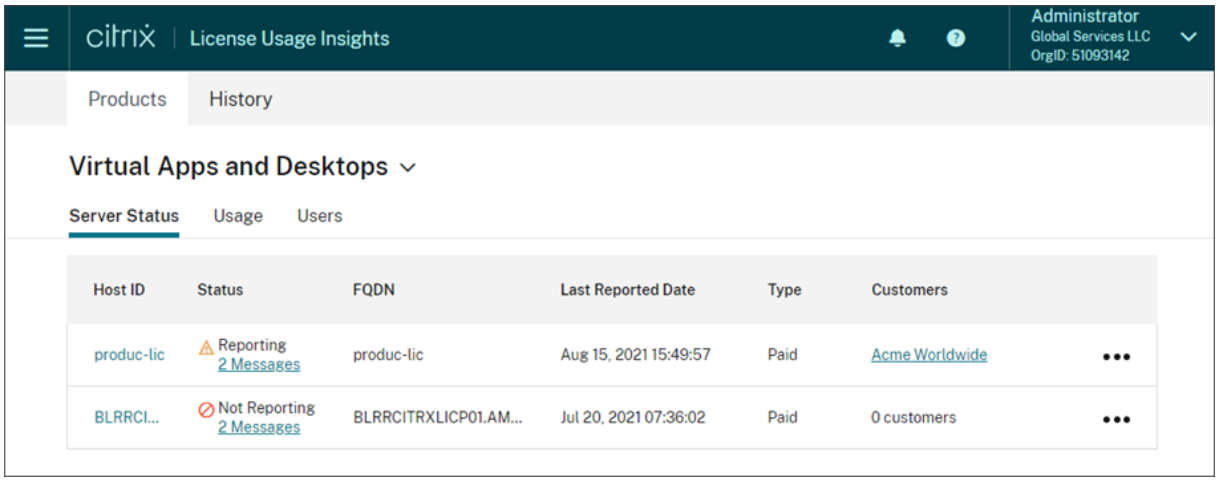
別の製品のライセンスの詳細を表示するには、製品名の横にある矢印をクリックし、表示する製品またはサービスを選択します。



ライセンスサーバーの状態

Citrix Service Provider のライセンスガイドラインに準拠するには、アクティブなライセンスサーバーをすべて更新して報告する必要があります。ライセンスサーバーの状態として、所有しているライセンスサーバーと、License Usage Insights で使用するために更新されているかどうかの情報が表示されます。

このサービスでは、シトリックスのバックオフィスに格納されているライセンス割り当てデータを使用して、アクティブなライセンスサーバー一覧を表示します。ライセンスサーバーが更新され、正常に報告が行われている場合、License Usage Insights は「報告」の状態を、最新のアップロード時刻とともに表示します。



アップロードに含まれるライセンスサーバー情報

Call Home がライセンスサーバー上でアクティブになると、次の情報が毎日アップロードされます:

- ライセンスサーバーのバージョン
- ライセンスファイル情報:
  - サーバーにインストールされているライセンスファイル
  - ライセンスファイルの有効期限
  - 製品機能およびエディションの使用権情報
  - ライセンス数量
- ライセンス使用状況:
  - 現在の暦月に使用されたライセンス
  - ライセンスのチェックアウトに関連付けられたユーザー名
  - アクティブ化された製品の機能とエディション

ライセンスサーバーのアップロードを表示する

CSP パートナーは、ライセンスサーバー上に最後にアップロードされたペイロードを検査して、ライセンスサーバーがシトリックスに送信する情報の詳細を完全に把握することができます。このペイロードのコピーは、ライセンスサーバー上に.zip ファイルとして保存されます。デフォルトでは、保存場所は C:\Program Files (x86)\Citrix\Licensing\LS\resource\usage\upload_1456166761.zip です。

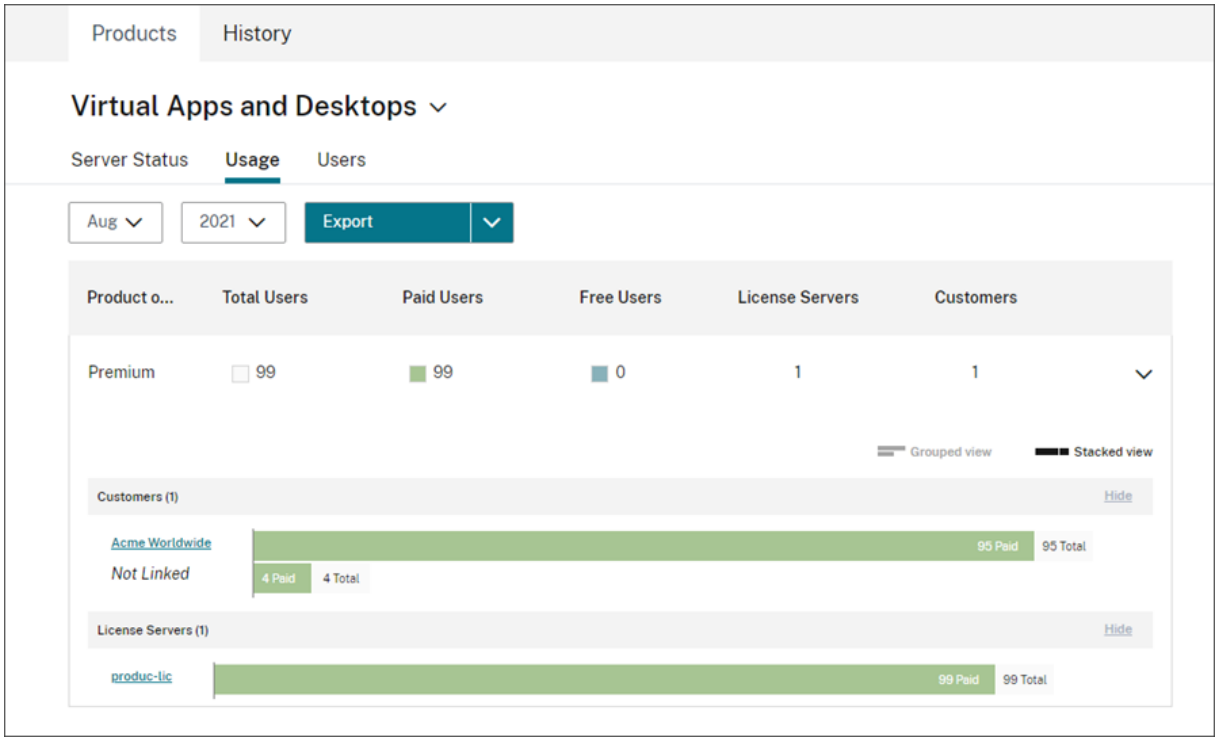
> 注:
>
> 成功したアップロードは最新のものを除いて削除されます。アップロードが成功するまで、失敗したアップロードはディスクに残ります。この場合、最新のアップロード以外すべてが削除されます。

使用状況収集

使用状況収集機能は、自動化されたデータ収集および集計によって製品の使用状況を把握するために役立ちます。追加のツールを展開する必要はありません。

License Usage Insights では、すべての Citrix ライセンスサーバーの製品使用状況を自動的に集計して表示するため、すべての環境の使用状況を完全に把握できます。特定のユーザーを所属する顧客またはテナントに関連付けることによって、ライセンス使用状況の内訳を作成することもできます。

ライセンスサーバーは、製品ライセンスの使用状況を収集して追跡し、安全な送信チャネルを使用してシトリックスに報告します。この自動化されたアプローチでは、更新された使用状況データが常に提供されるため、時間を節約でき、パートナーが展開環境内の使用傾向をより適切に理解できるようになります。



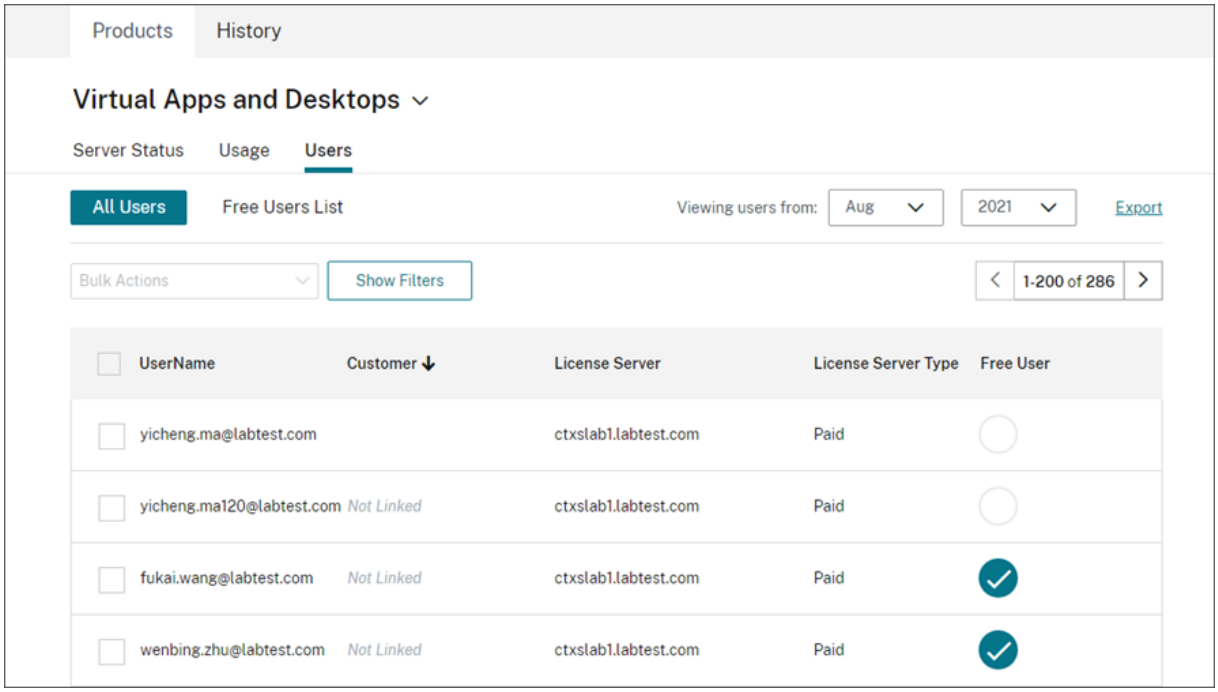
Virtual Apps and Desktops 製品使用状況の顧客内訳の作成

顧客ごとのライセンス使用状況内訳を作成するには、最初にユーザーを所属する顧客またはテナントに関連付ける必要があります。顧客ダッシュボードに顧客が定義されていない場合は、新しい顧客を追加したり、既存の Citrix Cloud 顧客に接続することができます。

1. 必要な場合は、［顧客］ダッシュボードに顧客を追加します：Citrix Cloud 管理コンソールのホームページで［顧客］を選択し、［追加または招待］をクリックして、画面の指示に従います。
2. メニューボタンをクリックし、［マイサービス］**>**［**License Usage Insights**］の順に選択します。
3. ［**Virtual Apps and Desktops**］製品を選択した状態で、［ユーザー］をクリックします。
4. 関連付けるユーザーを選択し、［一括操作］**>**［顧客へのリンクを管理］の順にクリックします。
5. 一覧から、ユーザーを関連付ける顧客を選択します。
6. ［保存］をクリックします。
7. 顧客ごとの内訳を表示するには、［使用状況］タブをクリックします。

無料ユーザー管理

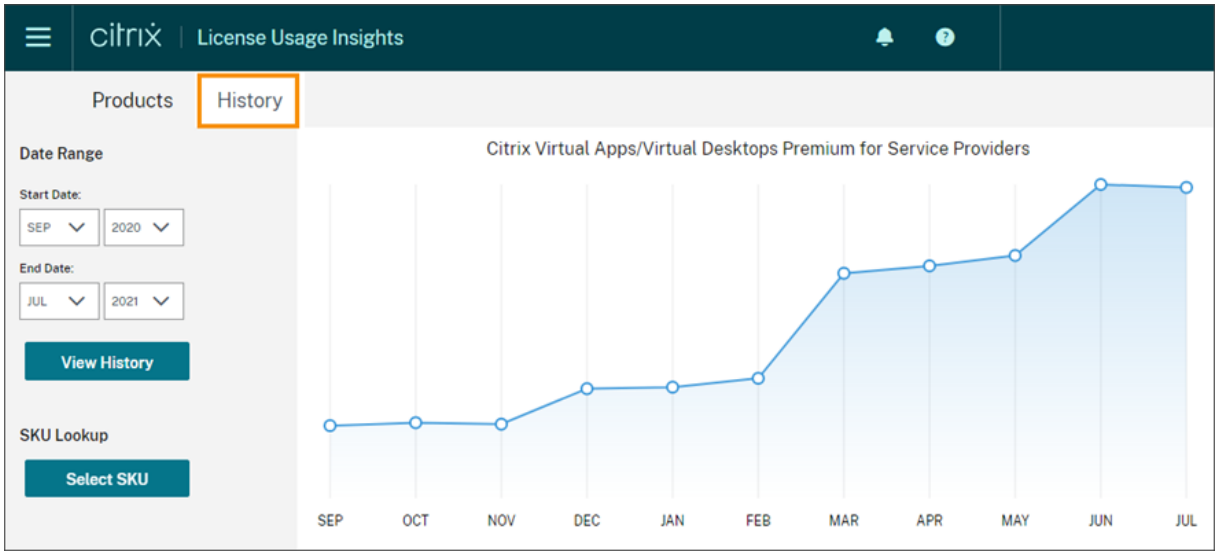
License Usage Insights では、トライアル、テスト、管理の各ユーザーをサポートする Citrix Service Provider ライセンスプログラムを最大限に活用しながら、すべての環境の製品使用状況を包括的に把握できます。



履歴傾向

シトリックスとの過去のビジネスに関する完全な履歴を表示できます。先月、昨年、または設定可能な期間にわたって報告された使用状況を確認します。

履歴表示はビジネスに関する価値ある情報を提供します。Citrix Service Provider は、シトリックスとのビジネス実績の推移や、顧客および利用者全体でどの製品が最も高い成長率を示しているかをすばやく把握できます。



使用状況と割り当てデータのエクスポート

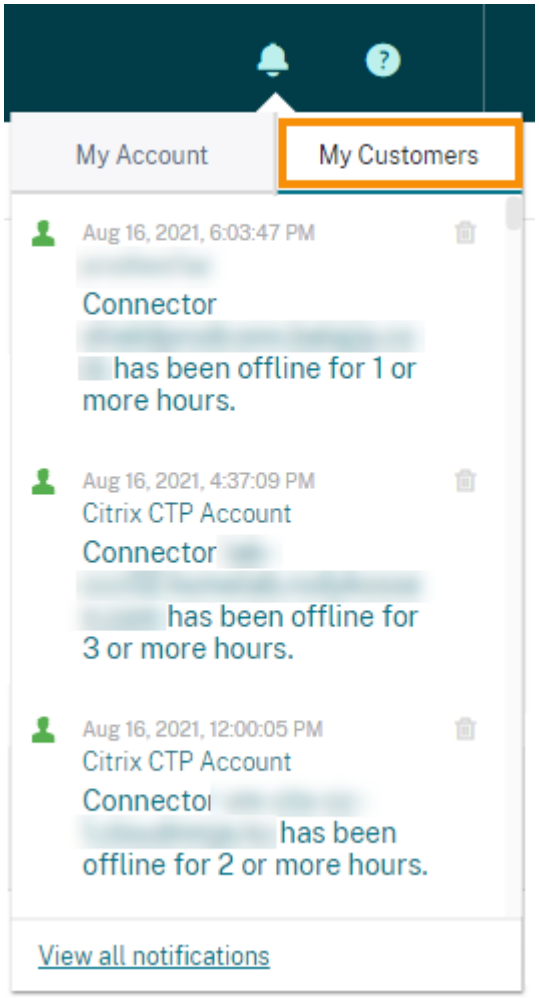
License Usage Insights から、次の種類のデータを CSV ファイルとしてエクスポートできます:

- 指定した月の Virtual Apps and Desktops 製品の使用状況とユーザー一覧
- 現在の ADC VPX 割り当ての詳細

1. 製品の一覧から、[**Virtual Apps and Desktops**] または ［ネットワーク］を選択します。
2. 該当する場合は、エクスポートするタブを選択します。たとえば、Virtual Apps and Desktops の使用状況の詳細をエクスポートするには、［使用状況］タブをクリックします。
3. 該当する場合は、エクスポートする月と年を選択します。
4. 画面右側の ［エクスポート］をクリックします。

顧客通知の表示

Citrix Cloud を使用すると、各展開環境に個別にアクセスすることなく、複数の顧客が使用するソリューションの正常性を監視できます。Citrix Cloud の通知領域は、ダッシュボード上の顧客に関する通知が集約されるため、アラートが確実に対応され、サービスが中断なく実行されるようにすることができます。

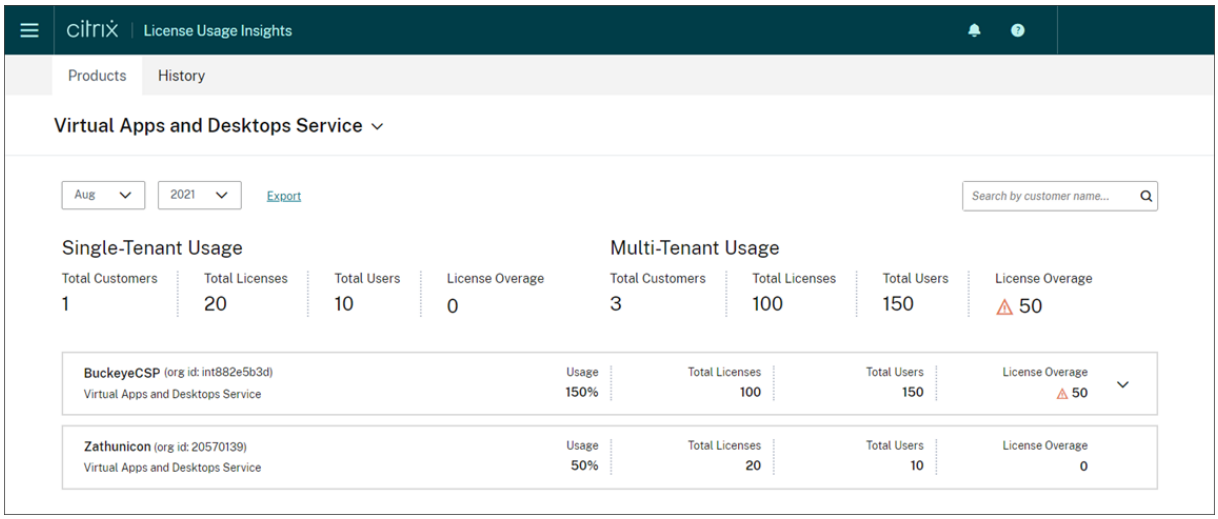


1. Citrix Cloud 管理コンソールで ［通知］アイコンをクリックし、［マイ顧客］をクリックします。最新の通知一覧が表示されます。
2. 顧客通知の全一覧を表示するには、［すべての通知を表示］をクリックします。

Cloud サービスのライセンス使用状況とレポート（**Citrix Service Providers** 向け）

September 17, 2021

License Usage Insights では、クラウドサービスの使用状況が自動的に集計され、すべてのシングルテナントの顧客とマルチテナントのパートナーの全体を把握することができます。より詳しい分析のために、特定の月の詳細データを CSV ファイルとしてエクスポートすることもできます。



サポートされるサービス

シングルテナントのライセンス使用状況は、次のサービス向けに利用できます:

- Virtual Apps Premium
- Virtual Apps and Desktops Premium

マルチテナントのライセンス使用状況は、次のサービス向けに利用できます:

- Virtual Apps and Desktops
- Virtual Apps and Desktops Standard for Azure

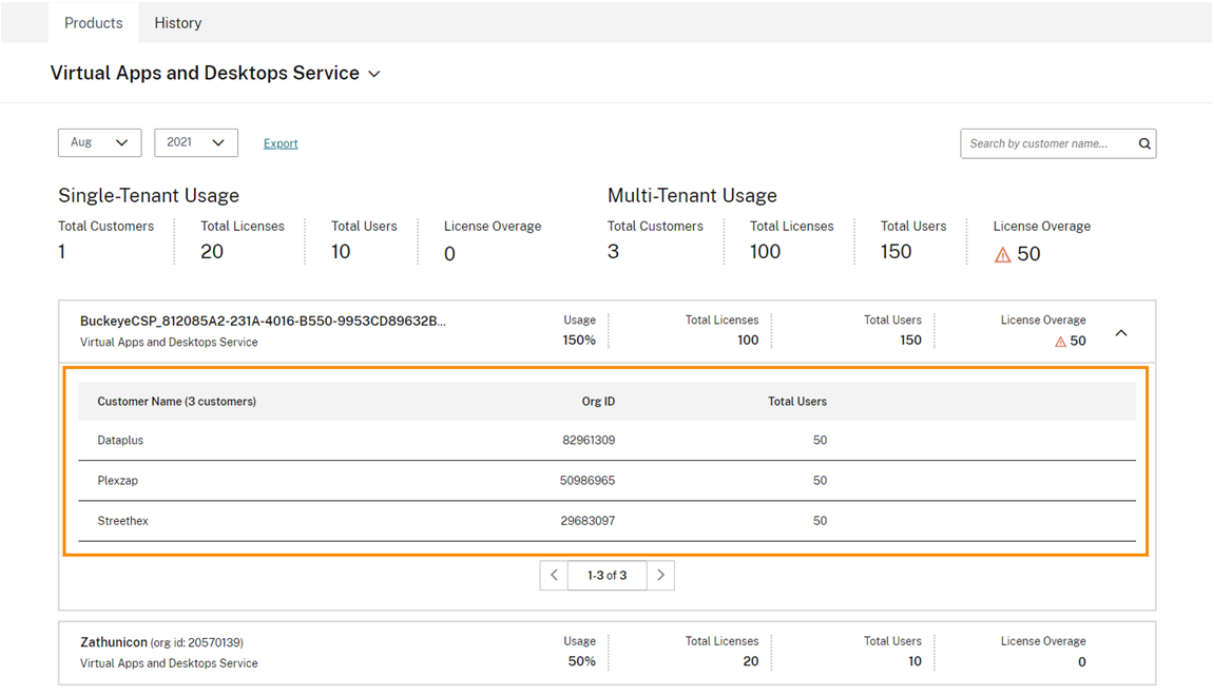
ライセンスの概要

License Usage Insights は、シングルテナントとマルチテナントの使用状況について、次の内訳を提供します:

- 顧客の総数、すべての顧客の購入済みライセンス、ユーザー、および割り当て超過ライセンスの総数など、テナントの種類ごとにグループ化された一目でわかる概要。

- 使用中のライセンスの合計、購入済みライセンスの合計、ユーザー、および割り当て超過ライセンス数のパーセンテージなど、各顧客またはパートナーの使用状況の概要。

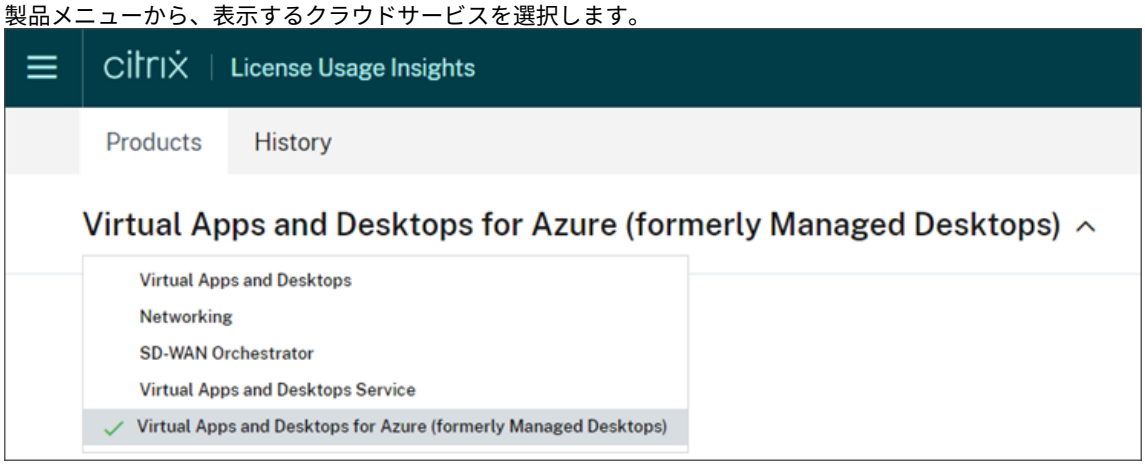
マルチテナントサービスの場合、使用状況の概要を開いて、各パートナーに関連付けられている顧客、組織 ID、および総ユーザーを表示できます。



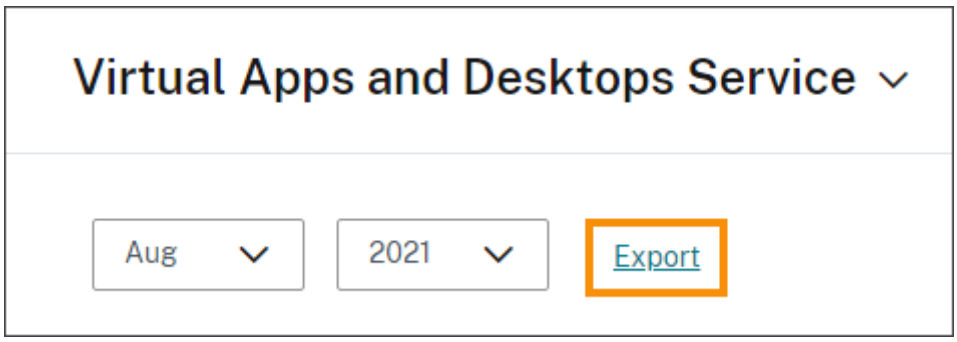
毎月の使用状況の表示およびエクスポート

すべての顧客とパートナーの前月のライセンス使用状況をいつでも表示できます。このデータを CSV ファイルとしてエクスポートして、より詳しい分析ができます。Virtual Apps and Desktops Standard for Azure の場合、毎月の消費データをエクスポートすることもできます。

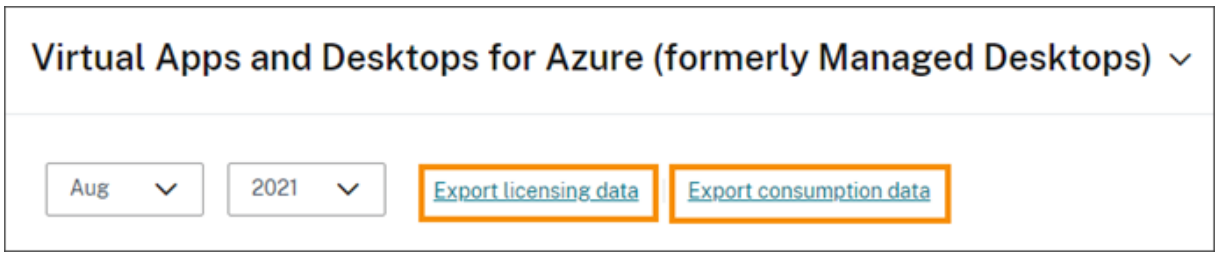
1. 製品メニューから、表示するクラウドサービスを選択します。



Virtual Apps and Desktops サービスの場合、表示する月と年を選択し、［エクスポート］を選択します。



Virtual Apps and Desktops Standard for Azure の場合、表示する月と年を選択してから、［ライセンスデータのエクスポート］または ［消費データのエクスポート］を選択します。

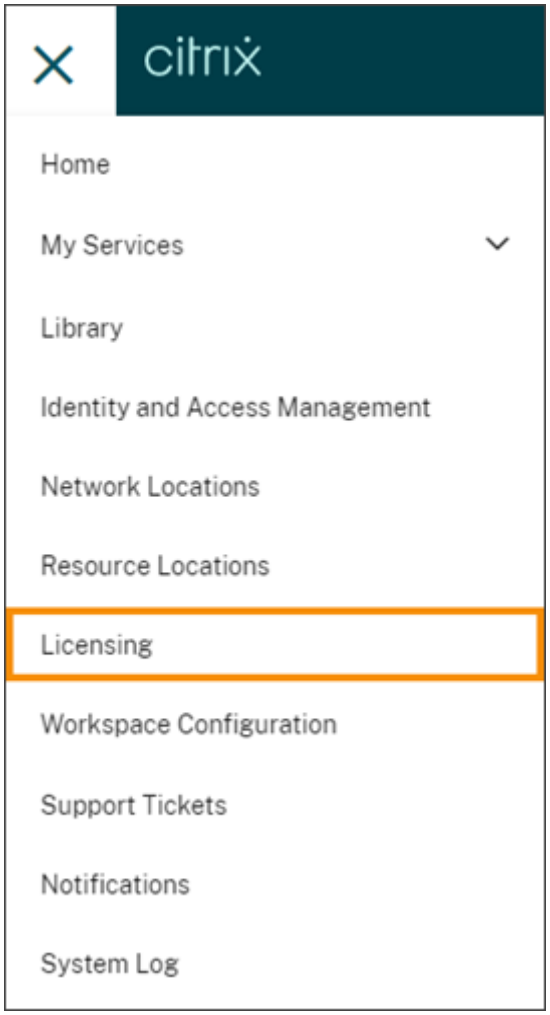


Citrix Virtual Apps and Desktops サービスの顧客のライセンスと使用状況の監視

September 17, 2021

Citrix Service Providers（**CSP**）の顧客は、Citrix Cloud で、ユーザーの Virtual Apps and Desktops サービスライセンスを簡単に監視できます。CSP の顧客として、Citrix Cloud でご自身のアカウントにサインインすることにより、詳細情報にアクセスできます。シングルテナントとマルチテナントの顧客について集計されたライセンス使用状況データを表示する方法については、「Cloud サービスのライセンス使用状況とレポート（Citrix Service Providers 向け）」を参照してください。

顧客は、Citrix Cloud メニューで ［ライセンス］を選択することで、ライセンスデータを表示できます。



ライセンス割り当て

Citrix Cloud は、一意のカスタマーユーザーがアプリまたはデスクトップをその月で初めて起動したときに、ライセンスを割り当てます。

ライセンスの概要

［クラウドサービス］タブのライセンスの概要で、次の情報を一目で確認できます：

- 購入済みライセンス合計に対する割り当て済みライセンスの割合。割合が 100% に近づくにつれて、表示は緑色から黄色に変わります。割合が 100% を超えると、表示が赤になります。
- 購入したライセンスに対する割り当てられたライセンスの比率、および使用可能なライセンスの残りの数。
- 割り当て超過ライセンスの数（割り当て超過がある場合）。割り当て済みライセンスの数が購入済みライセンスの総数を超えると、アラートメッセージが表示されます。

使用状況の傾向とライセンスアクティビティ

ライセンス概要の右端にある ［使用状況の詳細の表示］を選択すると、ライセンスの詳細ビューが表示されます。

［使用状況の傾向］セクションには次の情報の内訳が表示されます：

- ライセンス合計：合計したクラウドサービス使用権のために購入済みのライセンス合計数。
- 割り当てられたユーザー：各月にカスタマーユーザーに割り当てられたライセンスの累積数。
- 割り当て超過ユーザー：購入済みライセンスの合計を超えて、各月に割り当てられたライセンスの数。

［ライセンスアクティビティ］セクションには、当月中にライセンスが割り当てられた個別のカスタマーユーザーの一覧が表示されます。この一覧には、各ユーザーが属するドメイン、ライセンスが割り当てられた日付、およびサービスが最後に使用された日時も表示されます。

ライセンスの毎月の解放

毎月 1 日に、前月の割り当て済みライセンスが自動的に解放されます。解放が行われると、割り当てられたライセンスの数が 0 にリセットされ、ライセンスを割り当てられたカスタマーユーザーの一覧がクリアされます。ユーザーが新しい月に初めてアプリまたはデスクトップを起動したときに、ライセンスが再割り当てされます。

毎月のライセンス履歴の確認

毎月 1 日に、割り当て済みライセンスの数が 0 にリセットされると、前月にライセンスを割り当てられたカスタマーユーザーの一覧（[ライセンスアクティビティ］の下にあります）がクリアされます。ただし、必要に応じていつでも、前月のユーザーの詳細にアクセスして、CSV ファイルとしてダウンロードできます。

1. ［ライセンスアクティビティ］セクションで、セクションの右端にある ［ライセンス履歴を表示］を選択します。
2. 表示する月を選択します。選択した月のユーザー詳細一覧が表示されます。
3. 一覧をエクスポートするには、セクションの右端にある ［**CSV** にエクスポート］を選択して、ファイルを保存します。

ライセンス詳細のエクスポート

詳細な分析のために、顧客はいつでも、ライセンスを割り当てられたユーザーの詳細を CSV ファイルにエクスポートできます。その後、必要に応じて CSV ファイルを使用して、ライセンスの詳細を分析できます。

当月の詳細をエクスポートするには、［ライセンスアクティビティ］セクションの右端にある ［**CSV** にエクスポート］を選択して、ファイルを保存します。

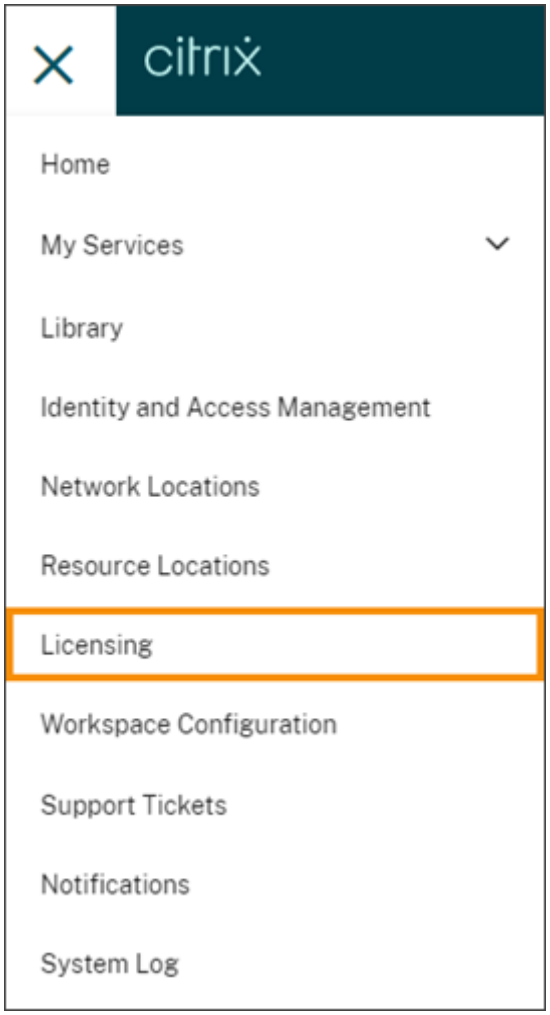
前月の詳細をエクスポートするには、「毎月のライセンス履歴の確認」の説明に従って、選択した月の一覧を生成します。［**CSV** にエクスポート］を選択してファイルを保存します。

Citrix Virtual Apps and Desktops Standard for Azure の顧客のライセンスと使用状況の監視

September 17, 2021

Citrix Service Providers（**CSP**）の顧客は、Citrix Cloud で、ユーザーの Virtual Apps and Desktops Standard for Azure ライセンスを簡単に監視できます。CSP の顧客として、Citrix Cloud でご自身のアカウントにサインインすることにより、詳細情報にアクセスできます。シングルテナントとマルチテナントの顧客について集計されたライセンス使用状況データを表示する方法については、「Cloud サービスのライセンス使用状況とレポート（Citrix Service Providers 向け）」を参照してください。

顧客は、Citrix Cloud メニューで ［ライセンス］を選択することで、ライセンスデータを表示できます。



ライセンス割り当て

Citrix Cloud では、一意のユーザーによるデスクトップの初回起動時にライセンスが割り当てられます。

ライセンスの概要

［クラウドサービス］タブのライセンスの概要で、次の情報を一目で確認できます：

- 購入済みライセンス合計に対する割り当て済みライセンスの割合。割合が 100% に近づくにつれて、表示は緑色から黄色に変わります。割合が 100% を超えると、表示が赤になります。
- 購入したライセンスに対する割り当てられたライセンスの比率、および使用可能なライセンスの残りの数。
- 割り当て超過ライセンスの数（割り当て超過がある場合）。割り当て済みライセンスの数が購入済みライセンスの総数を超えると、アラートメッセージが表示されます。

概要の右端にある ［使用状況の詳細の表示］をクリックして、使用状況レポートおよび傾向の内訳と、Citrix Virtual Apps and Desktops Standard for Azure ライセンスを消費しているユーザーの一覧を表示できます。

使用状況レポート

使用状況の情報を標準の間隔、または指定の間隔でダウンロードできます。
情報には、次の項目に関するメーターの使用量が含まれます：

- Azure 仮想マシン
- ネットワーク接続（VNet ピアリングなど）
- Managed Disks、ブロック BLOB、ページ BLOB のような Azure ストレージの項目

すべての使用状況がデータに反映されるまで 1 日または 1 月の終わりから最大 72 時間を要することがあります。

［使用状況レポート］で、期間を選択し、［データのダウンロード］を選択して、CSV ファイルをローカルマシンにダウンロードします。

使用状況の傾向とライセンスアクティビティ

管理コンソールの ［使用状況の傾向］セクションには、次の情報の内訳が表示されます：

- ライセンス合計：合計したクラウドサービス使用権のために購入済みのライセンス合計数。
- 割り当てられたユーザー：各月にカスタマーユーザーに割り当てられたライセンスの累積数。
- 割り当て超過ユーザー：購入済みライセンスの合計を超えて、各月に割り当てられたライセンスの数。

特定の月のグラフ上のバーをポイントすると、ライセンス、割り当てられたライセンス、割り当てられたユーザー、および割り当て超過ライセンスの総数が表示されます。

ライセンス使用ユーザー

［ライセンスアクティビティ］セクションには、当月中にライセンスが割り当てられた個別のカスタマーユーザーの一覧が表示されます。この一覧には、各ユーザーが属するドメイン、ライセンスが割り当てられた日付、およびサービスが最後に使用された日時も表示されます。

ライセンスの毎月の解放

毎月 1 日に、前月の割り当て済みライセンスが自動的に解放されます。解放が行われると、割り当てられたライセンスの数が 0 にリセットされ、ライセンスを割り当てられたカスタマーユーザーの一覧がクリアされます。ユーザーが新しい月に初めてアプリまたはデスクトップを起動したときに、ライセンスが再割り当てされます。

毎月のライセンス履歴の確認

毎月 1 日に、割り当て済みライセンスの数が 0 にリセットされると、前月にライセンスを割り当てられたカスタマーユーザーの一覧（[ライセンスアクティビティ］の下にあります）がクリアされます。ただし、必要に応じていつでも、前月のユーザーの詳細にアクセスして、CSV ファイルとしてダウンロードできます。

1. ［ライセンスアクティビティ］セクションで、セクションの右端にある［ライセンス履歴を表示］を選択します。
2. 表示する月を選択します。選択した月のユーザー詳細一覧が表示されます。
3. 一覧をエクスポートするには、セクションの右端にある［**CSV** にエクスポート］を選択して、ファイルを保存します。

ライセンス詳細のエクスポート

詳細な分析のためにいつでも、ライセンスを割り当てられたユーザーの単一の顧客の詳細を CSV ファイルにエクスポートできます。その後、必要に応じて CSV ファイルを使用して、ライセンスの詳細を分析できます。

当月の詳細をエクスポートするには、［ライセンスアクティビティ］セクションの右端にある［**CSV** にエクスポート］を選択して、ファイルを保存します。

前月の詳細をエクスポートするには、「毎月のライセンス履歴の確認」の説明に従って、選択した月の一覧を生成します。［**CSV** にエクスポート］を選択してファイルを保存します。

Citrix Cloud 管理者を管理する

July 28, 2021

Citrix Cloud コンソールで管理者を管理します。既存の Citrix Cloud アカウントに管理者として追加する場合は、アカウントの既存の管理者が招待する必要があります。

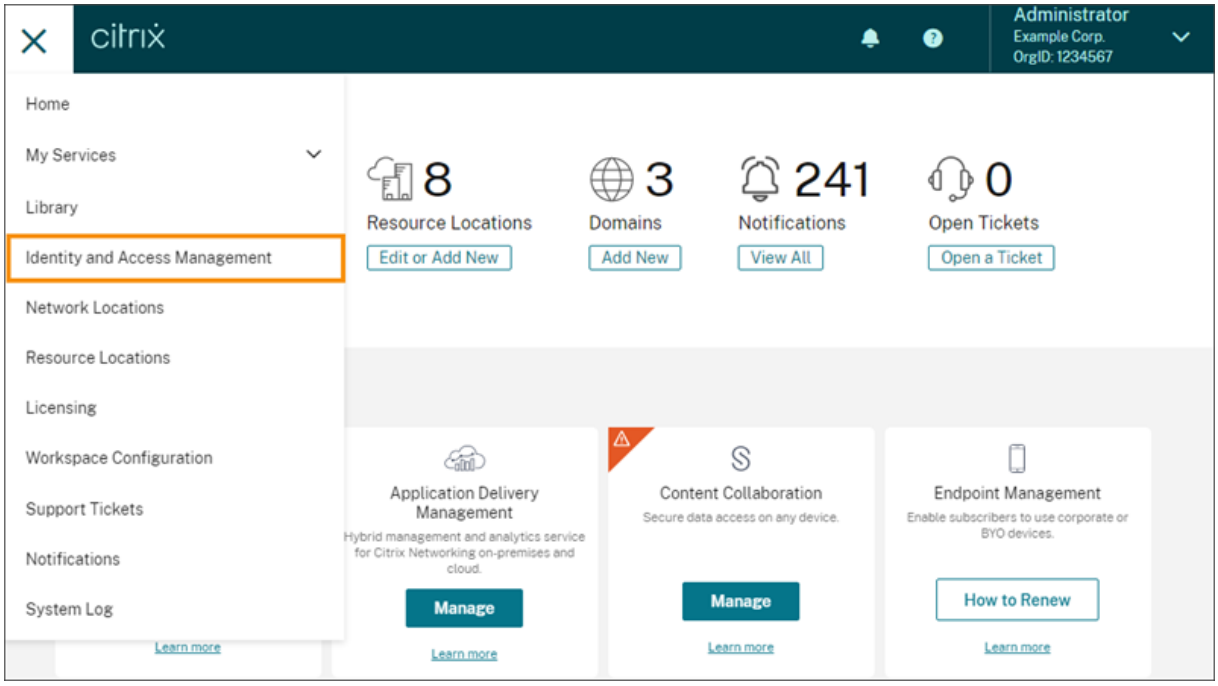
Citrix Cloud は、Citrix Cloud 管理者の認証の第 2 要素としてトークンの使用もサポートしています。管理者として追加されると、デバイスを多要素認証に登録し、Citrix SSO や Google Authenticator などの時間ベースのワンタイムパスワード標準に準拠したアプリを使用してトークンを生成できます。

> ヒント：
>
> 「Citrix Cloud の基礎」コースの「Citrix Cloud プラットフォーム」モジュールには、Citrix Cloud と各種サービスの管理方法を説明した短い動画があります。また、このコースをすべて履修すると、Citrix Cloud、組織

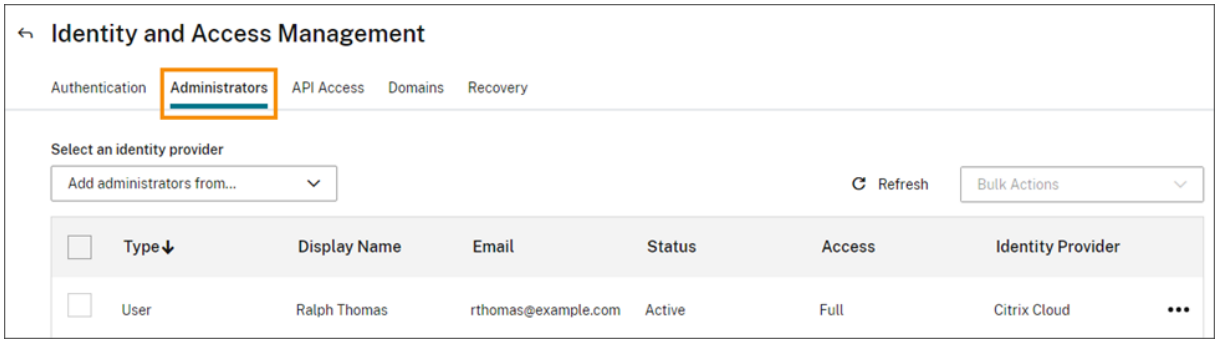
> にとってのメリット、および Citrix Cloud サービスで対処できる重要なユースケースの理解のために必要なしっかりとした基礎を身につけることができます。

新しい管理者を招待する

Citrix Cloud 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。



［**ID** およびアクセス管理］ページで ［管理者］をクリックします。アカウント内の現在の管理者がすべて一覧表示されます。



管理者を招待するには：

1. ［追加する管理者の場所］で、管理者の選択先となる ID プロバイダーを選択します。選択した ID プロバイダーによっては、まず ID プロバイダーにサインインするよう Citrix Cloud から要求されることがあります（たとえば、Azure Active Directory）。
2. **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 ［招待］をクリックします。
3. Azure Active Directory を選択した場合は、追加するユーザーの名前を入力して ［招待］をクリックします。AAD ゲストユーザーの招待はサポートされていません。

4. 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）は、すべての Citrix Cloud 機能とサブスクライブ済みサービスを制御できます。カスタムアクセスは、選択した機能とサービスを制御できます。
5. ［招待を送信する］をクリックします。

Citrix Cloud は、指定されたメールアドレスに招待状を送信し、管理者を一覧に追加します。cloud@citrix.com から送信されたメールには、アカウントへのアクセス方法が記載されています。Citrix Cloud には招待状のステータスも表示されるため、ユーザーが招待状を受け入れて Citrix Cloud にサインインしたかを確認できます。

メールを受信した管理者は、［参加］リンクをクリックして招待を承諾します。ブラウザーウィンドウが開き、パスワードを作成するページが表示されます。

> 注:
>
> 管理者が既にアカウントを持っている場合、Citrix Cloud は既存のパスワードを使用してサインインするよう指示します。招待を承諾すると、管理者はウェルカムメールを受信し、Citrix Cloud のコンソールに管理者が「アクティブ」と表示されます。

管理者権限を変更する

Citrix Cloud アカウントに管理者を追加するときは、組織内での役割に適した管理者権限を定義します。ただし、時に既存の管理者に異なるレベルのアクセス権を割り当てる必要がある場合があります。

他の管理者の権限を定義できるのは、フルアクセス権限を持つ Citrix Cloud 管理者だけです。

既存の管理者権限を変更するには:

1. Citrix Cloud（https://citrix.cloud.com）にサインインします。
2. Citrix Cloud メニューから、［**ID** およびアクセス管理］を選択し、次に ［管理者］を選択します。
3. 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。
4. 特定の権限を許可または禁止するには、［カスタムアクセス］を選択します。
5. 権限ごとに、必要に応じてチェックマークを選択またはクリアします。
6. ［変更の保存］をクリックします。

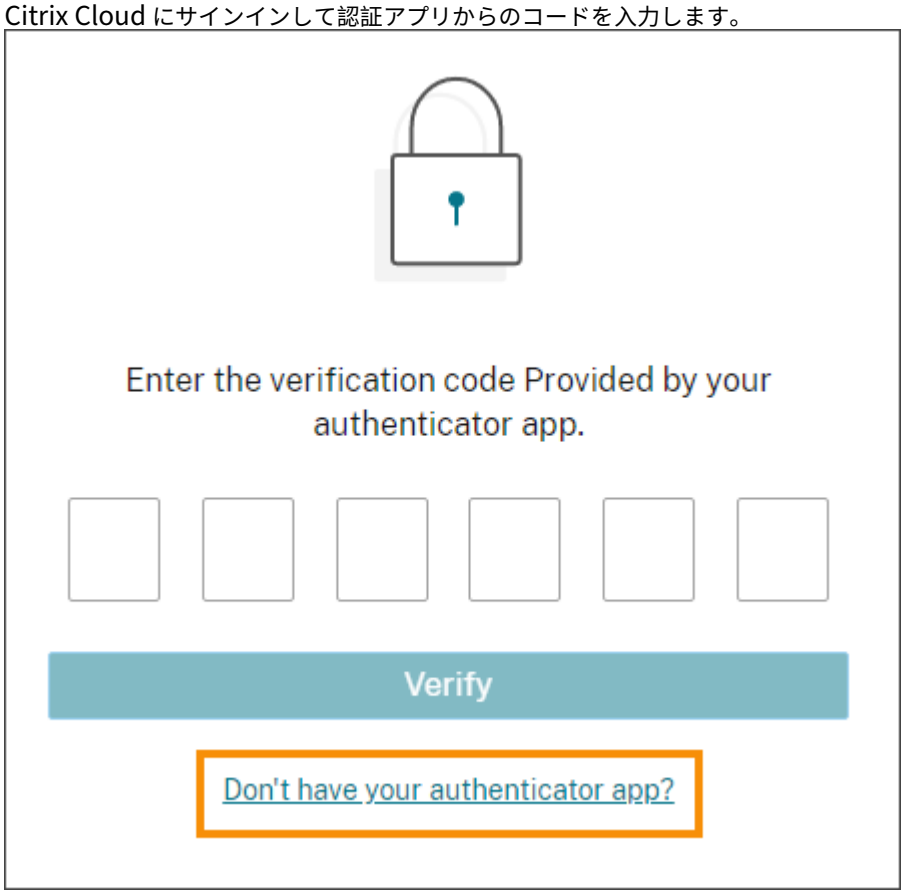
多要素認証用のデバイスを変更する

登録済みのデバイスを紛失し、Citrix Cloud で別のデバイスを使用する場合、または認証アプリをリセットする場合は、Citrix Cloud の多要素認証に再登録できます。

> メモ
>
> - 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 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 エントリが表示され、Citrix Cloud 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 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。

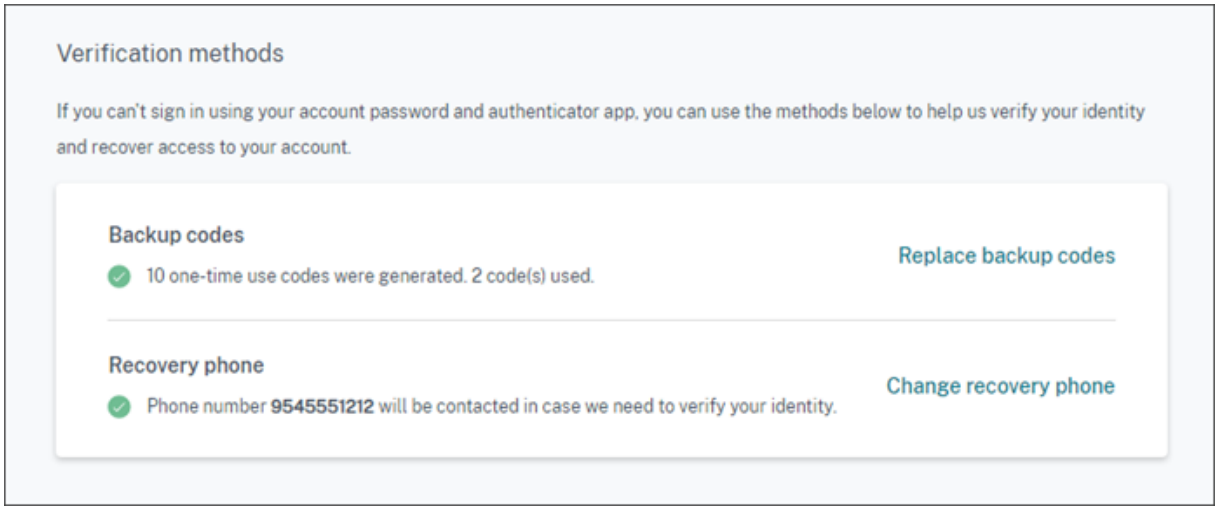
2. 複数の顧客組織の管理者である場合は、任意の組織を選択します。
3. 右上のメニューから ［マイプロファイル］を選択します。
4. ［認証アプリ］で ［デバイスの変更］を選択します。

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 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

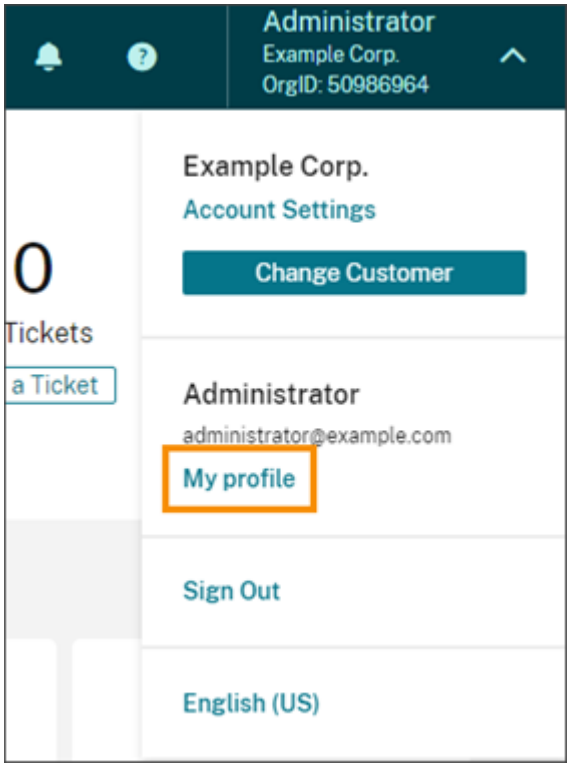
> 重要:
>
> Citrix Cloud アカウントの安全を確保するには、確認方法を最新の状態に保ち、正確な情報を使用します。認証アプリにアクセスできなくなった場合、これらの確認方法がアカウントへのアクセスを復旧する唯一の方法です。



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 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 は新しいバックアップコードのセットを生成して表示します。
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。

> 注:
>
> Citrix Endpoint Management（CEM）の管理者権限を変更できるのは、管理者が管理者への招待を受け入れ、CEM タイルで [管理] をクリックした後のみです。すべての Citrix Cloud 管理者と同様に、CEM 管理者はデフォルトでフルアクセス権限を持っています。

復旧用の電話番号を変更する

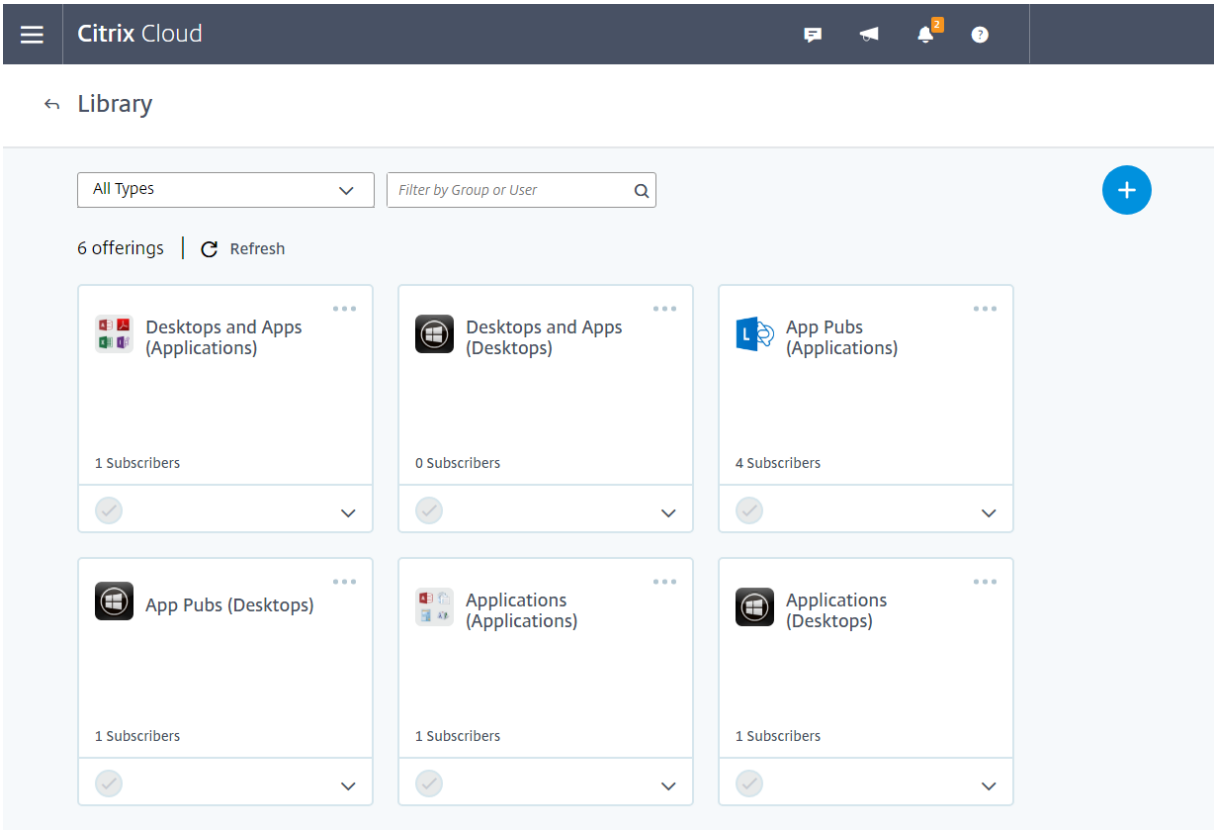
1. Citrix Cloud にサインインして認証アプリからのコードを入力します。
2. 複数の顧客組織の管理者である場合は、多要素認証で最初に登録した組織を選択します。
3. 右上のメニューから [マイプロファイル] を選択します。
4. [確認方法] の [復旧用の電話番号] で [復旧用の電話番号を変更する] を選択します。
5. 使用する新しい電話番号を入力し、[保存] を選択します。

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

February 4, 2020

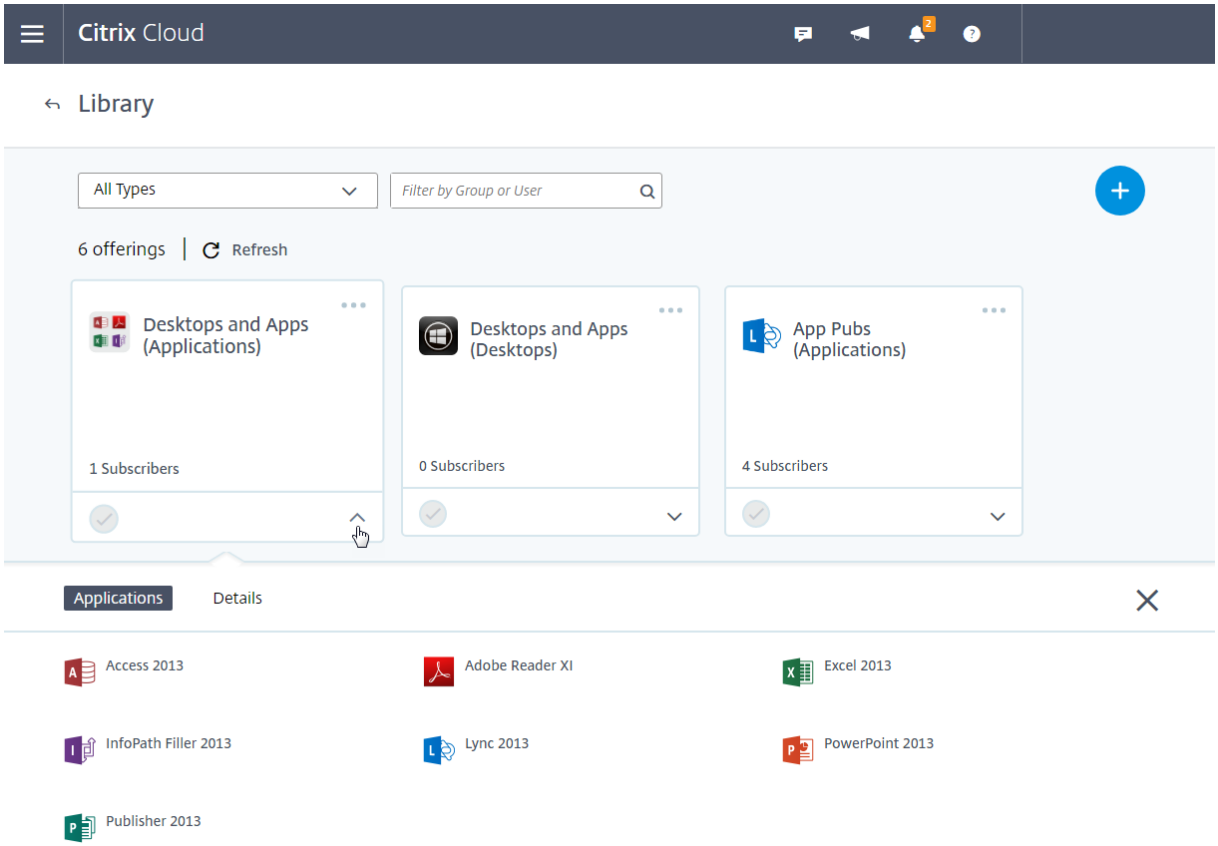
ライブラリを使用して、Active Directory のユーザーやグループに、サービスで構成しているリソースなどの項目（たとえば、Virtual Apps and Desktops サービスで構成されているアプリケーションまたはデスクトップ）を割り当てることができます。

オファリングは、Citrix サービスによって作成したアプリケーション、デスクトップ、データ共有、Web アプリケーションで構成されています。ライブラリには、すべてのオファリングが単一のビューで表示されます。



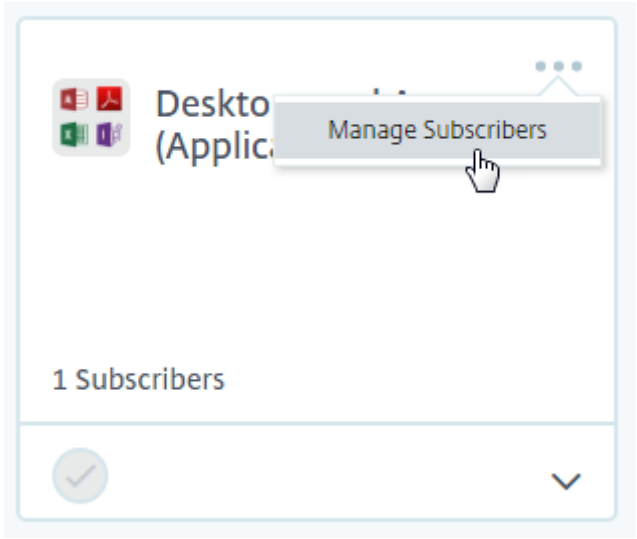
オファリングの詳細を表示する

オファリングカードで矢印ボタンをクリックすると、アプリケーション、デスクトップ、ポリシー、他のオファリング関連情報が表示されます。



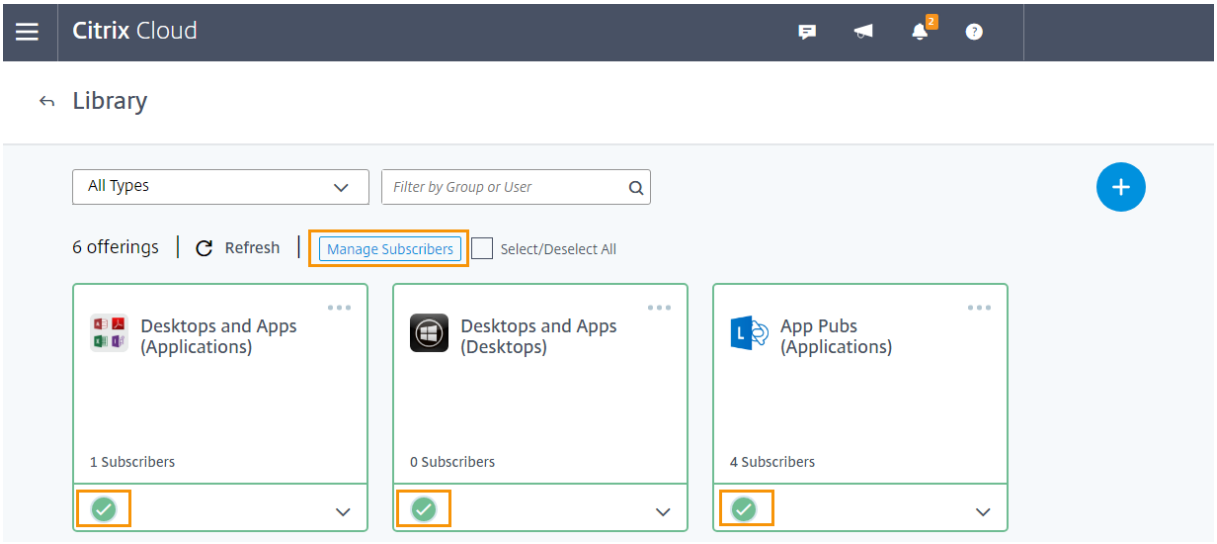
利用者を追加または削除する

単一のオファリングについてユーザーまたはグループを管理するには、オファリングカードのメニューで ［利用者を管理］をクリックします。

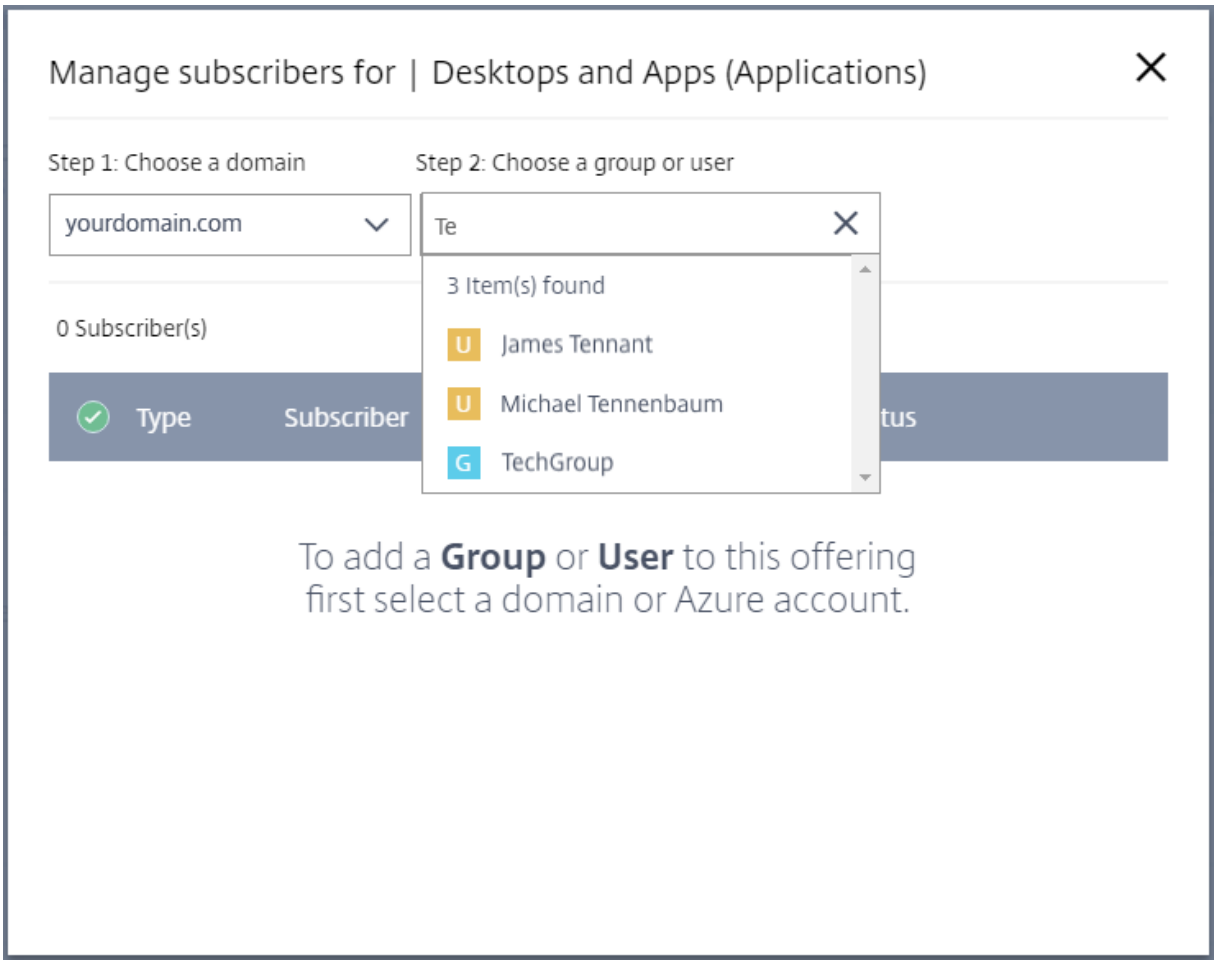


複数のオファリングについて利用者を管理するには、各オファリングのチェックマークを選択し、［利用者の管理］を

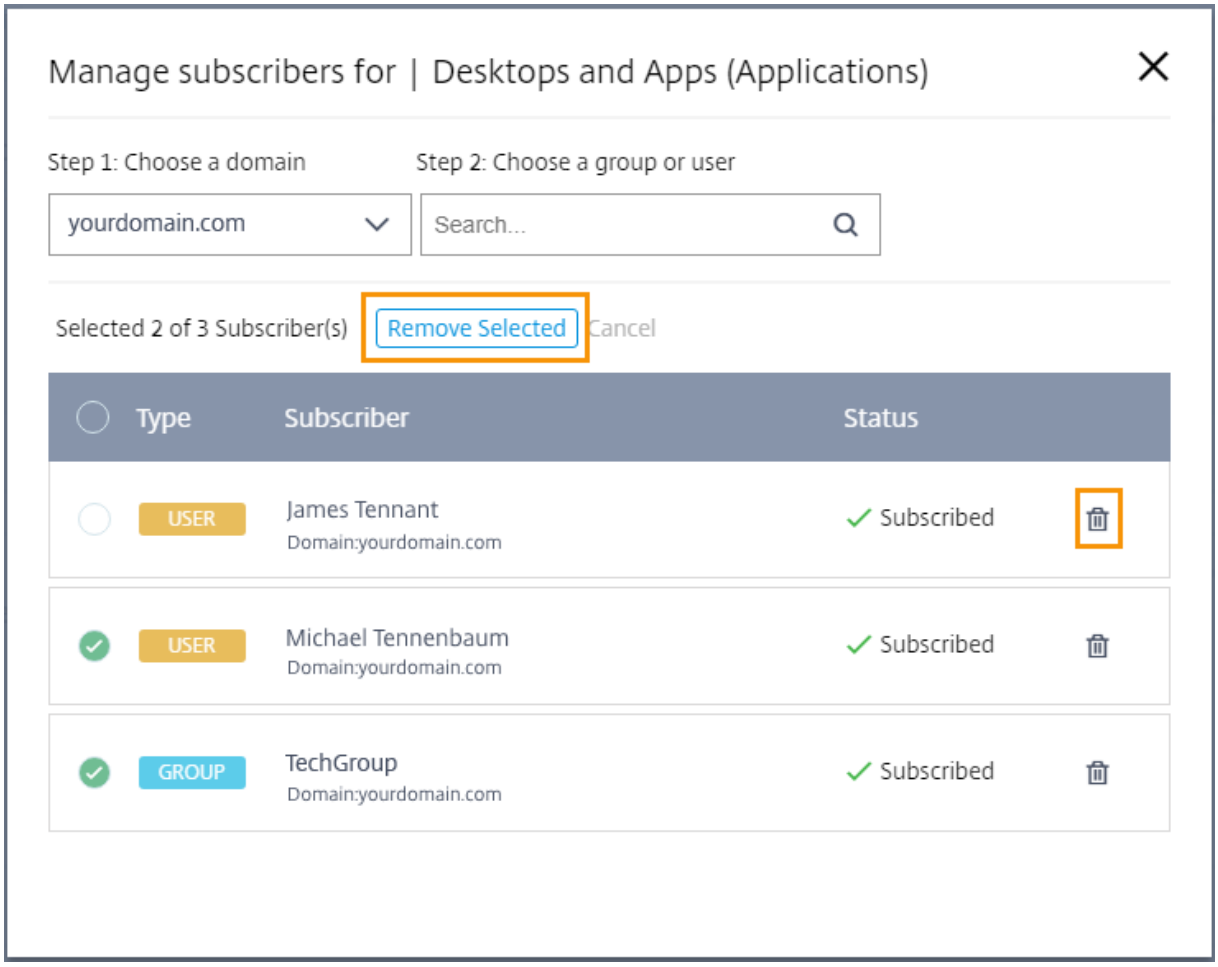
クリックします。



オファリングに利用者を追加するには、ドメインを選択して、追加するユーザーまたはグループを選択します。



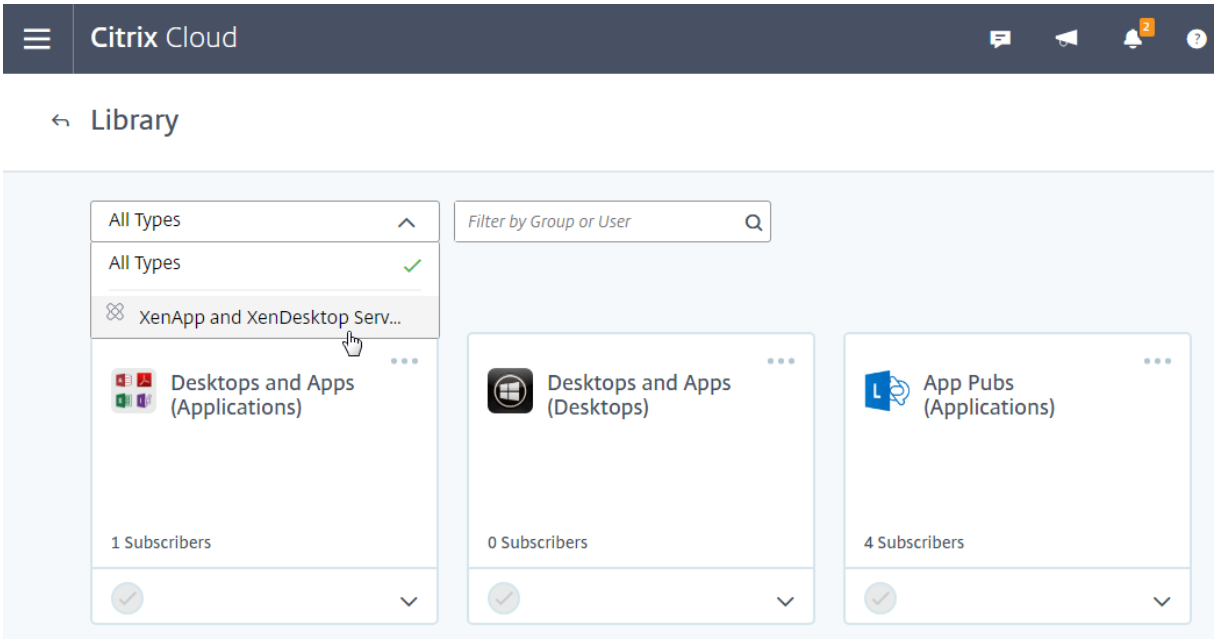
単一の利用者を削除するには、ユーザーまたはグループのごみ箱アイコンをクリックします。複数の利用者を削除するには、ユーザーまたはグループを選択し、［選択項目の削除］をクリックします。



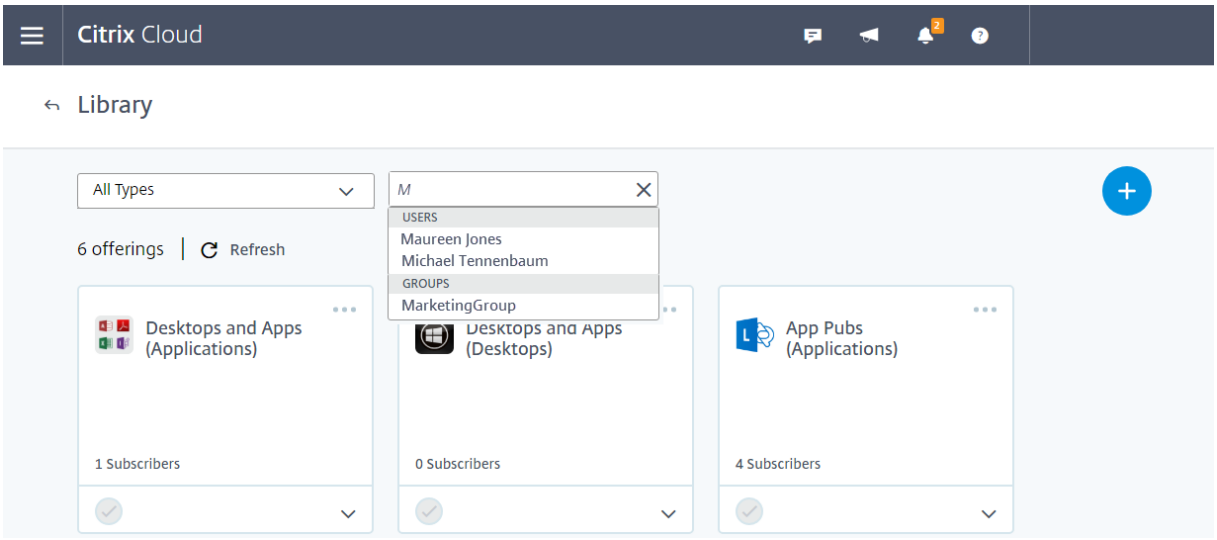
オファリングから利用者を追加または削除すると、オファリングカードには現在の利用者数が表示されます。

製品を絞り込む

デフォルトでは、ライブラリにすべてのオファリングが表示されます。特定のサービスのオファリングをすばやく表示するには、そのサービスのフィルターを選択します。



ライブラリ内のオファリングを現在利用しているすべてのユーザーまたはグループを検索できます。Citrix Cloud は、選択したユーザーまたはグループに関連するオファリングのみを表示します。すべてのユーザーのすべてのオファリングを表示するには、[X] をクリックしてフィルターをクリアします。



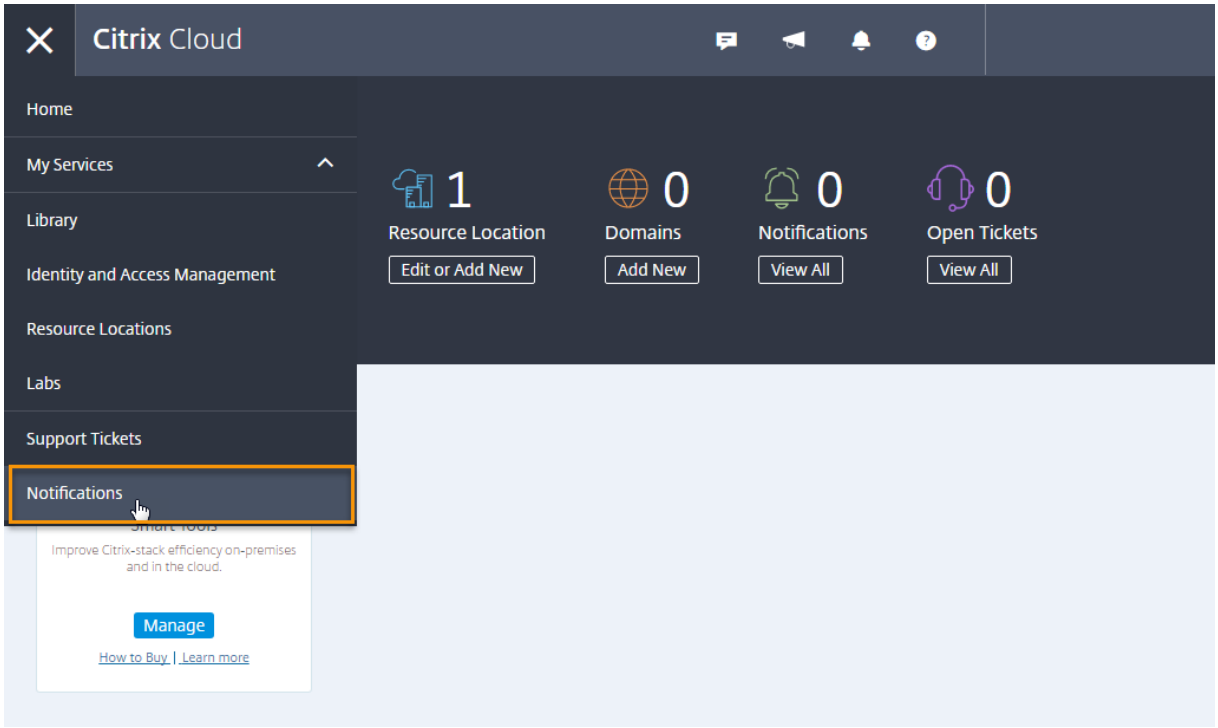
通知

November 11, 2020

通知は、Citrix Cloud 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 のすべてのサービスで使用できます。

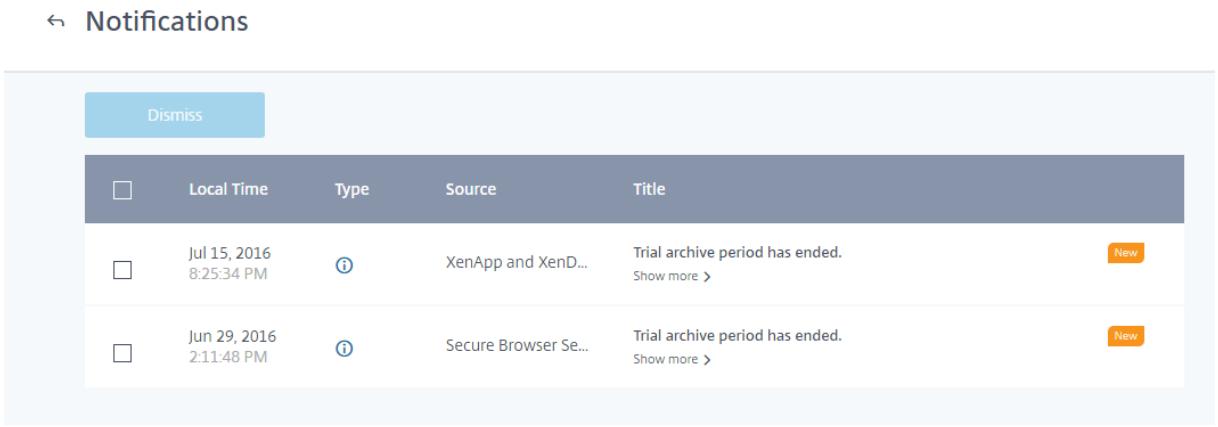
通知を表示する

通知の数は、Citrix Cloud コンソールページの上部付近に表示されます。詳しくは、コンソールの ［通知］で ［すべて表示］をクリックするか、コンソールメニューで ［通知］を選択してください。



通知を削除する

通知内容を確認し、（必要であれば）その指示どおりに処理した後、通知を選択して ［削除］をクリックします。通知を削除すると一覧から削除され、Citrix Cloud によりコンソールのホームページに戻ると通知の数が更新されます。



管理者は、Citrix Cloud で管理者宛ての通知を受信します。これによって、通知を削除しても、他の管理者は通知を表示できます。

メールで通知を受信する

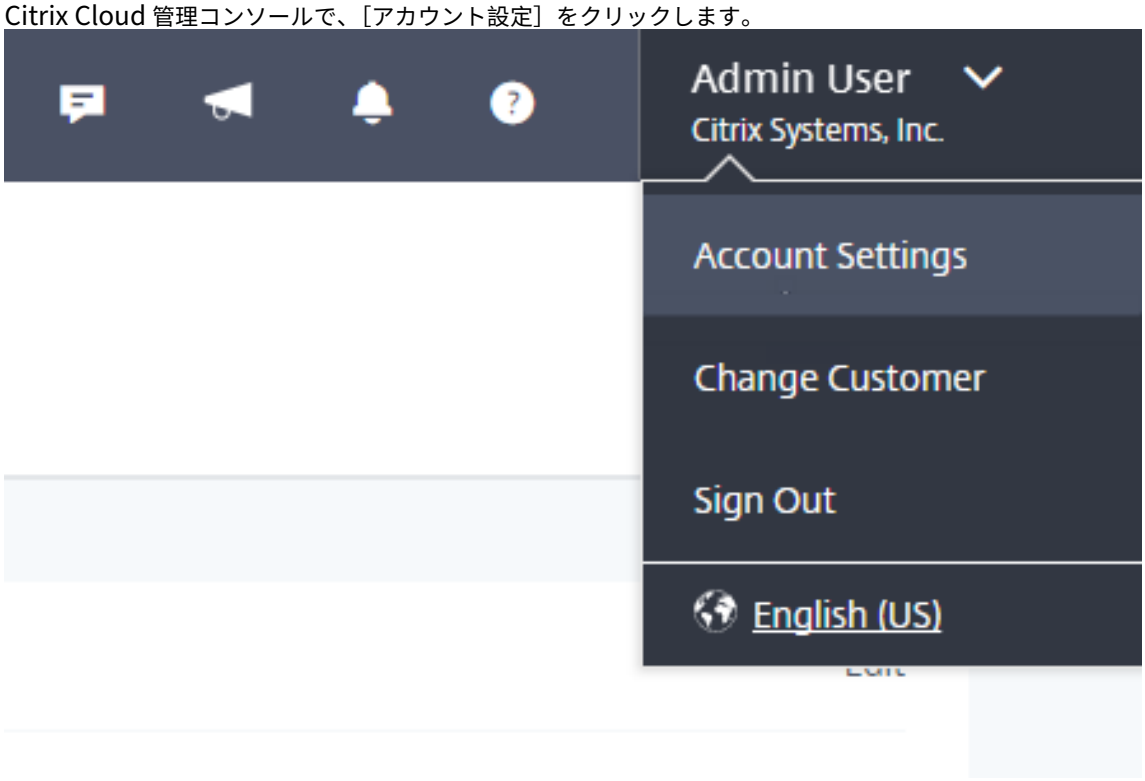
サインインする代わりにメールで通知を受信することを選択できます。デフォルトでは、メール通知は無効になっています。

メールによる通知を有効にすると、通知ごとに Citrix Cloud からメールが送信されます。通知は可能な限り早いタイミングで送信されます。1 通のメールにまとめられたり、何通かごとにまとめて後から送信されることはありません。

メールの通知を読み終えたら、Citrix Cloud の通知ページで通知を削除することができます。

メールの通知を有効にするには

1. Citrix Cloud 管理コンソールで、［アカウント設定］をクリックします。



2. ［マイプロファイル］を選択します。
3. ［メール通知］トグルボタンをクリックしてメール通知をオンにします。
4. 受信する通知を選択します。デフォルトでは、すべての通知の種類が選択されています。

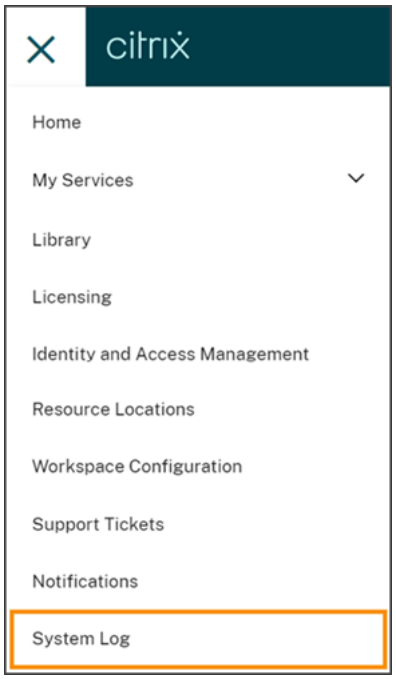
システムログ（**Technical Preview**）

September 17, 2021

> 注:
>
> システムログとSystemLog APIは Technical Preview 段階にあります。Citrix ではこれらの機能を非実稼働環境でのみ使用することをお勧めします。

システムログには、Citrix Cloud 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 メニューで ［システムログ］を選択します。



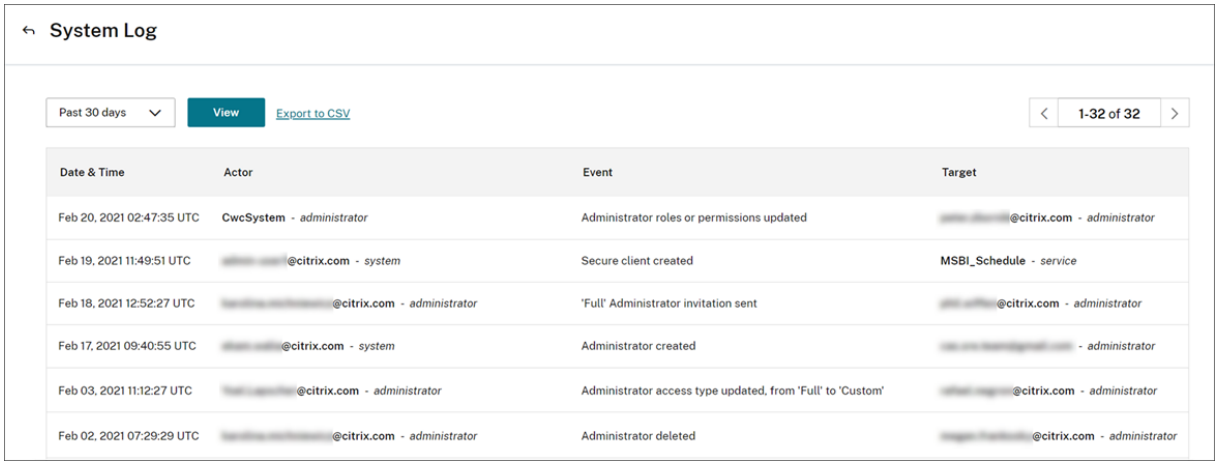
システムログのデータの保持について詳しくは、この記事の「データ保持」を参照してください。

ログに記録されたイベント

システムログには、次のイベントが記録されます:

- 管理者の追加、変更、および削除
- セキュアクライアントの作成と削除

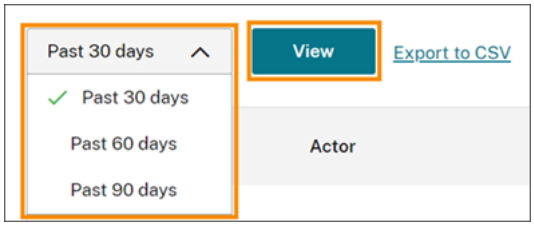
デフォルトでは、過去 30 日間に発生したイベントがシステムログに表示されます。最新のイベントが一番上に表示されます。



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 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 30 日間よりも前の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。過去 90 日間までに発生したイベントを表示できます。

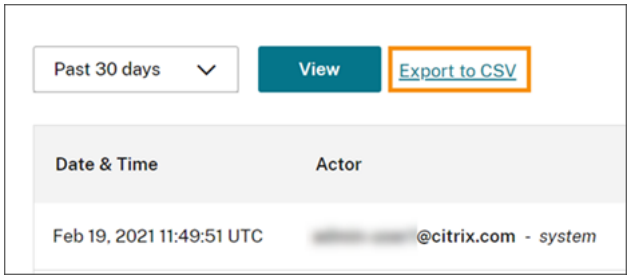


SystemLog API を使用して、指定した期間中に発生した古いイベントを取得できます。詳しくは、この記事の「特定期間のイベントの取得」を参照してください。

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 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。

特定期間のイベントの取得

特定の期間のイベントを取得する必要がある場合は、SystemLog API を使用できます。API を使用する前に、Citrix Developer Docs Web サイトの「Getting Started」で説明されているようにセキュアクライアントを作成する必要があります。

SystemLog API の使用について詳しくは、Citrix Developer Docs Web サイトの「Citrix Cloud - SystemLog」を参照してください。

システムログイベントの転送

Splunk 用の Citrix システムログアドオンを使用すると、Splunk インスタンスを Citrix Cloud に接続できます。この接続で、システムログデータを Splunk に転送できます。詳しくは、GitHub のシトリックスリポジトリの「add-on documentation」を参照してください。

Microsoft Azure Sentinel や IBM QRadar など、他のセキュリティ情報イベント管理（SIEM: security information event management）ソリューション用のアドオンはまだ利用できません。開発の進捗とリリースについては、次のリソースを定期的に確認してください:

- Citrix ブログ
- Citrix Cloud ディスカッションフォーラム
- シトリックスのソーシャルメディア: Twitter、LinkedIn、Facebook

データ保持

シトリックスとお客様は、Citrix Cloud が記録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。

シトリックスは、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。

Citrix Workspace

June 15, 2021

Citrix Workspace は、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安全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 により、ユーザーはコラボレーション、意思決定の改善、作業への集中に必要とする最も重要な詳細を整理および自動化できます。

Citrix Workspace の各エディションおよびその機能に関する説明については、「Citrix Workspace の機能マトリックス」を参照してください。

導入

Citrix Workspace には、ワークスペースをすばやく提供するための手順ごとのチュートリアルが含まれています。各手順では、Citrix Cloud コンソールを使用して、ID プロバイダーの構成、ワークスペース認証の選択、Workspace のその他のサービスの有効化などのタスクに関する指示を記載しています。このチュートリアルでは、展開チームを編成してインフラストラクチャとリソースを構成するのに必要となる技術情報にすばやくアクセスできるようになっています。タスクの概要と、展開を進めるときに必要となる情報については、「Citrix Workspace の利用を開始する」を参照してください。

マイクロアプリ

マイクロアプリは、関連する実用的な通知をアプリケーションからユーザーのワークスペースに直接配信するために使用できます。ユーザーは、組織内の主要なビジネスシステムを操作するためにアプリケーション間で切り替えをする必要がないとき、時間を節約でき、主要な作業に集中できます。アプリケーションデータソースからの統合を構築して、アクションを Workspace にプルします。マイクロアプリはソースシステムに書き戻すので、ユーザーはワークスペースを離れることなくこれらのアクションに対処できます。

詳しくは、マイクロアプリサービスのドキュメントを参照してください。

Citrix Virtual Apps Essentials サービス

Citrix Virtual Apps Essentials は仮想 Windows アプリへの安全なアクセスを提供します。このサービスには、デフォルトで有効になっているワークスペース URL が含まれています。通常は次の形式です: `https://yourcompanyname.cloud.com`。手順に従ってCitrix Virtual Apps Essentialsをセットアップし、利用者がアプリにアクセスできるように、ワークスペースの URL リンクをテストして利用者と共有します。

Citrix Virtual Desktops Essentials サービス

Citrix Virtual Desktops Essentials は Windows 10 仮想デスクトップへの安全なアクセスを提供します。このサービスには、デフォルトで有効になっているワークスペース URL が含まれています。通常は次の形式です: `https://yourcompanyname.cloud.com`。手順に従ってCitrix Virtual Desktops Essentialsをセットアップし、利用者がデスクトップにアクセスできるように、ワークスペースの URL リンクをテストして利用者と共有します。

Citrix Virtual Apps and Desktops サービス

Citrix Virtual Apps and Desktops サービスは、仮想アプリおよびデスクトップへの安全なアクセスを提供します。このサービスには、デフォルトで有効になっているワークスペース URL が含まれています。通常は次の形式です: `https://yourcompanyname.cloud.com`。手順に従ってCitrix Virtual Apps and Desktops サービスをセットアップし、利用者がアプリとデスクトップにアクセスできるように、ワークスペースの URL リンクをテストして利用者と共有します。利用者は、特に構成する必要なくワークスペース URL にアクセスできます。

Citrix Endpoint Management

ワークスペース環境が有効になっている Endpoint Management のお客様の場合、ユーザーがSecure Hubを開いて ［アプリの追加］をクリックすると、ユーザーは Secure Hub ストアではなく Workspace アプリストアに移動します。この機能は新規のお客様にのみ提供されます。既存のお客様はご利用いただけません。この機能を使用するには、次のタスクを実行します:

- Workspace 環境を新しいデバイスに展開するには、それらを Workspace デリバリーグループに追加します。詳しくは、「Citrix Endpoint Management と Citrix Workspace との統合」を参照してください。
- パスワードのキャッシュポリシーおよびパスワード認証ポリシーを有効にします。これらのポリシーの構成について詳しくは、「MDX ポリシーの概要」を参照してください。
- Active Directory 認証を AD または AD+Cert として構成します。この 2 つのモードがサポートされています。認証の構成について詳しくは、「ドメインまたはドメイン + セキュリティトークン認証」を参照してください。
- Endpoint Management のワークスペース統合を有効にします。ワークスペース統合について詳しくは、「ワークスペース構成」を参照してください。

  > 重要:
  >
  > この機能を有効にすると、ShareFile SSO は Endpoint Management 経由ではなく、Workspace を通じて実行されます。ワークスペースの統合を有効にする前に、Endpoint Management コンソールで ShareFiles の統合を無効にすることをお勧めします。

Citrix Gateway

Citrix Gateway（以前の NetScaler Gateway Service）は、Identity and Access Management（IdAM）機能を備えた安全なリモートアクセスを提供します。Citrix Gateway は、SaaS（Software as a Service）アプリ、および仮想アプリとデスクトップに、統合されたエクスペリエンスを提供します。手順に従ってCitrix Gateway サービスをセットアップし、ワークスペース URL をテストして利用者と共有し、利用者のリモートアクセスを可能にします。Citrix Gateway サービスで SaaS アプリを構成する方法について詳しくは、「Support for Software as a Service Apps」を参照してください。

Citrix Content Collaboration

Citrix Content Collaboration（旧称：ShareFile）により、あらゆるデバイスから安全にデータアクセス、同期、ファイル共有ができるようになります。ビジネスクラスのファイル共有、合理化されたワークフロー、リアルタイムコラボレーションを 1 つの場所にまとめて、ユーザーが思いどおりに作業できるようにします。

1. Content Collaboration の使用権があることを確認します。
2. Citrix Workspace を Content Collaboration アカウントにリンクします。詳しくは、「Content Collaboration（ShareFile）アカウントの作成または Citrix Cloud へのリンク」の記事に記載されている「Content Collaboration について」を参照してください。
3. Citrix Workspace で Content Collaboration を有効にします。Citrix Content Collaboration ドキュメントセットの「Citrix Workspace に Citrix Content Collaboration を展開して有効にする」を参照してください。このプロセスを設定している場合は、Citrix Workspace UI の左側ナビゲーションに ［ファイル］タブが表示されます。

電子署名

Citrix は、Citrix RightSignature を使用して電子署名機能を提供します。電子署名は、電子であることを除いては紙の文書に書き込む手書きの署名と同じであり、文書の条件に同意する意図を示すために電子契約書や電子文書に付けられるマークです。RightSignature について詳しくは、「RightSignature のよくある質問」を参照してください。

ユーザーは、Citrix RightSignature と Citrix Content Collaboration を統合して、Citrix Workspace から直接署名を送信できます。ShareFile RightSignature 統合を参照して、次の手順を実行します：

1. Content Collaboration と RightSignature の使用権があることを確認します。
2. Citrix Workspace を Content Collaboration アカウントにリンクし、Citrix Workspace で Content Collaboration を有効にします。詳しくは、「Content Collaboration（ShareFile）アカウントの作成または Citrix Cloud へのリンク」の記事に記載されている「Content Collaboration について」および Citrix Content Collaboration ドキュメントの「Citrix Workspace に Citrix Content Collaboration を展開して有効にする」を参照してください。このプロセスを設定している場合は、Citrix Workspace UI の左側ナビゲーションに ［ファイル］タブが表示されます。
3. エンドユーザーに対して RightSignature を有効にします。「RightSignature にユーザーを追加する」のサポート記事を参照してください。このプロセスを設定している場合は、Citrix Workspace UI の ［ファイル］

から開いたすべてのファイルで ［署名の送信］タイルを確認できます。

Citrix RightSignature は、スタンドアロンソリューションとしても利用できます。はじめに、「RightSignature」を参照してください。Content Collaboration の電子署名については、「Citrix Content Collaboration - 電子署名」を参照してください。

Secure Browser サービス

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、Web ブラウザーベースの攻撃から企業ネットワークを保護します。利用者が管理者から提供された URL に移動すると、他の Citrix Cloud サービスで構成されているアプリやデスクトップとともに、公開 Web ブラウザーが表示されます。手順に従ってSecure Browser サービスをセットアップし、ワークスペース URL をテストして利用者と共有し、利用者がセキュリティで保護されたブラウザーにアクセスできるようにします。

ユースケースの例

所属する組織は現在、Citrix Virtual Apps and Desktops サービスを介して複数の Microsoft Office アプリを管理し、Citrix Gateway で Workday などの SaaS アプリを管理しています。

また、オンプレミス Virtual Apps and Desktops 環境にはレガシーアプリもあります。これらすべてのアプリを 1 つの統合されたユーザーエクスペリエンスに配信できるようになりました。

ユーザーは、必要なすべてのアプリが利用できる自分のワークスペースにブラウザーまたはアプリ（**Citrix Workspace** アプリ）からアクセスできます。Citrix Cloud のシンプルなコンソール（[ワークスペース構成]）でエクスペリエンスをカスタマイズし、ユーザーの認証方法を選択できます。

このユースケースでは、まず、個々のサービスのセットアップを完了します。［ワークスペース構成］に切り替えて、Workspace のユーザーエクスペリエンス全体の動作をさらにカスタマイズして構成します。［ワークスペース構成］（［サイト］タブ内）で、オンプレミス Virtual Apps and Desktops 環境を Workspace ユーザーエクスペリエンスに接続します（「サイトアグリゲーション」と呼ばれます）。クライアントレスアクセス用のワークスペース **URL** をユーザーと共有し、最適なエクスペリエンスを得るために **Citrix Workspace** アプリをインストールするようにユーザーに指示します。

パートナー向けの **Citrix Cloud**

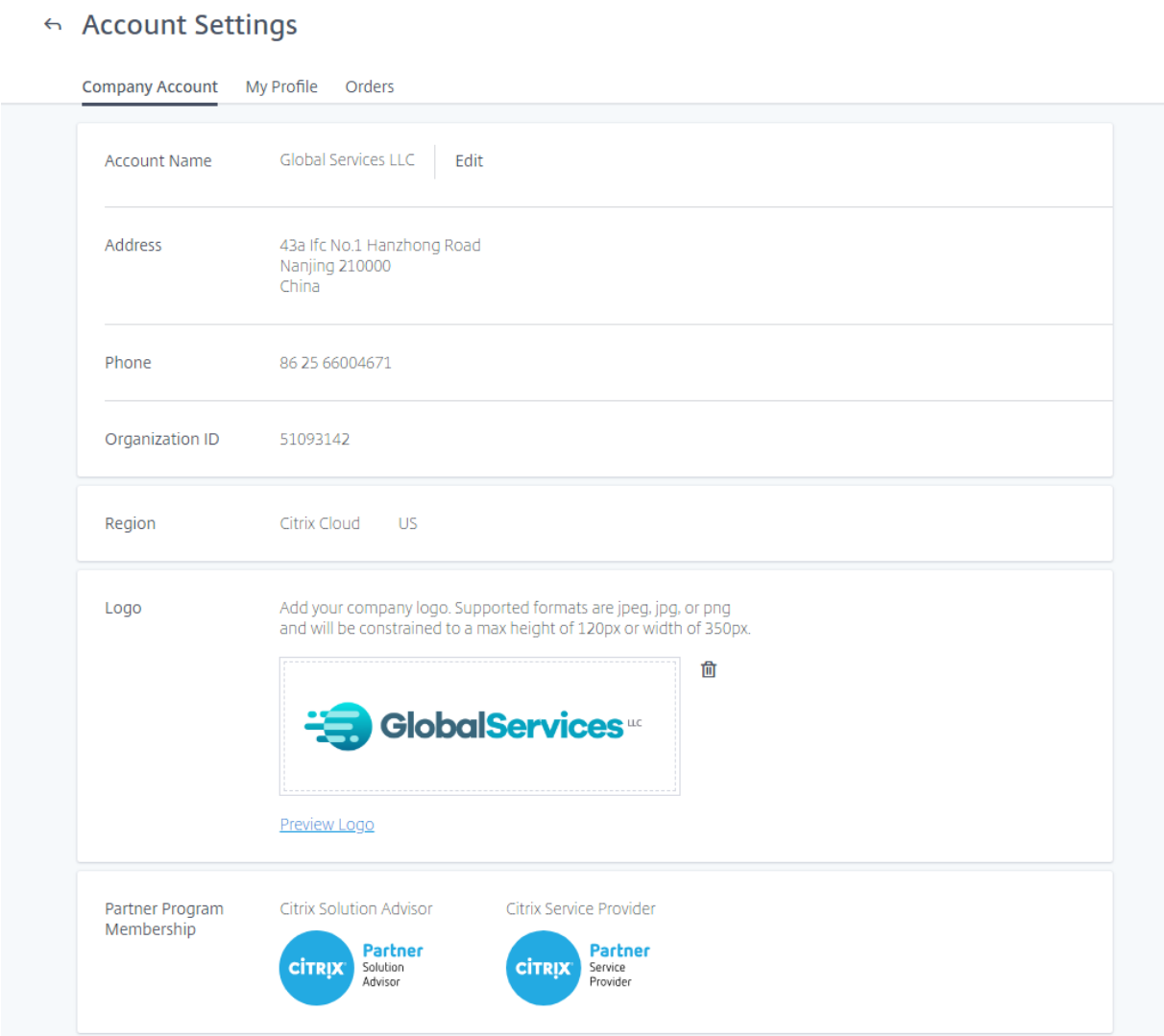
September 17, 2021

Citrix Cloud 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。このセクションでは、Citrix Cloud サービスおよびソリューション上でシトリックスパートナーが利用できる、顧客とのコラボレーションに役立つ機能について説明します。

パートナー **ID**

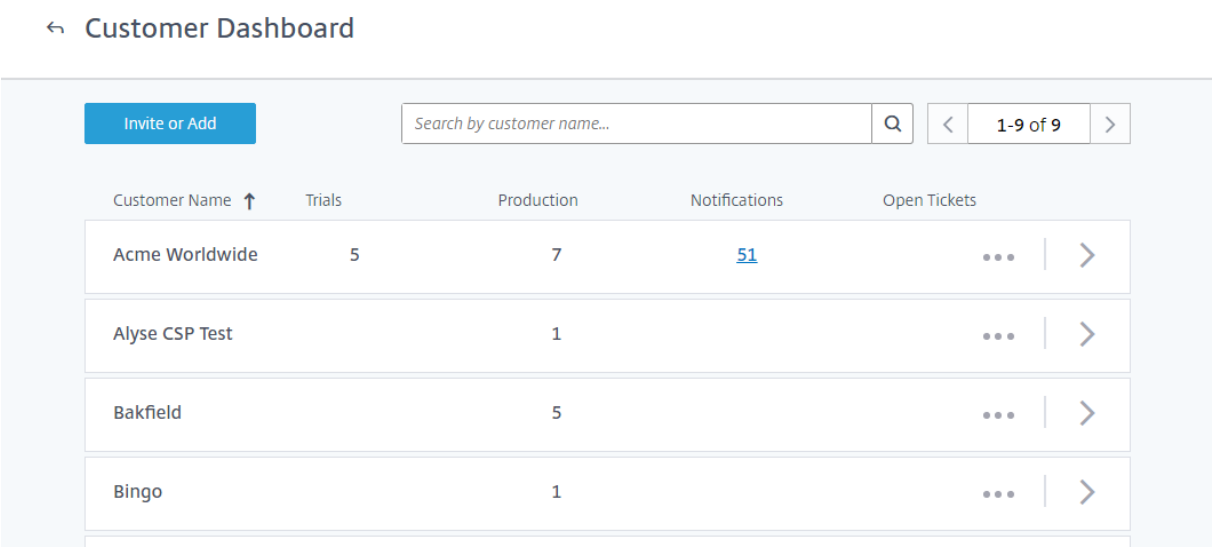
パートナーは、Citrix 組織 ID（ORGID）に基づいて Citrix Cloud で識別されます。Citrix Cloud の各アカウントは Citrix ORGID に関連付けられています。Citrix ORGID は Citrix Cloud のアカウントの詳細で確認できます。

アカウントの ORGID がシトリックスパートナープログラム（Citrix Solution Advisor や Citrix Service Provider）のアクティブなメンバーである場合は、シトリックスパートナーがこのアカウントを所有していることを示すプログラムバッジが表示されます。パートナー ID は、追加のクラウドサービスや機能へのアクセスを管理するために使用されます。



顧客ダッシュボード

顧客ダッシュボードは、パートナーが統合されたビューで複数の Citrix Cloud 顧客の状態を確認できるように設計されています。顧客がダッシュボードに表示されるためには、パートナーと顧客の間で接続が確立されている必要があります。顧客ダッシュボードは、パートナーバッジを持つ Citrix Cloud アカウントで使用できます。



顧客との接続

Citrix Cloud ソリューションで顧客とコラボレーションしているパートナーは、アカウント間で信頼済みリンクを確立できます。このアカウントレベルの関係によって、顧客は特定の情報を簡単にパートナーと共有できるようになります。顧客はパートナーとの接続を承諾することにより、Citrix Cloud アカウントおよびシトリックスとの関係に関する情報を閲覧する権限をパートナーに付与します。

パートナー接続を確立すると、以下のことが可能になります。

- 顧客がパートナーのダッシュボードに表示される
- 顧客アカウントの設定にパートナーがアクティブな接続として表示される
- Citrix Cloud サービス使用権のパートナーへの表示
- ライセンス使用状況とアクティブな Citrix Cloud サービス使用権のパートナーへの表示

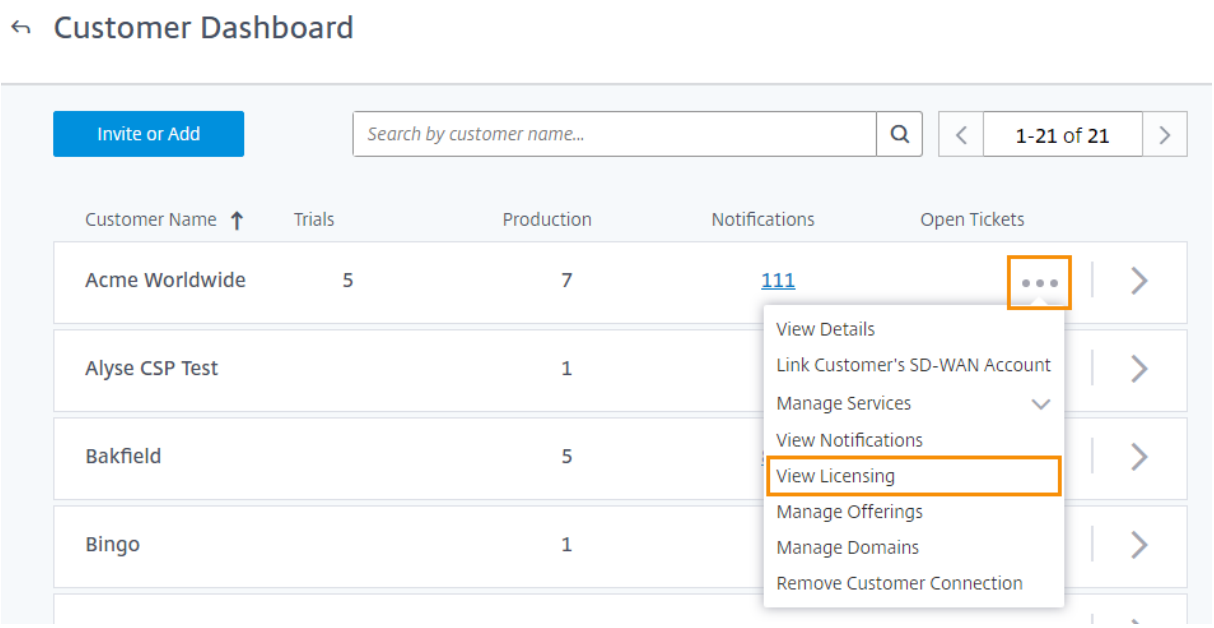
以下は、パートナー接続に関するその他の情報です。

- パートナーは複数の顧客との接続を確立できる
- 顧客は複数のパートナーとの接続を確立できる
- 顧客とパートナーとの接続数に制限はない
- 顧客またはパートナーのいずれも、接続を随時終了できる
  - 顧客の場合はアカウントの詳細ページから
  - パートナーの場合は顧客ダッシュボードから
- Citrix Cloud の通知は、接続ワークフローに従って送信される
  - 顧客の接続が作成されるとパートナーに通知される
  - 顧客が接続を終了するとパートナーに通知される
  - パートナーが接続を終了すると顧客に通知される
- ライセンスの表示は、ライセンスの割り当てと使用状況の傾向の概要に限定される
- パートナーから顧客への接続に有効期限はない

パートナーと顧客との接続が確立されると、パートナーの管理者は、顧客の基本アカウント情報、顧客の注文の詳細とともに、サービス、ライセンス数、有効期限などの使用権情報を表示できます。

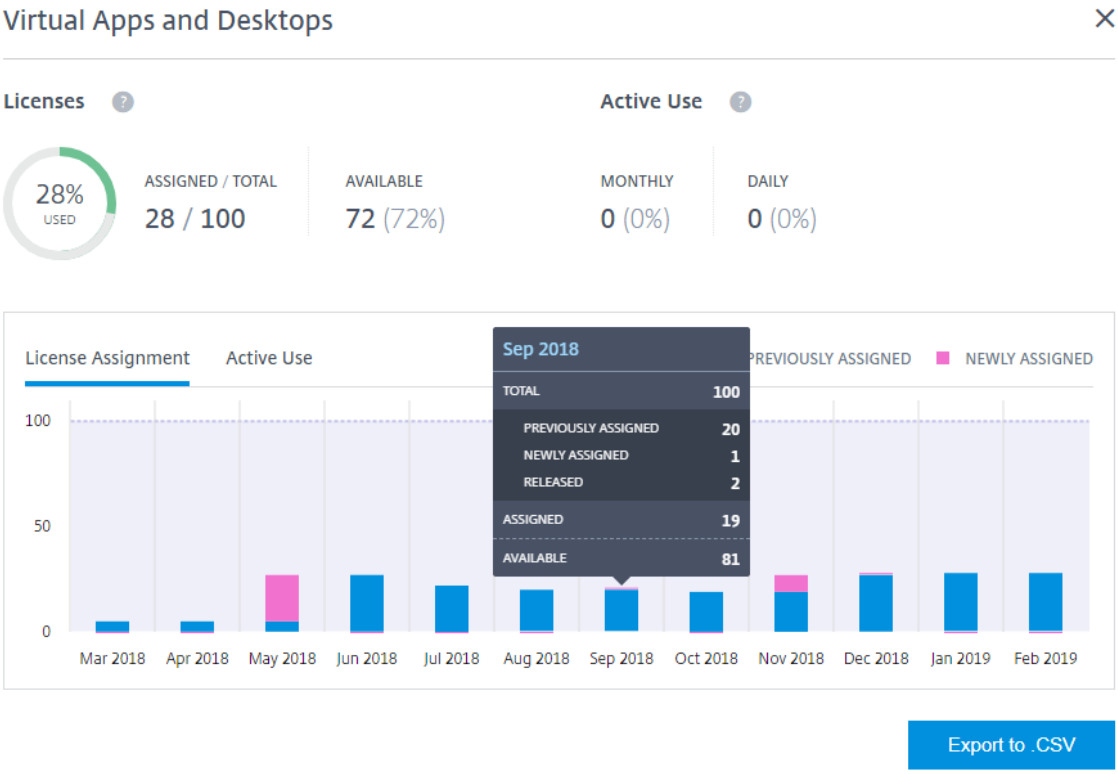
ライセンスの傾向

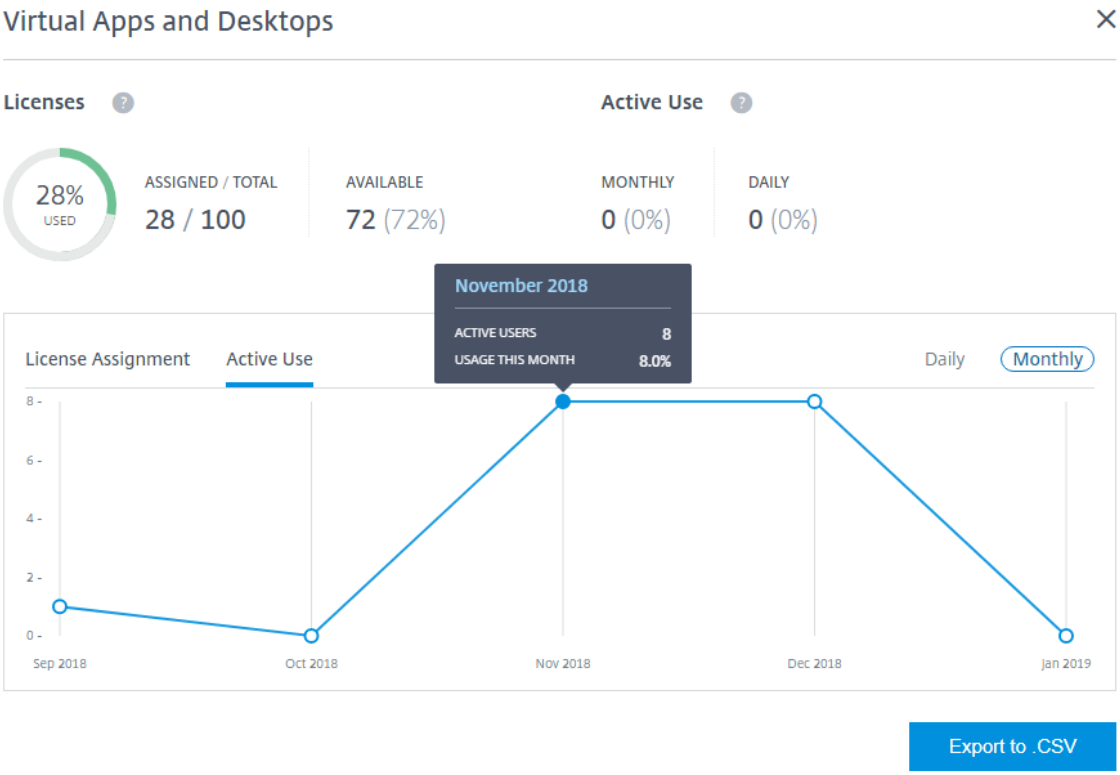
パートナーは、対象顧客の横の省略記号ボタンをクリックし、［ライセンスの表示］を選択することで、顧客ダッシュボードからライセンス情報を表示できます。



> 注:
>
> シトリックスパートナーは、ライセンスの概要ビューと、アクティブな使用状況の履歴の傾向のみを表示できます。特定のサービスのライセンスを消費する個々のユーザーを表示することはできません。

概要を表示するには、顧客ページの ［使用状況］タブで ［使用状況の傾向の表示］を選択します。概要には、購入済みライセンスに対する割り当て済みライセンスの比率、割り当て済みライセンスの内訳、および月ごと/日ごとのアクティブユーザーなどが表示されます。必要に応じて、パートナーはこの情報を.csv ファイルとしてエクスポートできます。

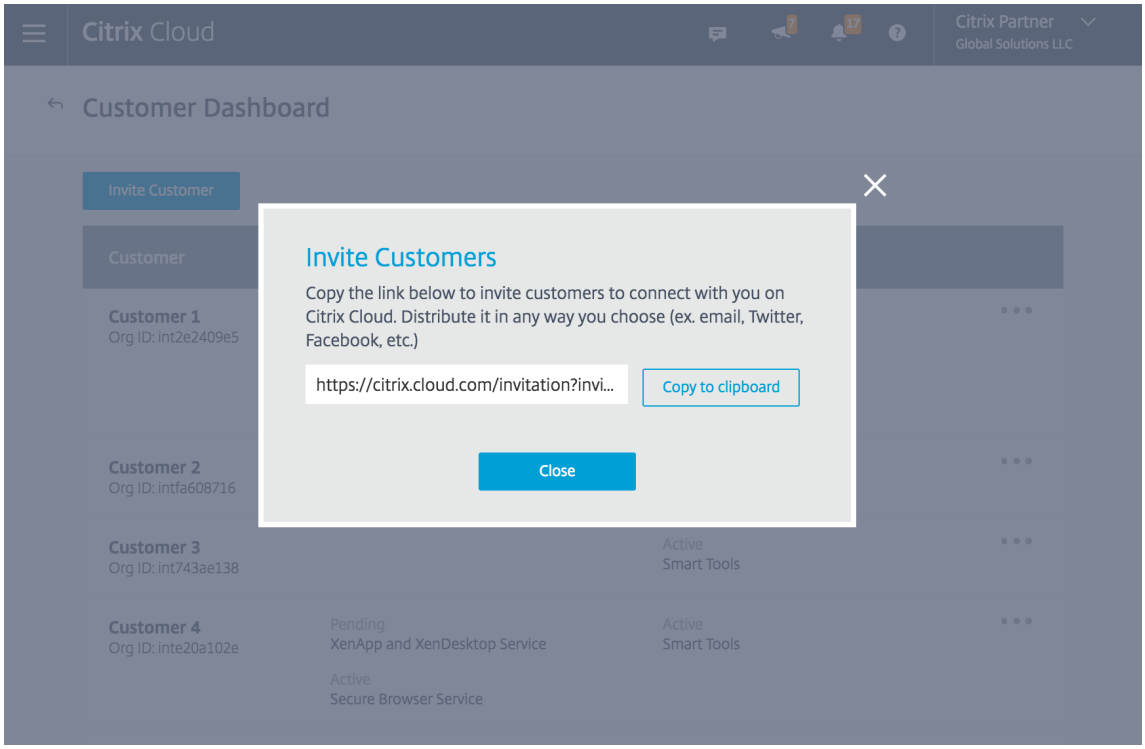




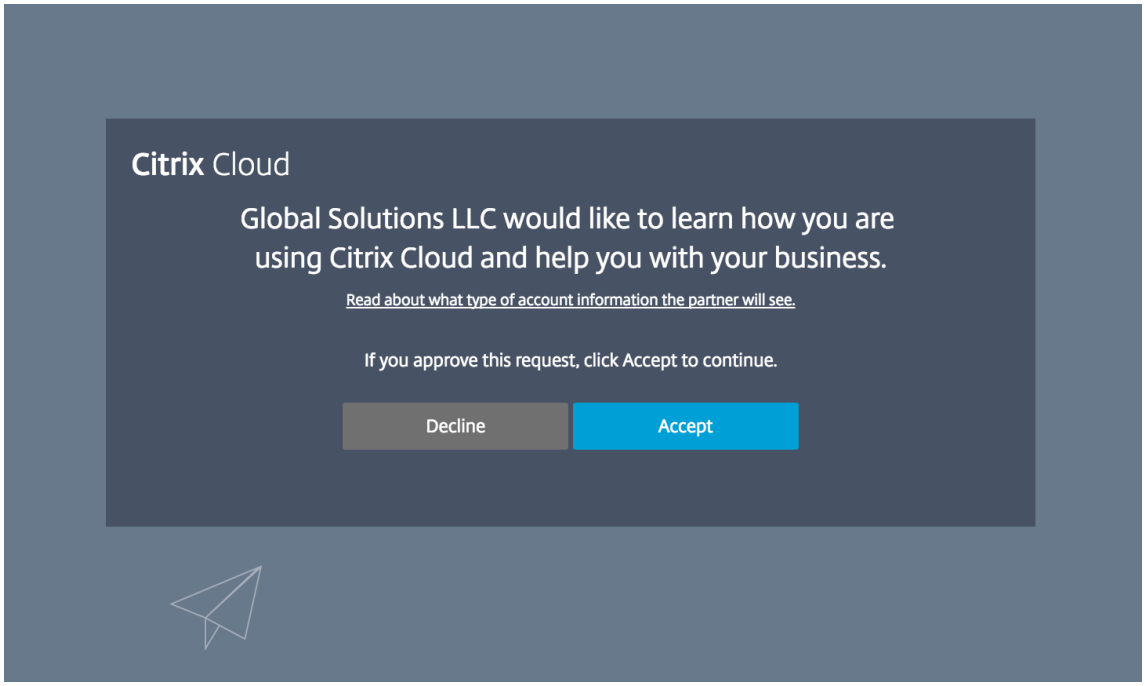
顧客を接続に招待する

パートナーは、以下の簡単な 3 つの手順で顧客に接続できます。

1. パートナーが顧客ダッシュボードから招待リンクを取得します。



2. パートナーが招待リンクをコピーして顧客に送信します。
3. 顧客がリンクをクリックし、サインイン（または登録）して接続要求を承諾します。



以下は、パートナー招待リンクに関するその他の情報です。

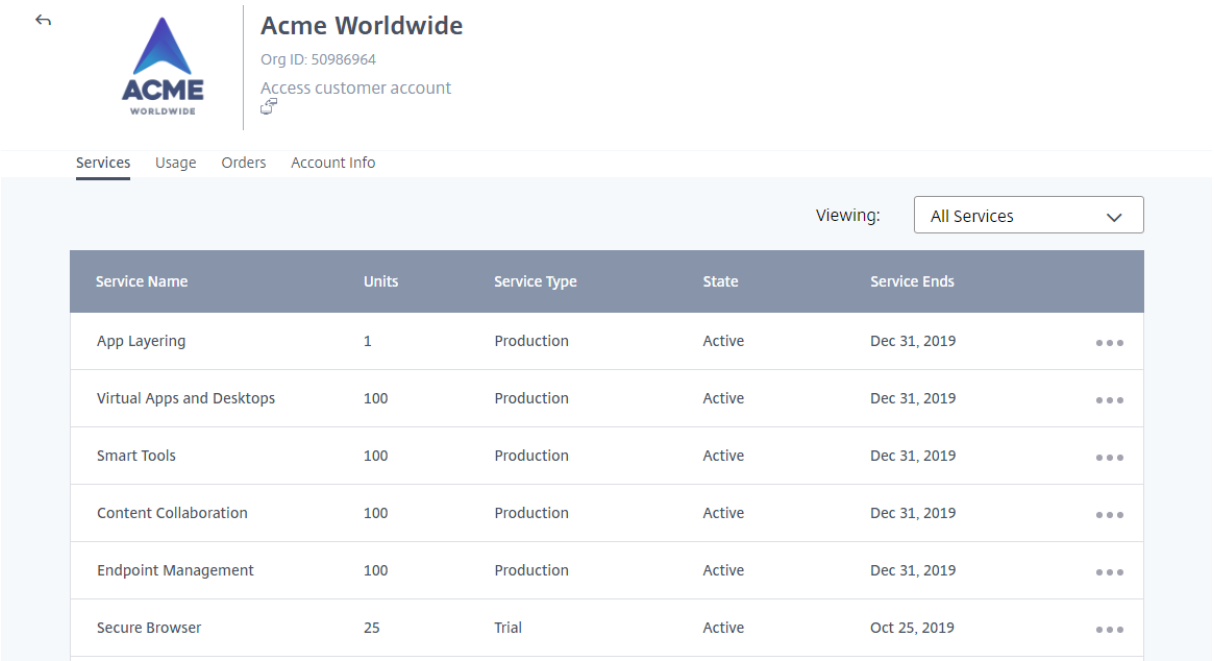
- パートナーには、1 つの招待リンクが提供されます。リンクは固定されており、カスタマイズや変更はできません。

- 接続を確立するためにリンクを使用できる回数に制限はない
- 接続を再作成する必要がある場合はリンクを再使用できる
- リンクは失効しない

Citrix Cloud サービス使用権のパートナーへの表示

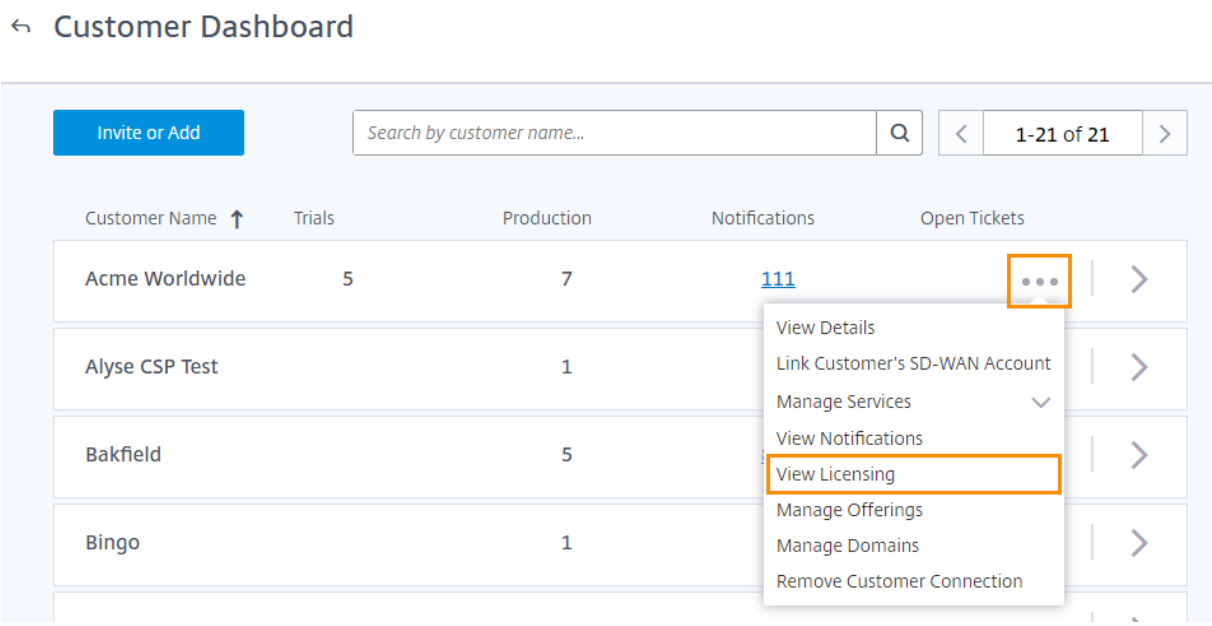
顧客がシトリックスパートナーの接続の招待を承諾すると、パートナーは顧客の Citrix Cloud サービス使用権の状態の基本情報を閲覧できるようになります。この情報には、トライアルとトライアル以外の両方の使用権の状態が含まれます。さらに、以下の情報が含まれます。

- アクティブなサービストライアル
- 保留中のサービストライアルリクエスト
- 期限切れのサービストライアル
- アクティブなサービスの使用権（顧客が購入したサービス、または権限が付与されたサービスや有効なサービス）
- 使用権のライセンス数と有効期限



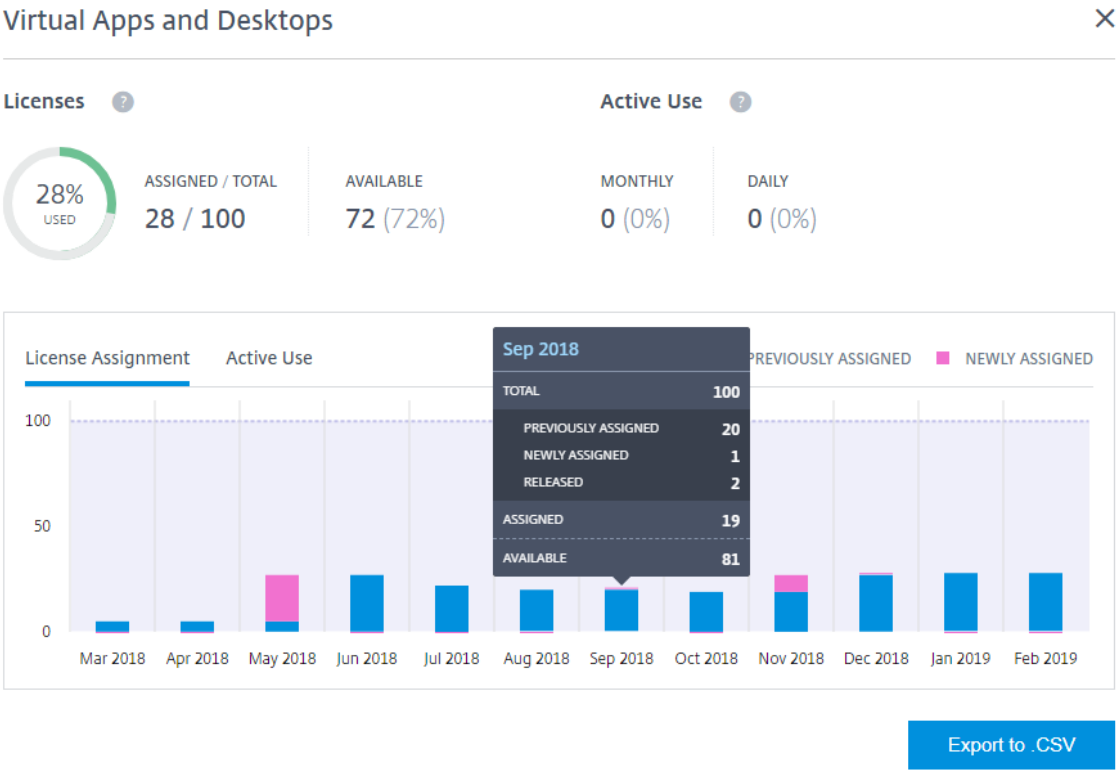
ライセンスの傾向

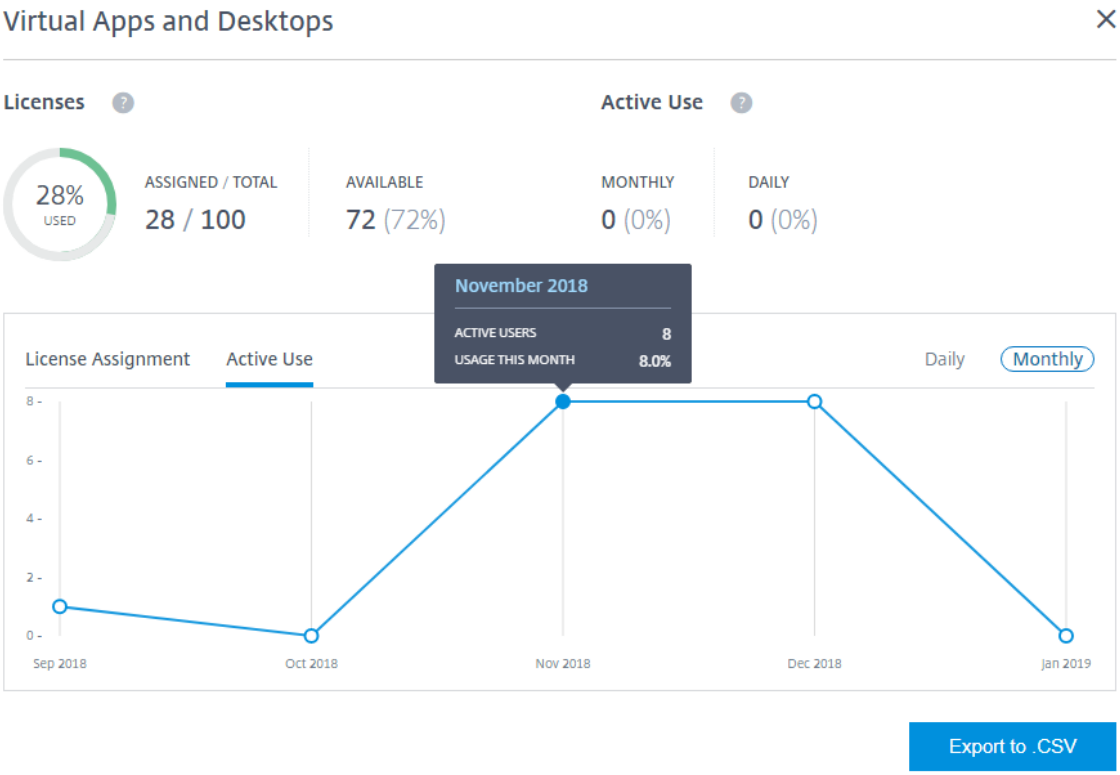
パートナーは、対象顧客の横の省略記号ボタンをクリックし、［ライセンスの表示］を選択することで、顧客ダッシュボードからライセンス情報を表示できます。



> 注:
>
> シトリックスパートナーは、ライセンスの概要ビューと、アクティブな使用状況の履歴の傾向のみを表示できます。特定のサービスのライセンスを消費する個々のユーザーを表示することはできません。

顧客ページの ［使用状況］タブで ［使用状況の傾向の表示］をクリックすると、購入済みライセンスに対する割り当て済みライセンスの比率、割り当て済みライセンスの内訳、および月ごと/日ごとのアクティブユーザーを含む概要が表示されます。必要に応じて、パートナーはこの情報を.csv ファイルとしてエクスポートできます。





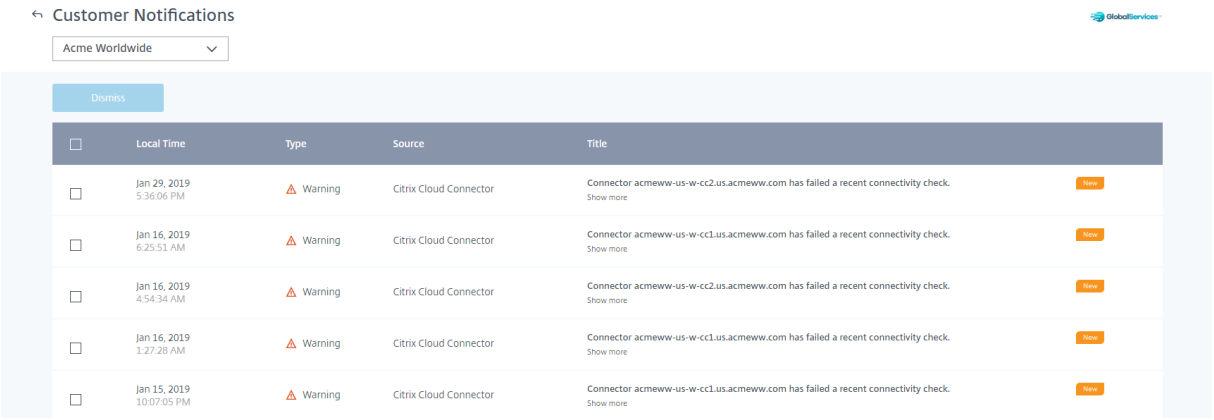
Citrix Service Provider の顧客のライセンスと使用状況

Citrix Cloud のライセンス機能により、Citrix Service Provider（CSP）の顧客は、サポートされている Virtual Apps and Desktops 製品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、次の記事を参照してください:

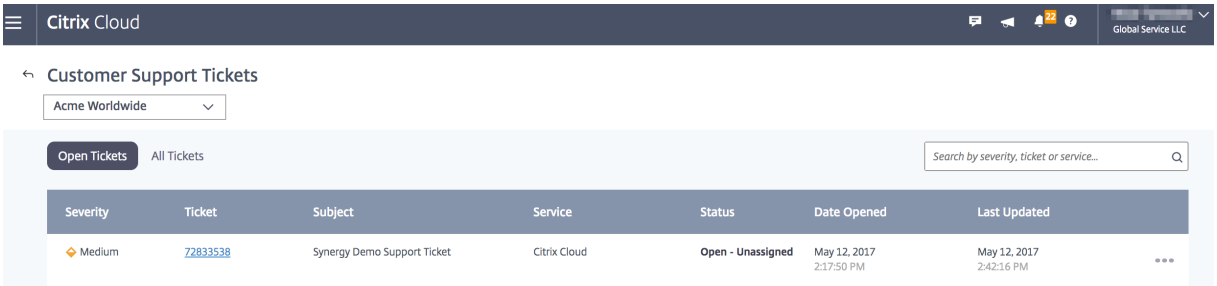
- Citrix Virtual Apps and Desktops サービスの顧客のライセンスと使用状況の監視
- Citrix Virtual Apps and Desktops Standard for Azure の顧客のライセンスと使用状況の監視

顧客のサポートチケットおよび通知のパートナーへの表示

パートナーは、接続された顧客のサポートチケットと通知を表示できます。また、特定の顧客ごとに通知を絞り込み、通知を消去するなどの対応を取ることもできます。消去された通知は、パートナーには表示されません。ただし、顧客は Citrix Cloud にサインインした後、アカウントで通知を表示できます。



顧客サポートチケットの表示は、パートナーが顧客のために問題を解決するのに役立ち、合理化されたエラーのないエクスペリエンスをユーザーに提供できるようになります。



Citrix Service Provider のフェデレーションドメイン

_ フェデレーションドメイン _ を使用すると、顧客ユーザーは、Citrix Service Provider のリソースの場所に関連付けられたドメインの資格情報を使用して、ワークスペースにサインインできます。これにより、顧客ユーザーが *customer.cloud.com* などのカスタムワークスペースの URL を使用してアクセスできる専用のワークスペースを提供できます。リソースの場所は引き続きパートナーの Citrix Cloud アカウント上にあります。顧客が Citrix Serivce Provider ワークスペースの URL（csppartner.cloud.com など）を使用してアクセスできる共有ワークスペースとともに、専用のワークスペースを提供できます。顧客が専用のワークスペースにアクセスできるようにするには、管理する適切なドメインに顧客を追加します。ワークスペースを構成した後、顧客ユーザーはワークスペースにサインインして、Virtual Apps and Desktops サービスで利用可能にしたアプリとデスクトップにアクセスできます。

フェデレーションドメインから顧客を削除すると、顧客のユーザーはパートナーのドメインの資格情報を使用してワークスペースにアクセスできなくなります。

フェデレーションドメインを使用してアプリとデスクトップを配信する方法について詳しくは、「Citrix Service Provider 用の Citrix Virtual Apps and Desktops サービス」を参照してください。

Citrix Service Provider のワークスペースの外観オプション

カスタムテーマを使用して、ワークスペースの色とロゴを構成できます。カスタムテーマを作成する方法については、「ワークスペースの外観をカスタマイズする」を参照してください。

> 注
>
> カスタムテーマはシングルテナント機能です。サービスプロバイダーのテナントがリソースの場所、Cloud Connector、および Active Directory ドメイン（マルチテナント）を共有する Citrix Service Provider は、現在サポートされていません。専用のリソースの場所、Cloud Connector、および専用の Active Directory ドメイン（シングルテナント）を持つ Citrix Service Provider テナントが完全にサポートされています。

Content Collaboration

January 21, 2021

Content Collaboration を使用すると、クラウドおよびオンプレミスのストレージサービスからのコンテンツを共有、同期、保護することができます。

Citrix Cloud での Content Collaboration アカウントの作成については、「Content Collaboration（ShareFile）アカウントの作成または Citrix Cloud へのリンク」を参照してください。

セットアップタスクの詳細については、「ShareFile をセットアップ」を参照してください。

Content Collaboration を展開し Citrix Workspace で Citrix Files を使用する方法については、「Citrix Content Collaboration」を参照してください。

サポートされている各プラットフォームでの Citrix Files の使用について詳しくは、ユーザーヘルプセンターの「Citrix Files」を参照してください。

サービスレベルアグリーメント

Content Collaboration は、業界のベストプラクティスを使用して、クラウドの規模と高度なサービス可用性を実現するように設計されています。

Citrix Cloud サービスの可用性に関するシトリックスの目標について詳しくは、「サービスレベルアグリーメント」を参照してください。

Content Collaboration（ShareFile）アカウントの作成または Citrix Cloud へのリンク

September 17, 2021

Content Collaboration の使用を開始するには、次のオプションを利用できます:

- Content Collaboration を使用した経験がなく試用する場合、トライアルをリクエストすることができます。

- ShareFile アカウントを持っているが新しい使用権を購入していない場合、アカウントを Citrix Cloud に接続できます。
- ShareFile または Workspace の使用権を購入済みの場合、Citrix Cloud で新しいアカウントを作成して、そのアカウントに使用権を割り当てることができます。
- ShareFile または Workspace の使用権を購入済みの場合、既存の ShareFile アカウントを Citrix Cloud に接続して、新しい使用権を割り当てることもできます。

トライアルのリクエスト

Content Collaboration アカウントを持たずにサービスを試用する場合、以下の手順を実行します。

1. Citrix の資格情報で Citrix Cloud にサインインします。
2. Citrix Cloud コンソールの ［マイサービス］で、［**Content Collaboration**］タイルに移動します。
3. ［サービスの追加］で、［トライアルのリクエスト］を選択します。

［トライアルのリクエスト］タブが選択された［Content Collaboration アカウントの追加］ページが表示されます。

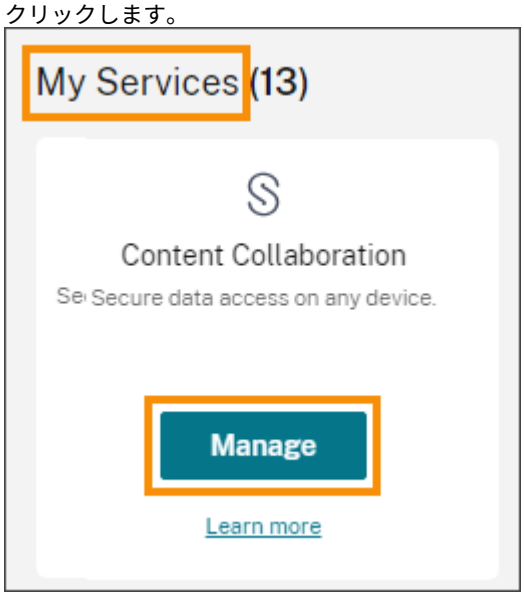
4. ［地理的な場所］セクションで、サービスを使用するリージョンを選択し、トライアルをリクエストした後で場所を変更できないことを承認します。
5. ［サブドメインを選択］セクションで、使用する固有のサブドメインを入力します。
6. ［トライアルのリクエスト］をクリックします。Content Collaboration アカウントが作成されたら、Citrix Cloud からメールが送信されます。
7. ［マイサービス］で Content Collaboration タイルの ［管理］をクリックして、［Content Collaboration Admin Overview］に進みます。

新しい **Content Collaboration** アカウントの作成と使用権の割り当て

Content Collaboration の使用権を購入済みで、新しいアカウントを作成してそのアカウントに使用権を割り当てる場合、以下の手順を実行します。

1. Citrix Cloud の資格情報でCitrix Cloudにサインインします。

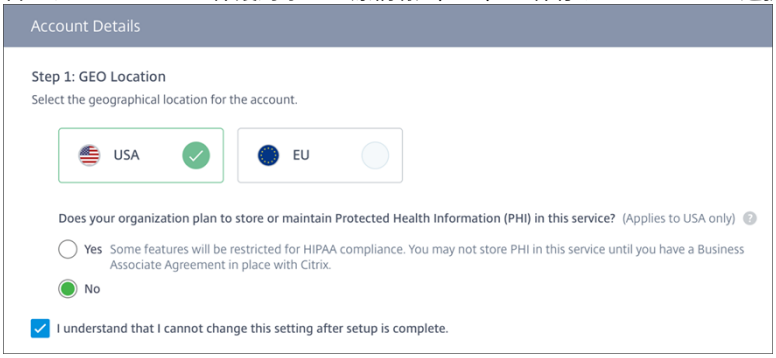
2. Citrix Cloud コンソールの ［マイサービス］で、［Content Collaboration］タイルに移動して ［管理］をクリックします。



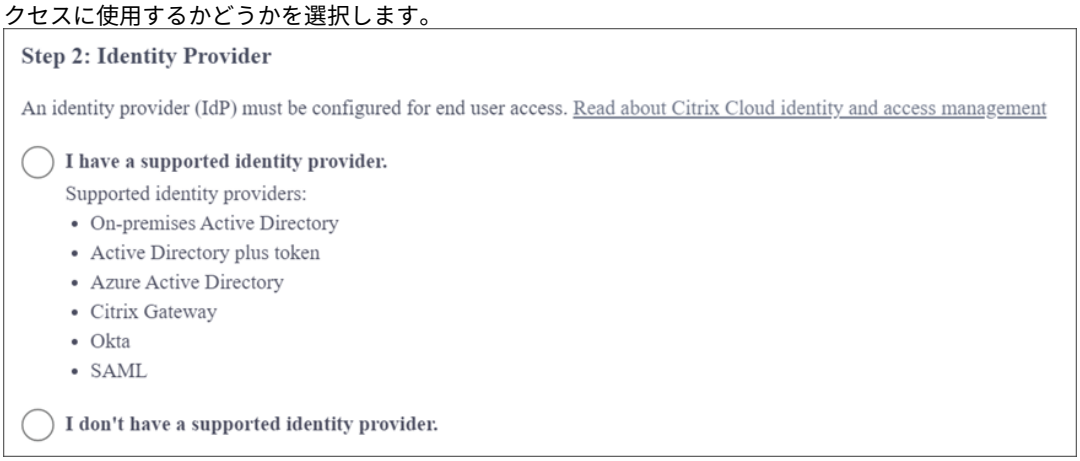
［Content Collaboration の使用権を割り当てる］ページに、Citrix OrgID を使用して購入した新しい Content Collaboration 使用権が表示されます。

3. アカウントに適用する使用権を選択して、［続行］をクリックします。
4. ［アカウント名］で、使用権に割り当てる新しいアカウントを選択し、［割り当て］をクリックします。

5. ［**Content Collaboration** アカウントの作成］ページの ［アカウントの詳細］で、次の情報を入力します。
   a) 手順 **1**：地理的な場所で、サービスを使用するリージョンを選択します。USA リージョンを選択した場合は、アカウントに保護対象の医療情報（PHI）を保存するかどうかを選択します。

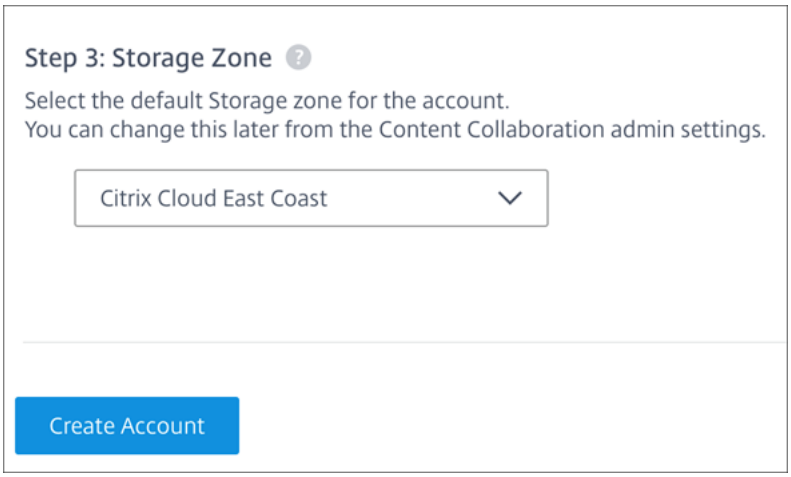


b) 手順 **2**：**ID** プロバイダーで、サポートされている ID プロバイダーをアカウントへのエンドユーザーアクセスに使用するかどうかを選択します。



ID プロバイダーがサポートされていない場合、または ID プロバイダーがない場合は、［サポートされている **ID** プロバイダーがありません］を選択し、ShareFile サブドメインを選択します。その後、Citrix が ShareFile.com アカウントを作成します。

c) 手順 **3**：ストレージゾーンで、アカウントのデフォルトのストレージゾーンを選択します。



6. ［アカウントの作成］を選択します。

既存の **ShareFile** アカウントのリンク

既存の ShareFile アカウントを Citrix Cloud アカウントにリンクするには、次の要件を満たしている必要があります：

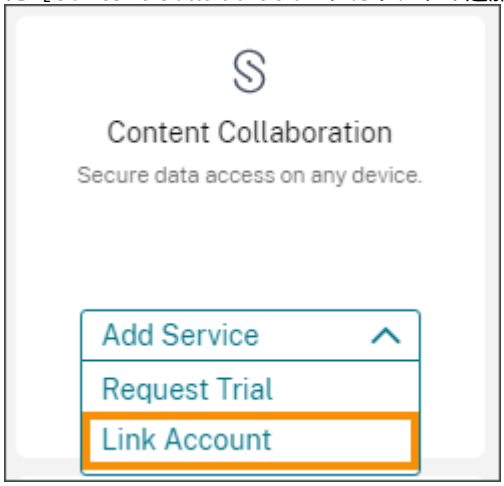
- Citrix Cloud と ShareFile の両方で管理者権限が必要です。
- ShareFile 管理者の権限には、［会社のアカウント権限にアクセス］が含まれている必要があります。
- Citrix Cloud にサインインするために使用するメールアドレスが、ShareFile のレコードにあるメールアドレスと一致する必要があります。

これらの要件のいずれかが満たされない場合、Citrix Cloud が割り当てる ShareFile アカウントを見つけることができない場合があります。これらの要件について詳しくは、シトリックスサポートにお問い合わせください。

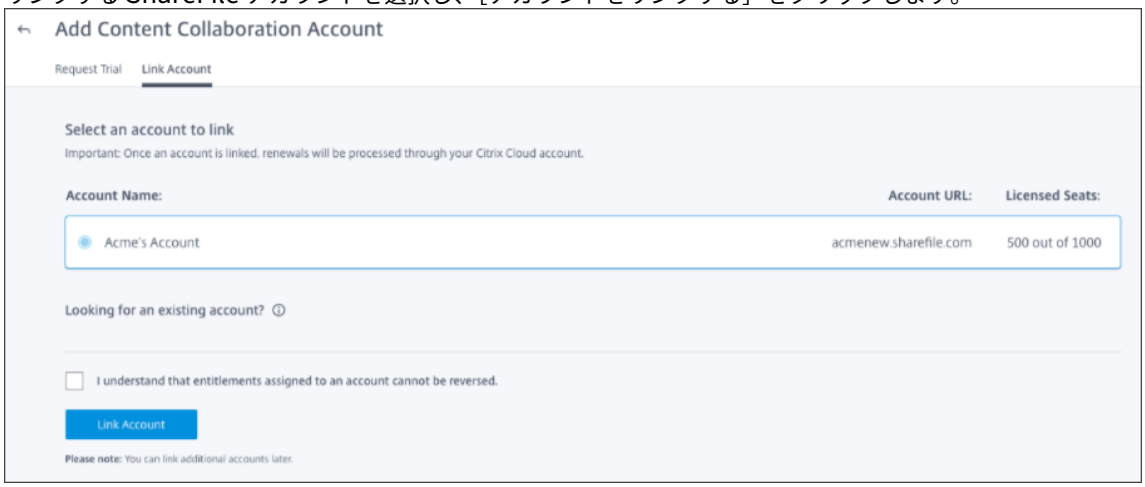
Content Collaboration アカウントを **Citrix Cloud** にリンクするには（新しい使用権なし）

新しい使用権を購入していないが既存の ShareFile アカウントを Citrix Cloud にリンクする場合、次の手順を実行します。

1. Citrix の資格情報で Citrix Cloud にサインインします。
2. Citrix Cloud コンソールの ［マイサービス］で、［Content Collaboration］タイルに移動します。
3. ［サービスの追加］で、［アカウントをリンクする］を選択します。［アカウントをリンクする］タブが選択された［Content Collaboration アカウントの追加］ページが表示されます。



4. リンクする ShareFile アカウントを選択し、［アカウントをリンクする］をクリックします。

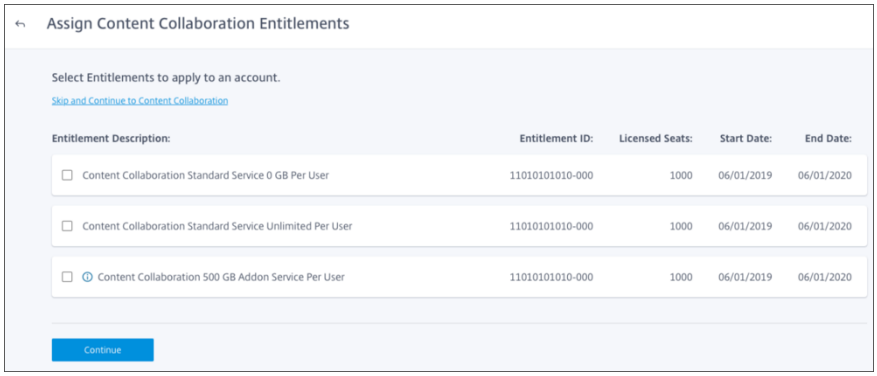


> 重要：
>
> アカウントが表示されない場合、ShareFile の管理者であること、かつ Citrix Cloud のメールアドレスが Content Collaboration のメールアドレスと一致することを確認してください。問題が解決されない場合、シトリックスサポートにお問い合わせください。

ShareFile アカウントをリンクして使用権を割り当てるには

新しい ShareFile または Workspace の使用権を購入済みの場合、Citrix Cloud でその使用権を割り当てて管理するには、次の手順を実行します。

1. Citrix の資格情報で Citrix Cloud にサインインします。
2. Citrix Cloud コンソールの ［マイサービス］で、［Content Collaboration］タイルに移動して ［管理］をクリックします。［Content Collaboration の使用権を割り当てる］ページが表示され、購入済みの新しい使用権が表示されます。
3. アカウントに適用する使用権を選択して、［続行］をクリックします。



4. 選択した使用権に適用するアカウントを選択します。

   > 重要:
   >
   > アカウントが表示されない場合、Content Collaboration の管理者であること、かつ Citrix Cloud のメールアドレスが ShareFile のメールアドレスと一致することを確認してください。問題が解決されない場合、シトリックスサポートにお問い合わせください。
   >
   > 「**Content Collaboration** アカウントが見つかりません」というメッセージが表示された場合、「Citrix Cloud に接続したことのないアカウントにリンクするには」を参照して手順を完了します。

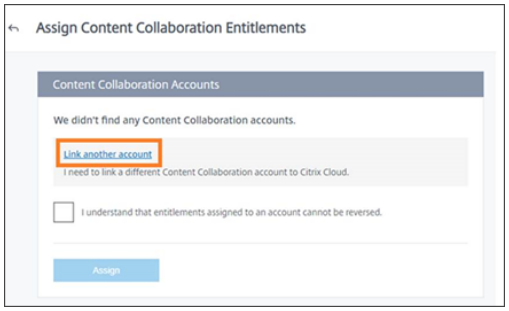
5. ［アカウントに割り当てられた使用権を取り消すことはできないことを了承します］チェックボックスをオンにします。
6. ［割り当てる］をクリックします。［Content Collaboration の使用権を割り当てる］ページに、使用権を割り当てられたアカウントが表示されます。
7. ［管理］をクリックして、［Content Collaboration Admin Overview］に進みます。

Citrix Cloud に接続したことのないアカウントにリンクするには

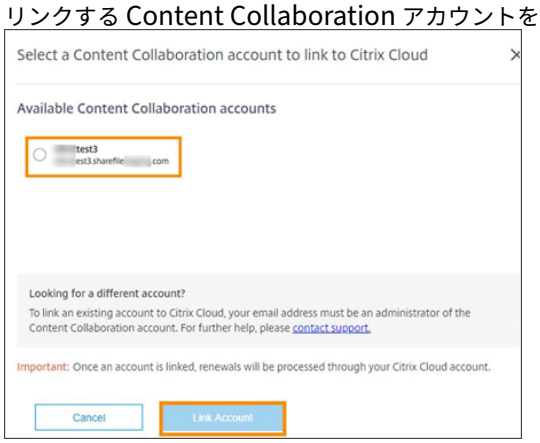
Citrix Cloud にアカウントをリンクしたことがない場合は、次の手順を実行します。

1. Citrix の資格情報で Citrix Cloud にサインインします。

2. Citrix Cloud コンソールの［マイサービス］で、[Content Collaboration］タイルに移動して［管理］をクリックします。「**Content Collaboration** アカウントが見つかりません」というメッセージが表示されます。



3. ［別のアカウントをリンクする］を選択します。
4. リンクする Content Collaboration アカウントを選択し、［アカウントをリンクする］をクリックします。



ShareFile をセットアップ

June 15, 2021

ShareFile アカウントを作成またはリンクしたら、次のタスクを実行します:

1. 管理者をプロビジョニングする
2. ユーザーをプロビジョニングする
3. Active Directory ユーザーを ShareFile にインポートする
4. 認証を構成する

管理者のプロビジョニング

まず、管理者をプロビジョニングする必要があります。アカウントが作成されると、マスター管理者アカウントにプロビジョニングされます。これは、Citrix Cloud アカウントに追加される最初の管理者です。次に、追加の管理者をプロビジョニングできます。Citrix Cloud 内でプロビジョニングされた追加の管理者は、ShareFile に追加され、管理者アクセス権が付与されます。

ユーザーのプロビジョニング

新しい ShareFile アカウントの使用を開始するには、ユーザーを追加して認証を構成する必要があります。Citrix Cloud 環境では、異なるコンポーネント間で SSO を有効にできます。エンドユーザーにシームレスなエクスペリエンスを提供するためには、SAML を使用して Active Directory ユーザーアカウントに対して認証を行います。

Active Directory ユーザーの **ShareFile** へのインポート

ShareFile User Management Tool（UMT）を使用すると、Active Directory ユーザーを ShareFile に簡単に追加できます。このツールで、ユーザーアカウントをプロビジョニングし、Active Directory（AD）から配布グループを作成できます。

Active Directory からユーザーをインポートするには時間がかかり、リソースが過剰に消費されます。これを軽減するために、特定の時間にツールを実行するようにスケジュールできます。最初のインポートに加えて、このツールで ShareFile ユーザーを AD ユーザーと同期させることもできます。

UMT について詳しくは、「User Management Tool によるポリシーベースの管理」を参照してください。

認証の構成

ユーザーを ShareFile にインポート後、認証を構成する必要があります。Citrix Cloud 環境では、シングルサインオン（SSO）を使用できます。SSO では SAML プロトコルが使用されます。この環境では、ADFS を使用するか、Endpoint Management の SAML 認証を使用するかの 2 つのオプションで SAML を構成できます。

ADFS で認証を構成する

ShareFile アカウントを Active Directory（AD）に統合して、AD 資格情報によるユーザーのシングルサインオンを有効にできます。ShareFile はシングルサインオン用の SAML（Security Assertion Markup Language）をサポートしています。既存の SAML ベースのフェデレーションツールと ShareFile が通信するように構成します。この場合、ユーザーのログオン要求が Active Directory にリダイレクトされます。既存の Web アプリケーションで使用している SAML ID プロバイダーをそのまま使用できます。詳しくは、「ShareFile Single Sign-On SSO」を参照してください。

Endpoint Management で **Active Directory** への認証を構成する

Endpoint Management および Citrix Gateway を、ShareFile の SAML ID プロバイダーとして構成できます。この構成では、ユーザーが、Web ブラウザーまたはほかの ShareFile クライアントを使用して ShareFile にログオンしている場合、ユーザー認証のため Endpoint Management 環境にリダイレクトされます。Endpoint Management で認証された後、ユーザーは ShareFile アカウントへのログオンに有効な SAML トークンを受信します。詳しくは、「Citrix Gateway を使用した ShareFile のシングルサインオン」を参照してください。

ShareFile へのアクセス

ユーザーと認証の構成後、ShareFile にアクセスする方法を選択します。アクセス方法には、管理者アクセスとユーザーアクセスの 2 種類があります。

管理者アクセス

管理者は、ShareFile の構成を変更するか、アカウントを管理する必要があります。

Citrix Cloud 経由で **Content Collaboration** 管理者 **UI** にアクセスする

Citrix Cloud 経由で Content Collaboration Web UI に直接アクセスできます。Citrix Cloud 経由のアクセスでは、ShareFile Web UI の縮小版が提供されます。これには、ユーザーのアクセスを構成してアカウントをセットアップするために必要な要素がすべて含まれています。

Citrix Cloud コンソールから Content Collaboration 管理者 UI にアクセスするには、Citrix Cloud メニューで［マイサービス］**>**［**Content Collaboration**］を選択します。

ShareFile 管理者 **UI** に直接アクセスする

一部の ShareFile 管理者設定は、Citrix Cloud バージョンのコンソールを使用してアクセス出来ない場合があります。追加の機能が必要な場合は、通常の ShareFile ログインページから ShareFile アカウントに直接アクセスできます。`https://YourSubdomain.sharefile.com`に移動して、ログインページにアクセスします。

> 注:
>
> これは、Citrix Cloud 環境の ShareFile 管理者 UI にアクセスする方法としてお勧めしません。

ユーザーアクセス

ユーザーが ShareFile でデータにアクセスする方法には、3 つのオプションがあります。Web UI を使用して直接データにアクセスできます。その他の 2 つのオプションは、有効になっている他のアプリケーションによって異なります。Citrix Virtual Apps and Desktops、または Endpoint Management が有効になっている場合、ユーザーはこれらのアプリケーションの１つを介してデータにアクセスできます。

Web UI 経由で **ShareFile** にアクセスする

エンドユーザーは以下に移動して、直接 ShareFile にアクセスできます: `http://YourSubdomain.sharefile.com`

Citrix Virtual Apps and Desktops を使用して **ShareFile** にアクセスする

Citrix Virtual Apps and Desktops で ShareFile にアクセスするには、Citrix Files for Windows を使用します。Citrix Files を使用すると、マップされたドライブを介して ShareFile のファイルに直接アクセスし、ネイティブの Windows エクスプローラエクスペリエンスを提供できます。

Citrix Files for Windows の使用

Citrix Virtual Apps and Desktops では、Citrix Files for Windows を使用します。Citrix Files for Windows は、エンドユーザーに展開する前にデスクトップイメージに事前インストールできます。アプリを一度インストールすると、環境内のすべての Citrix Virtual Apps and Desktops セッションに反映させることができます。Citrix Files for Windows の使用について詳しくは、次の記事を参照してください:

- Citrix Virtual Apps and Desktops 上の Citrix Files
- CTX228273: Citrix Files for Windows をインストールして使用する

Endpoint Management を使用して **ShareFile** にアクセスする

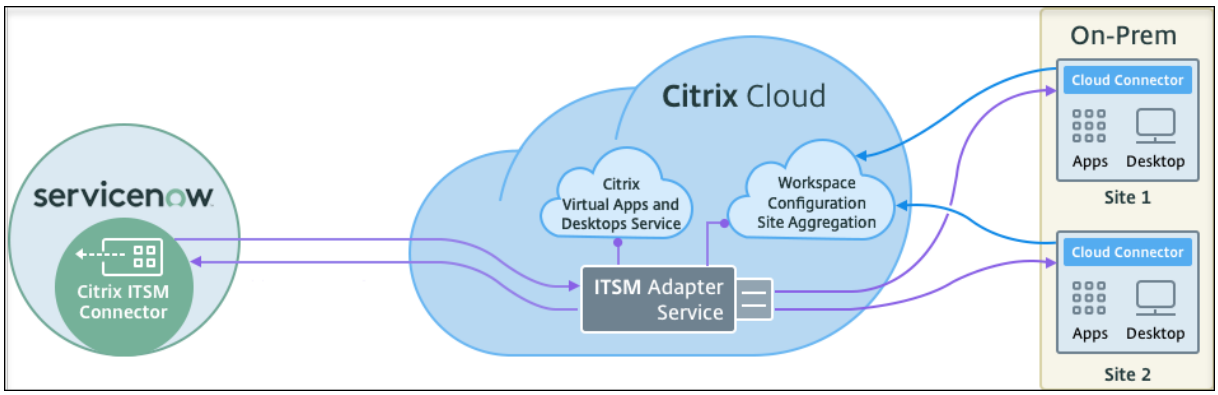
ShareFile アプリケーションをラップし、Single Sign-On を Endpoint Management と ShareFile の間に展開する方法については、「Citrix ShareFile for Endpoint Management」を参照してください。

IT サービス管理（ITSM）アダプター

September 17, 2021

概要

ITSM アダプターは Citrix Cloud サービスです。ITSM コネクタが ServiceNow にインストールされているため、ITSM アダプターを使用すると ServiceNow の機能を Citrix Virtual Apps and Desktops（CVAD）環境に簡単に拡張できます。ITSM アダプターは、Citrix Cloud に接続するクラウドサイトとオンプレミスサイトの両方を自動化および管理するためのワークフローを提供し、IT チームが戦略的プロジェクトに集中できるようにします。



ITSM アダプターが ServiceNow と通信できるようにするには、次の IP アドレスのいずれかを ServiceNow インスタンスの許可リストに追加します:

ITSM アダプターリージョン	IP アドレス
米国	52.158.218.132/30
EU	20.54.214.12/30
アジア太平洋	20.195.2.68/30

新機能

2021 年 **8** 月

- ITSM コネクタのバージョンを 2106.1.1 から 2108.1.0 に更新しました。
- ServiceNow の Citrix ITSM コネクタのグローバルナビゲーションを再構築しました。たとえば、Citrix Virtual Apps and Desktops（CVAD）の配信を単一の **Studio** ダッシュボードに集約し、以前のナビゲーションメニューの一部の名前を変更しました。以前の［**Requests**］、［**Reporting**］、［**Alerts**］、［**Settings**］、および［**Alert Policies**］メニューは、それぞれ［**User Requests**］、［**Statistics Report**］、［**Alerts and Notifications**］、［**Configurations**］、および［**CVAD Alert Policies**］という名前になりました。ナビゲーションメニュー［**Citrix Cloud Notification Policies**］も追加しました。
- Citrix Cloud に ServiceNow インスタンスを追加するプロセスを簡素化しました。詳しくは、本記事の「手順 4: ServiceNow インスタンスを Citrix Cloud に追加する」を参照してください。
- ユーザーリクエストに使用できるアプリケーションを設定できるようになりました。リクエスト一覧でアプリケーションを非表示にする場合は、**Studio** ダッシュボードの［**Published Applications**］タブで該当のアプリケーションを見つけ、選択し、［**Disable availability for requests**］操作を選択します。リクエスト一覧にアプリケーションを表示するには、アプリケーションを選択して、［**Enable availability for requests**］を選択します。詳しくは、本記事の「Studio ダッシュボード」を参照してください。
- 関心のある Citrix Cloud 通知をサブスクライブできるようになりました。詳しくは、本記事の「ServiceNow 内から Citrix Cloud 通知へのアクセス」を参照してください。
- Citrix Virtual Apps and Desktops サービスでホストされている VDI デスクトップから、アイドル状態のリソースを解放できるようになりました。詳しくは、本記事の「Studio ダッシュボード」を参照してください。

2021 年 **6** 月

- ITSM コネクタのバージョンを 1.8.0 から 2106.1.1 に更新しました。
- サービスオプションが拡張され、リクエストされたマシンカタログにマシンが不足している場合に、MCS で作成したマシンを追加できるようになりました。スケールアウトするマシンカタログは、Citrix Virtual Apps and Desktops サービスでホストされている必要があります。詳しくは、「MCS で作成されたマシンの追加」を参照してください。

2021 年 **4** 月

- ITSM アダプターサービスは ServiceNow Quebec をサポートしています。
- Citrix Cloud に ServiceNow インスタンスを追加すると、更新トークンとアクセストークンが自動的に生成されるように機能が拡張されました。この機能拡張により、別のツールを使用してトークンを生成する必要がなくなります。詳しくは、「手順 4: ServiceNow インスタンスを Citrix Cloud に追加する」を参照してください。
- Citrix Virtual Apps and Desktops サービスで設定した Citrix アラートポリシーと ServiceNow を［**Citrix IT Service Management Connector**］**>**［**Settings**］**>**［**Alert Policies**］で同期しました。アラートポリシーの Webhook モニターを有効にすると、［**Citrix IT Service Management Connector**］**>**［アラート］の ServiceNow にポリシーを満たすアラートが一覧表示されます。インシデントを作成して、特定の担当者に割り当てることもできます。ServiceNow でアラートポリシーを無効にするには、［**Disable Monitor**］をクリックします。詳しくは、「ServiceNow 内から Citrix アラートへのアクセス」を参照してください。

2020 年 **11** 月

- ITSM アダプターサービスの展開を簡素化しました。
- ITSM アダプターサービスに、要求統計を表示するための ［レポート］ダッシュボードを追加しています。
- ITSM アダプターサービスに、アプリケーションアクセス要求を処理するときに ServiceNow 管理者が選択できるよう、［アプリケーショングループにユーザーを追加］タブを追加しています。
- 特定のアプリケーションへのアクセスを、Active Directory グループ内の特定のユーザーに制限できます。制限を設定しやすくするため、ITSM アダプターサービスの ［ユーザーを **Active Directory** グループに追加］タブに、特定のアプリケーションにアクセスできるすべての Active Directory グループを表示します。ServiceNow 管理者は、アプリケーションアクセス要求を処理するときに、この Active Directory グループにユーザーを追加できます。

2020 年 **6** 月

- ITSM アダプターサービスは ServiceNow New York をサポートしています。
- ITSM アダプターサービスは、ユーザープリンシパル名（UPN）を実装して、Active Directory（AD）ユーザーが、メールアドレスのような形式でサインオンできるようにします。

ITSM アダプターサービスのオンボード

ITSM アダプターサービスのオンボードには、次の 5 つの手順があります:

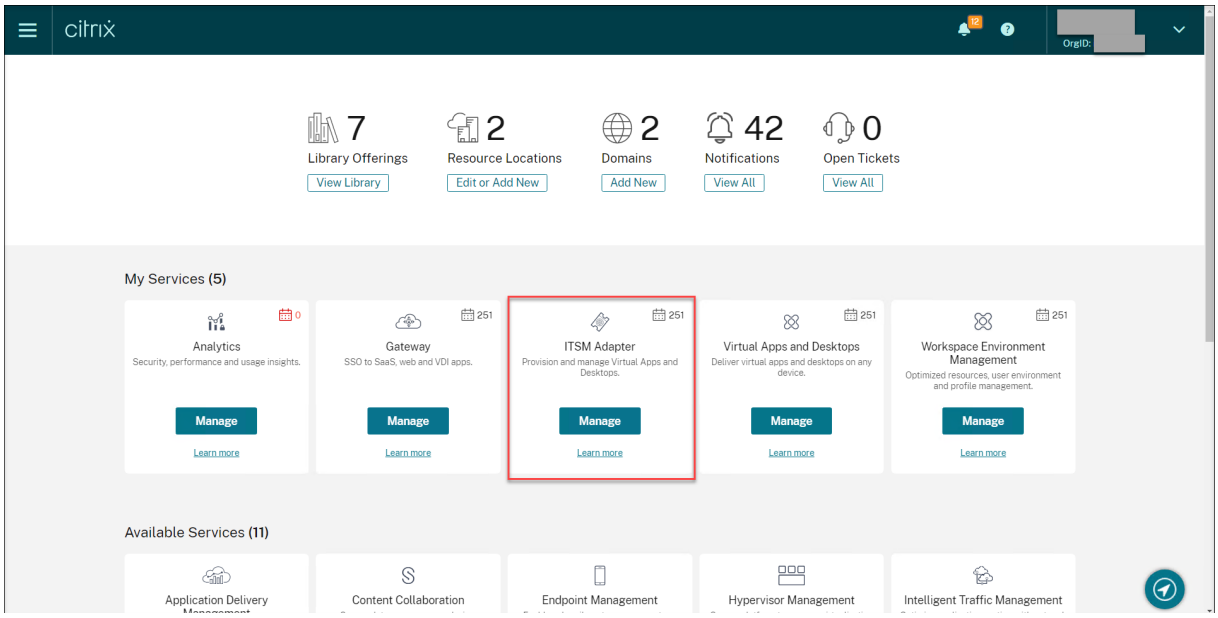
1. Citrix Virtual Apps and Desktops サービスにサブスクライブしていることを確認する
2. ServiceNow で ITSM コネクタを構成する

3.（オプション）サイトアグリゲーションでオンプレミスサイトを Citrix Cloud に追加する
4. ServiceNow インスタンスを Citrix Cloud に追加する
5. エンドユーザーがアクセスできるように、ITSM アダプターサービスを ServiceNow ポータルに公開する

> 注：
>
> 次の手順に進む前に、ServiceNow 管理者と Citrix 管理者の権限があることを確認してください。
>
> - ServiceNow 管理者は、ServiceNow Orchestration プラグインをアクティブ化し、ITSM コネクタプラグインをダウンロードしてインストールする権限を持つことができます。また、ServiceNow で ITSM コネクタプラグイン構成できる x_cion_citrix_it_s.ctx_itsm_admin 役割を与えることができます。
> - Citrix 管理者は、Citrix Virtual Apps and Desktops サービスポータルにアクセスして、次のように必要な構成を実行できます。

手順 **1**：**Citrix Virtual Apps and Desktops** サービスにサブスクライブしていることを確認する

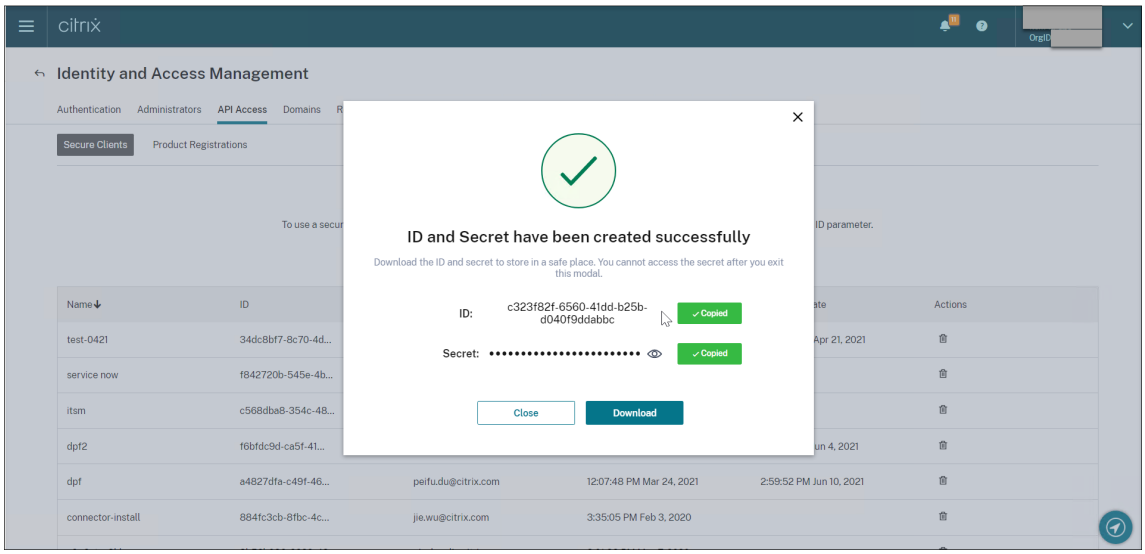
Citrix の資格情報で Citrix Cloud にサインインするか、新しいアカウントを登録します。無料のお試し版に正常にサインアップした場合、または Citrix Virtual Apps and Desktops サービスにサブスクライブした場合は、次のスクリーンショットのように ITSM アダプターサービスを表示できます。それ以外の場合は、Citrix の担当者に確認してください。



> ヒント：
>
> ユーザーアカウントに使用権が割り当てられると、［管理］ボタンを使用できるようになります。その前は、［デモのリクエスト］が表示されます。

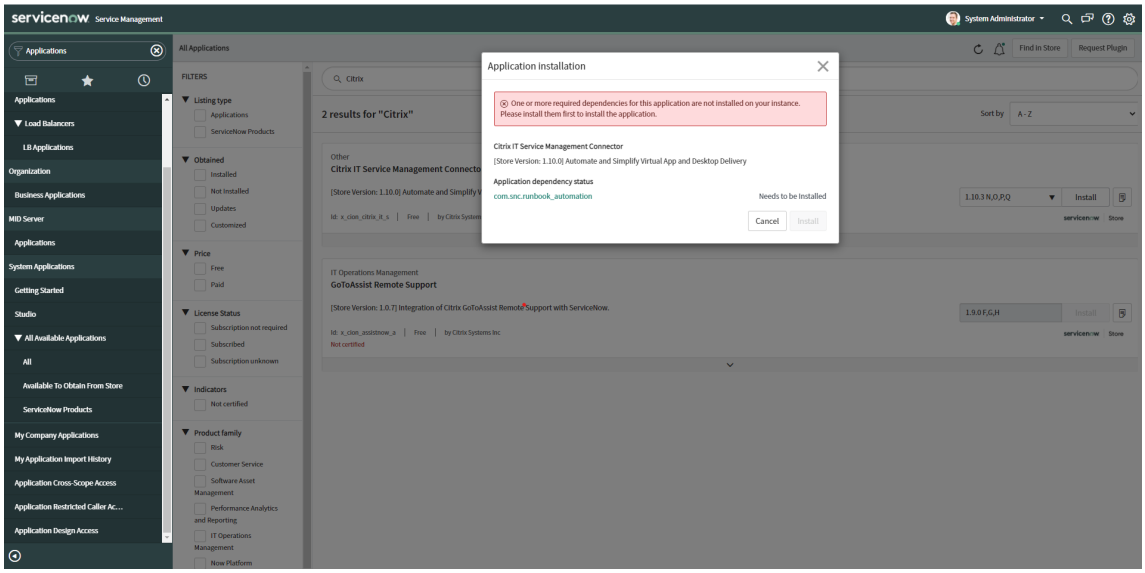
手順 **2**: **ServiceNow** で **Citrix ITSM** コネクタを構成する

1. Citrix Cloud に移動し、Citrix Cloud に ITSM アダプターサービスをオンボードするためのセキュアクライアントを作成します。セキュアクライアント ID とシークレットを記録しておきます。詳しくは、「Citrix Cloud API の使用を開始する」を参照してください。

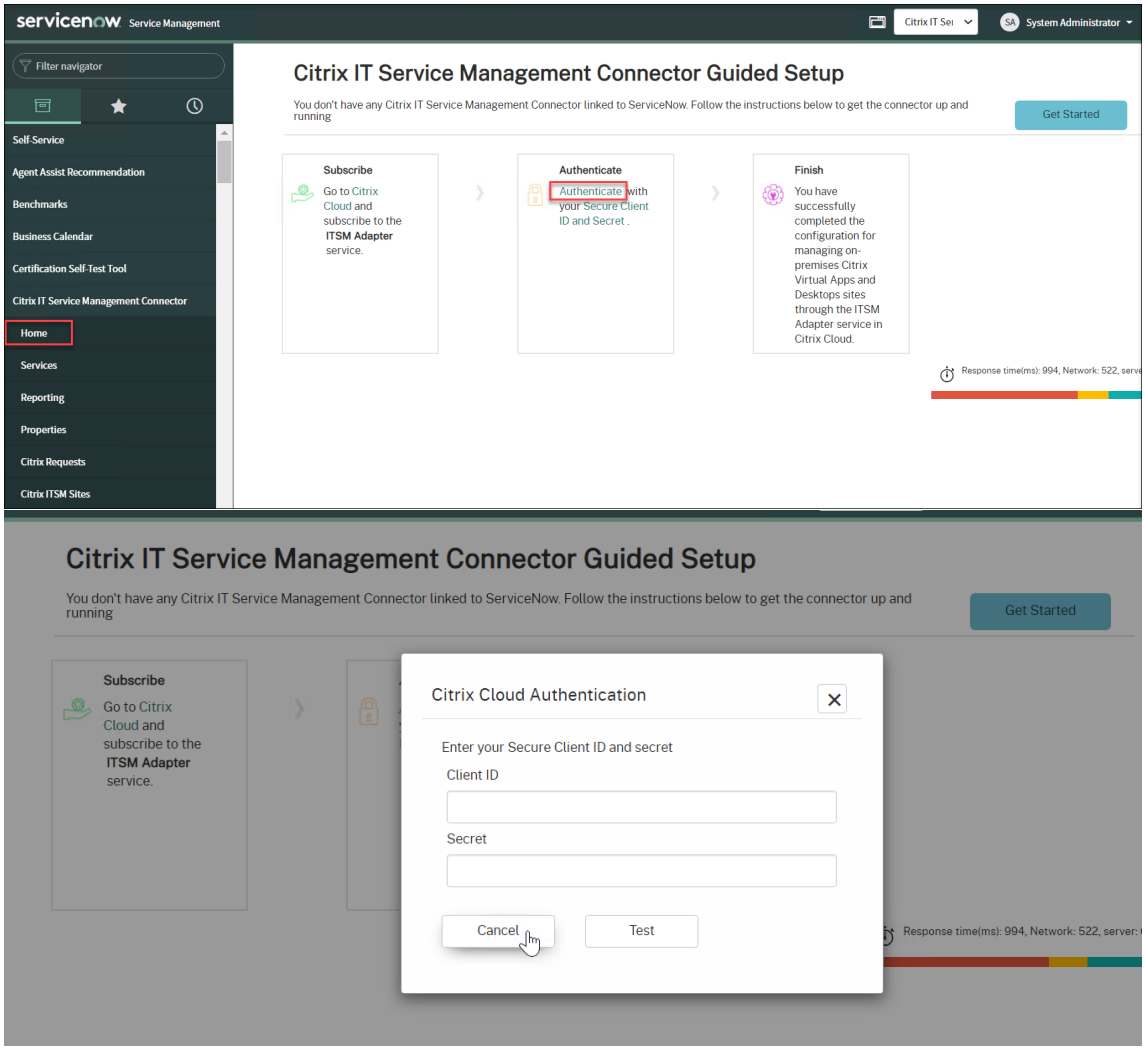


2. ServiceNow HI ポータルアカウントがあり、ServiceNow 管理者権限があることを確認してください。
3. ServiceNow オーケストレーションプラグインがアクティブになっていることを確認します。

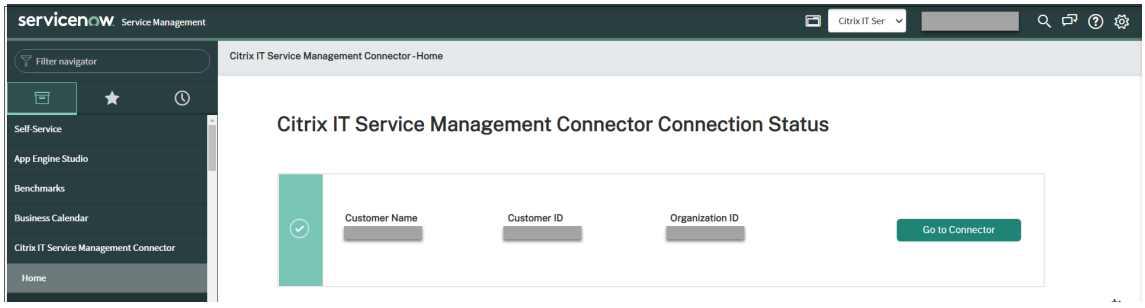
   ServiceNow インスタンスに必要な依存関係がない場合は、インストールするように求められます。



4. ServiceNow ストアから Citrix ITSM コネクタをダウンロードしてインストールします。
5. **Citrix IT Service Management Connector** ペインで、［ホーム］を選択し ［認証］をクリックします。セキュアクライアント ID とシークレット（Citrix Cloud から生成されたプロキシ資格情報）を入力します。

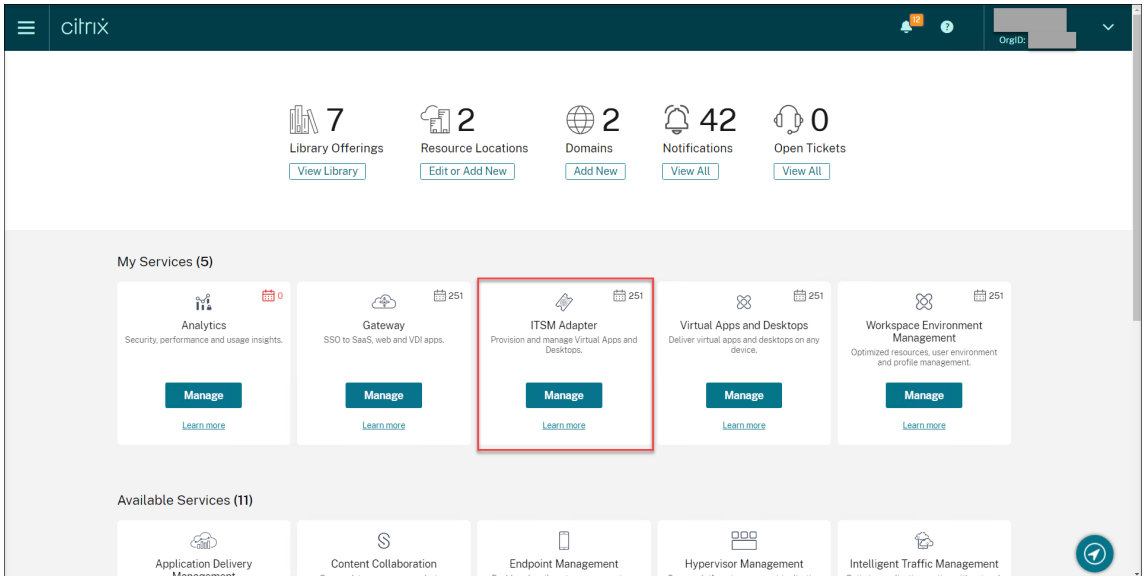


6. 接続をテストします。
7. 構成を保存します。接続が稼働中であることを示す ServiceNow からの受信確認が表示されます。

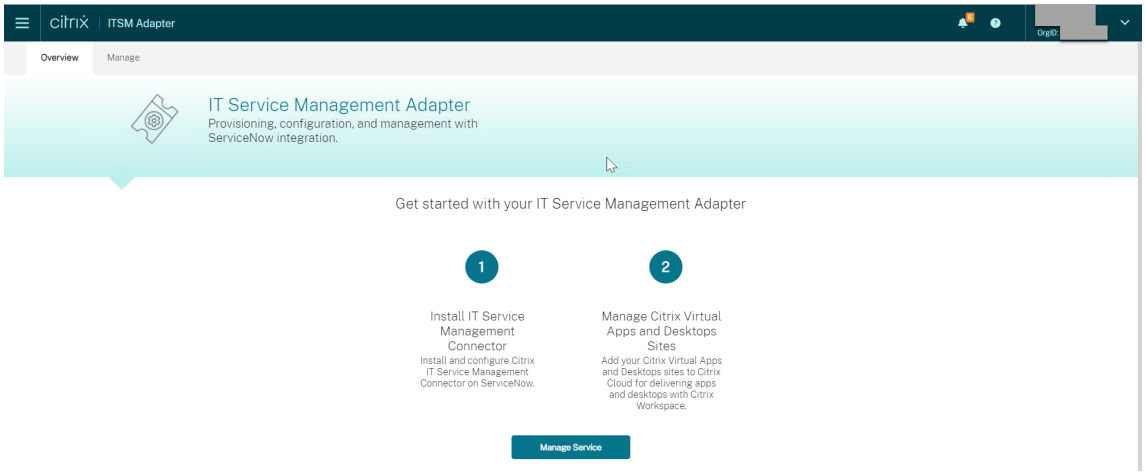


（オプション）手順 **3**：サイトアグリゲーションでオンプレミスサイトを **Citrix Cloud** に追加する

1. Citrix Cloud に移動し、ITSM アダプターサービスにアクセスします。



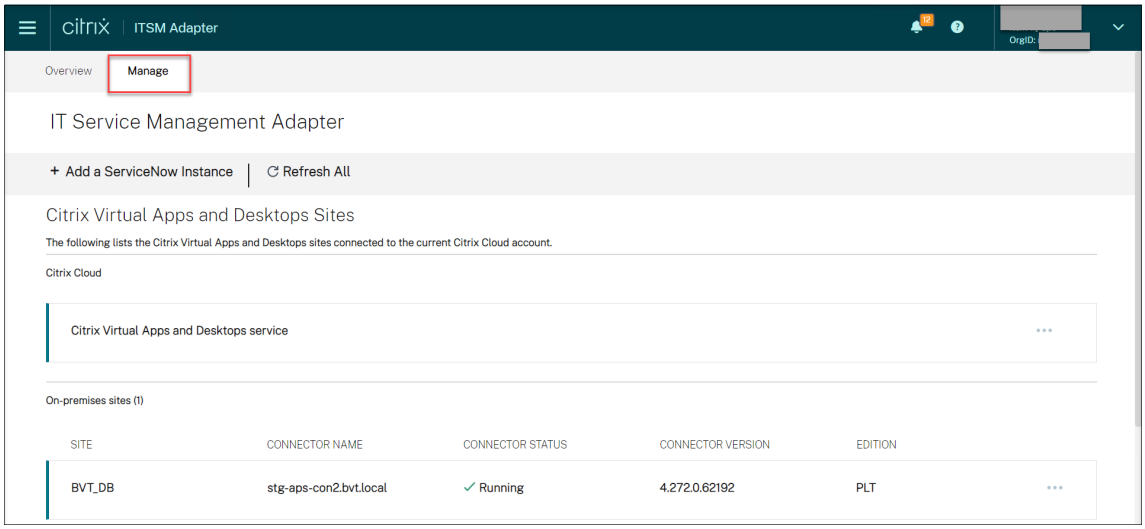
2. 青い ［管理］ボタンをクリックします。［概要］タブが表示されます。



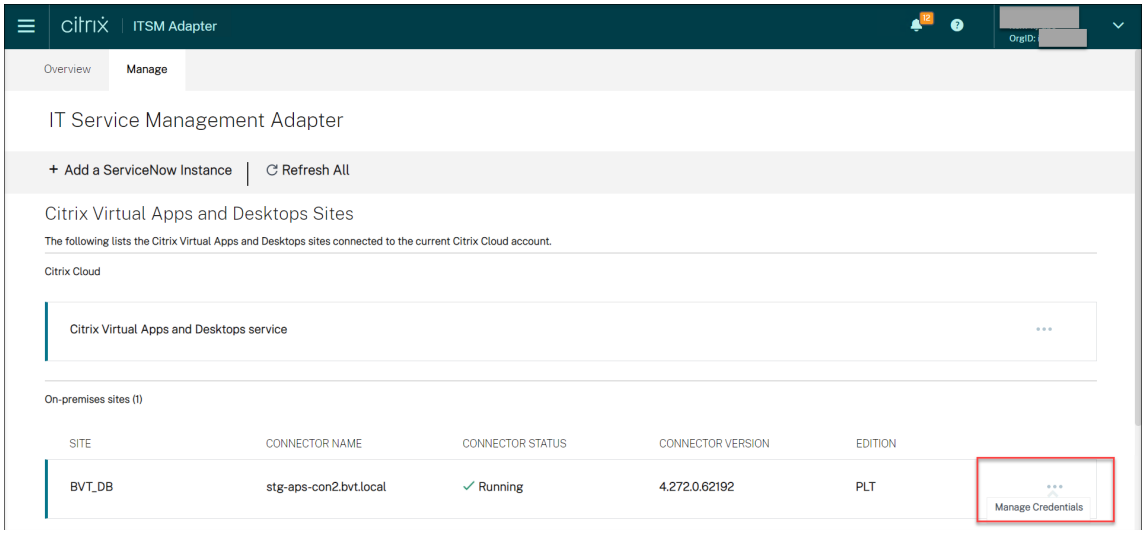
3. ［管理］タブをクリックします。［**Manage**］タブには、現在の Citrix Cloud アカウントに接続されている Citrix Virtual Apps and Desktops サイトが表示されます。

   Citrix Virtual Apps and Desktops サービスに既にサブスクライブしている場合、サービスサイトが自動的に一覧表示されます。サービスサイトの横のドットメニューで ［**Enable Integration**］または ［**Disable Integration**］を選択してサービスサイトの管理を有効または無効にできます。

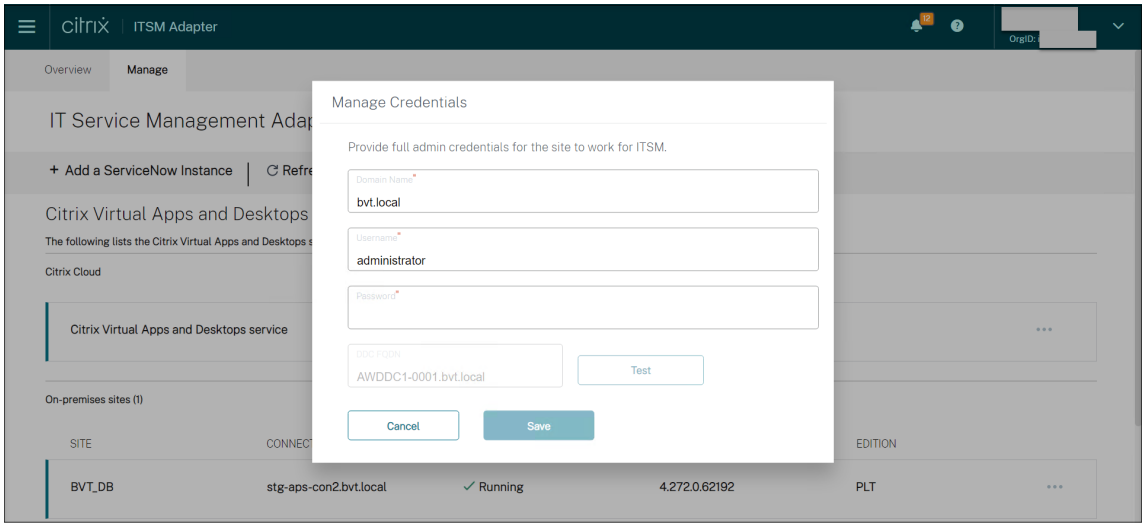
   管理しようとしているオンプレミスサイトが一覧に表示されない場合は、サイトアグリゲーションにより追加する必要があります。



4. サイトアグリゲーションによりオンプレミスサイトを追加します。
5. 新しく追加されたオンプレミスサイトの場合は、ドットメニューから ［資格情報の管理］を選択します。



6. サイトの完全な管理者資格情報の提供



7. 接続を確認するには、[**Test**] をクリックします。

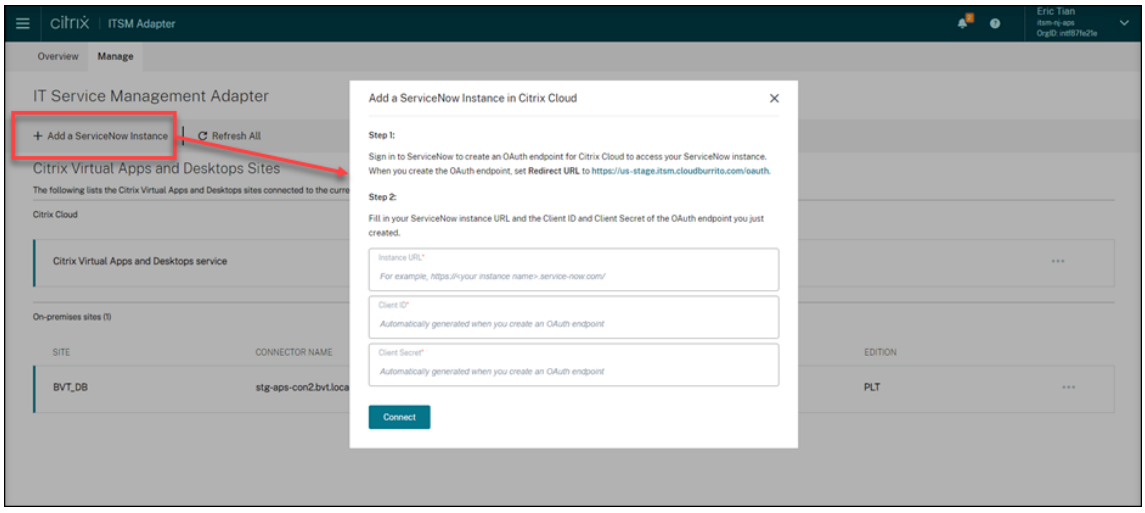
   これでサイトが動作し、ITSM アダプターサービスに接続されました。

8. [保存] をクリックします。

手順 **4**: **ServiceNow** インスタンスを **Citrix Cloud** に追加する

> 注:
>
> この手順は、Citrix Cloud を ServiceNow エンドポイントとして追加して、Citrix Cloud がアラートや通知などのメッセージを ServiceNow に送信できるようにするために必要です。

1. Citrix Cloud の ITSM アダプターサービスの [**Manage**] タブで、[**Add a ServiceNow Instance**] をクリックします。[**Add a ServiceNow Instance in Citrix Cloud**] ダイアログボックスが表示されます。[Manage] タブにアクセスする方法については、「手順 3: サイトアグリゲーションでオンプレミスサイトを Citrix Cloud に追加する」を参照してください。

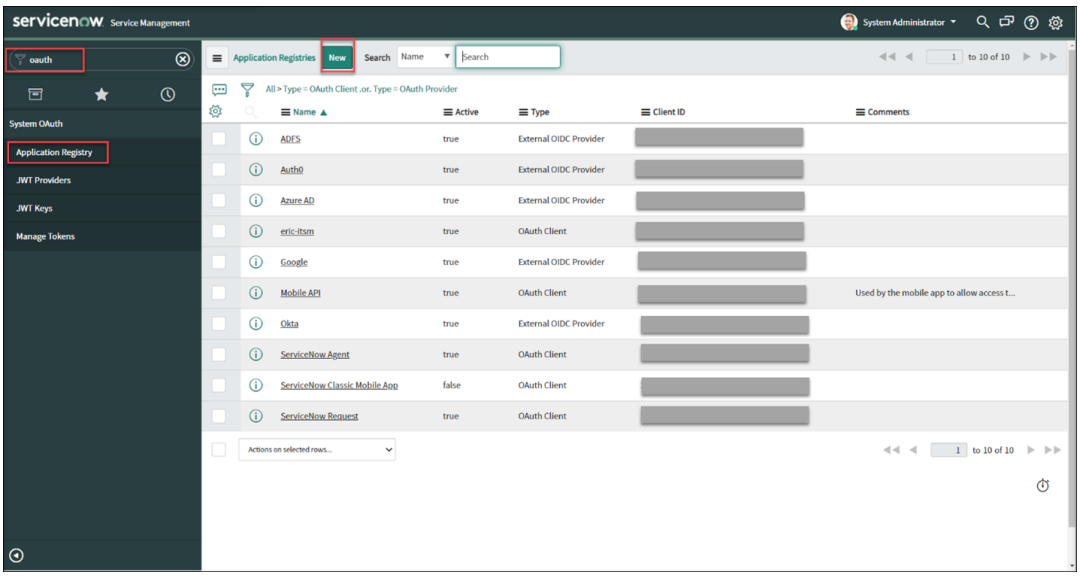


2. [**Add a ServiceNow Instance in Citrix Cloud**] ダイアログボックスの手順に従って、ServiceNow に

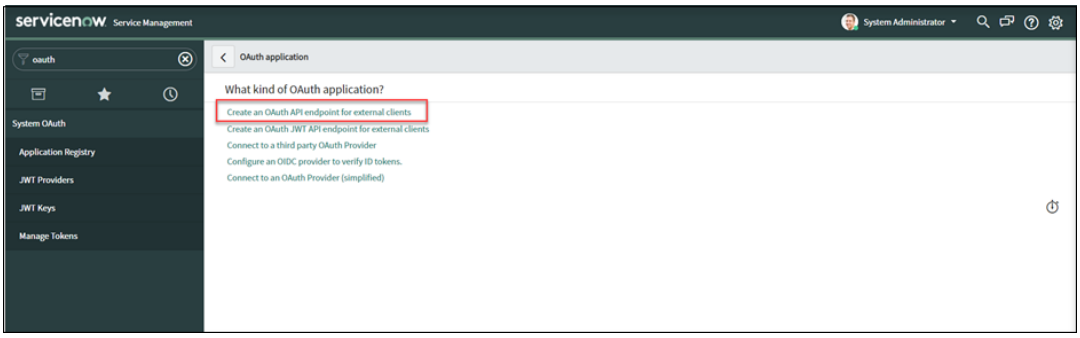
OAuth エンドポイントを作成し、ダイアログボックスに戻ってインスタンス URL、クライアント ID、およびクライアントシークレットを入力します。

a) Web ブラウザーで新しいウィンドウまたはタブを開き、ServiceNow にサインインします。

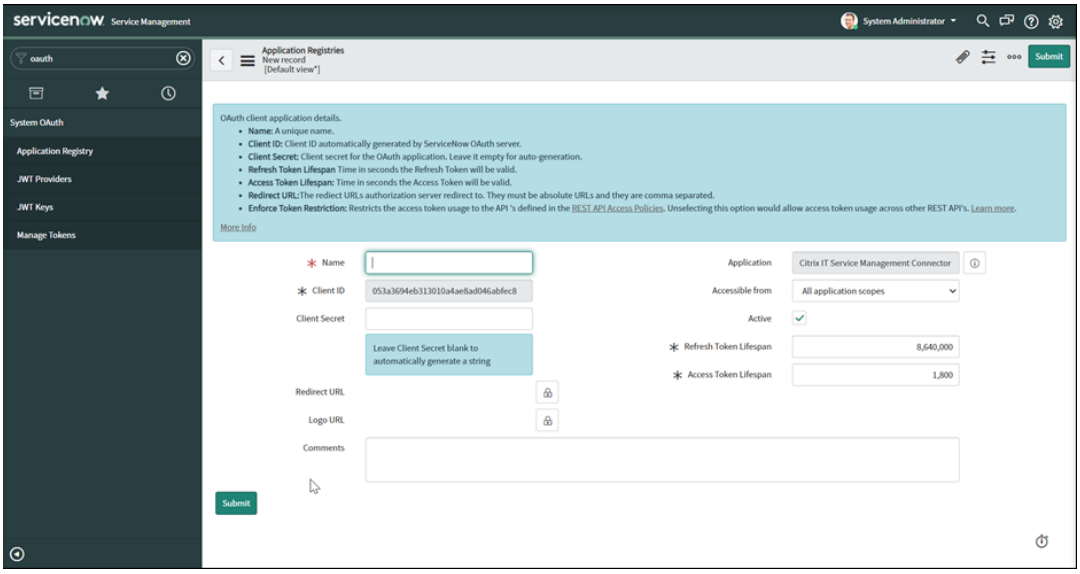
b) エントリを検索して、「**oauth**」などのキーワードで OAuth エンドポイントを作成します。左側のナビゲーションで［**Application Registry**］をクリックし、次に［**Application Registries**］の横にある［**New**］をクリックします。



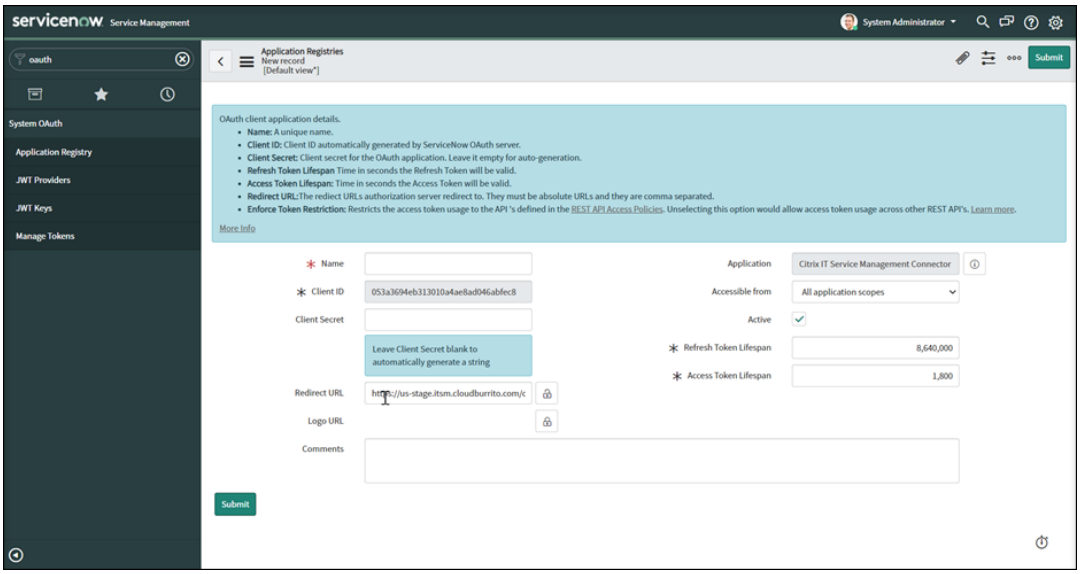
c)［**Create an OAuth API endpoint for external clients**］を選択します。



d) 作成する OAuth エンドポイントに名前を付けます。

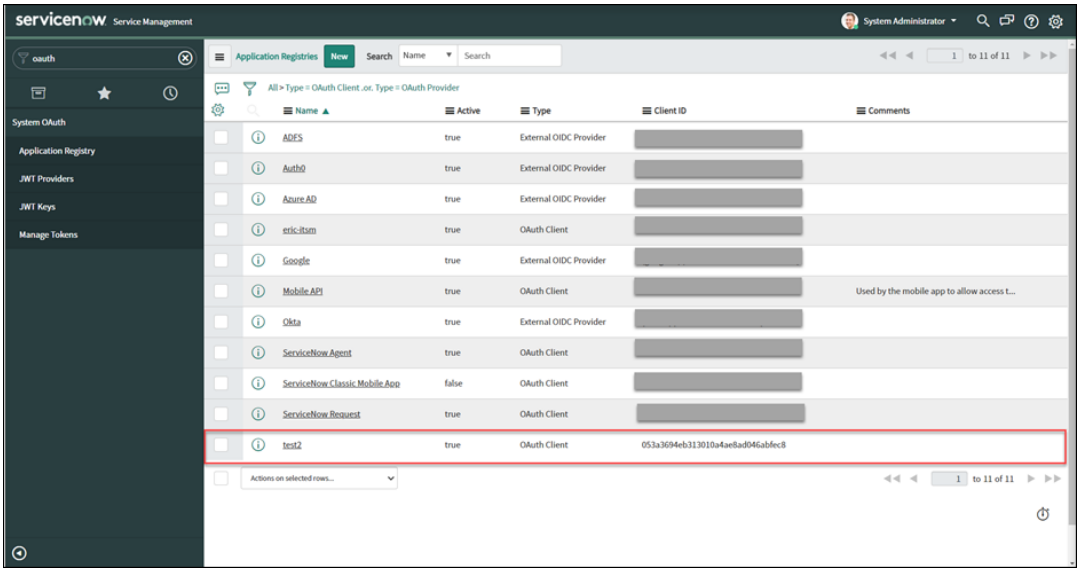


e) [**Redirect URL**] の横にあるロックアイコンをクリックし、前述の [**Add a ServiceNow Instance in Citrix Cloud**] ダイアログボックスで表示される値（この例では「**https://us-stage.itsm.cloudburrito.com/oauth**」）を [**Redirect URL**] に設定します。

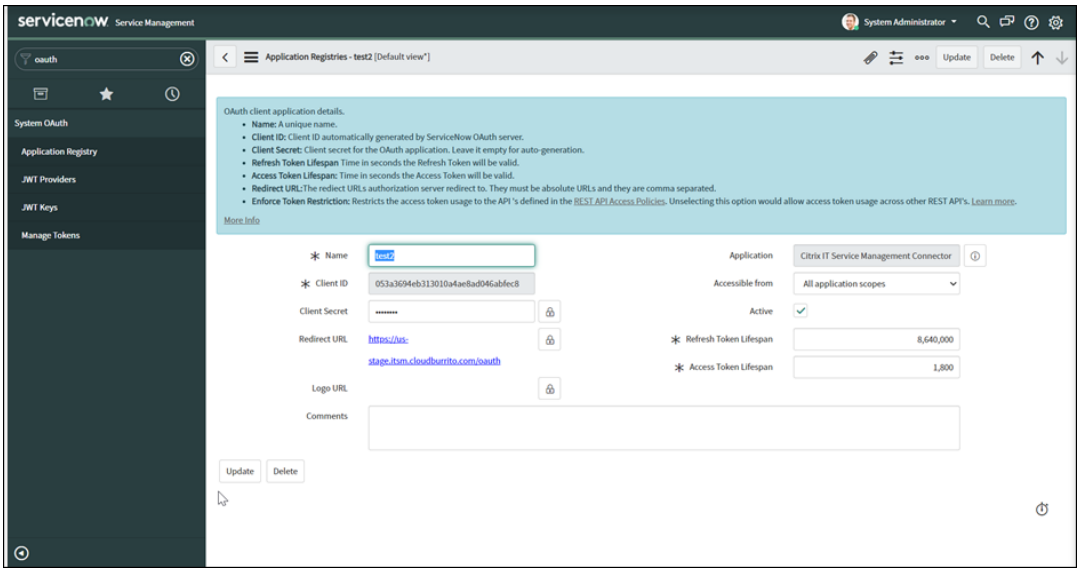


f) [**Summit**] をクリックします。

g) [**Application Registries**] ページに戻ります。作成した OAuth エンドポイントを見つけます。

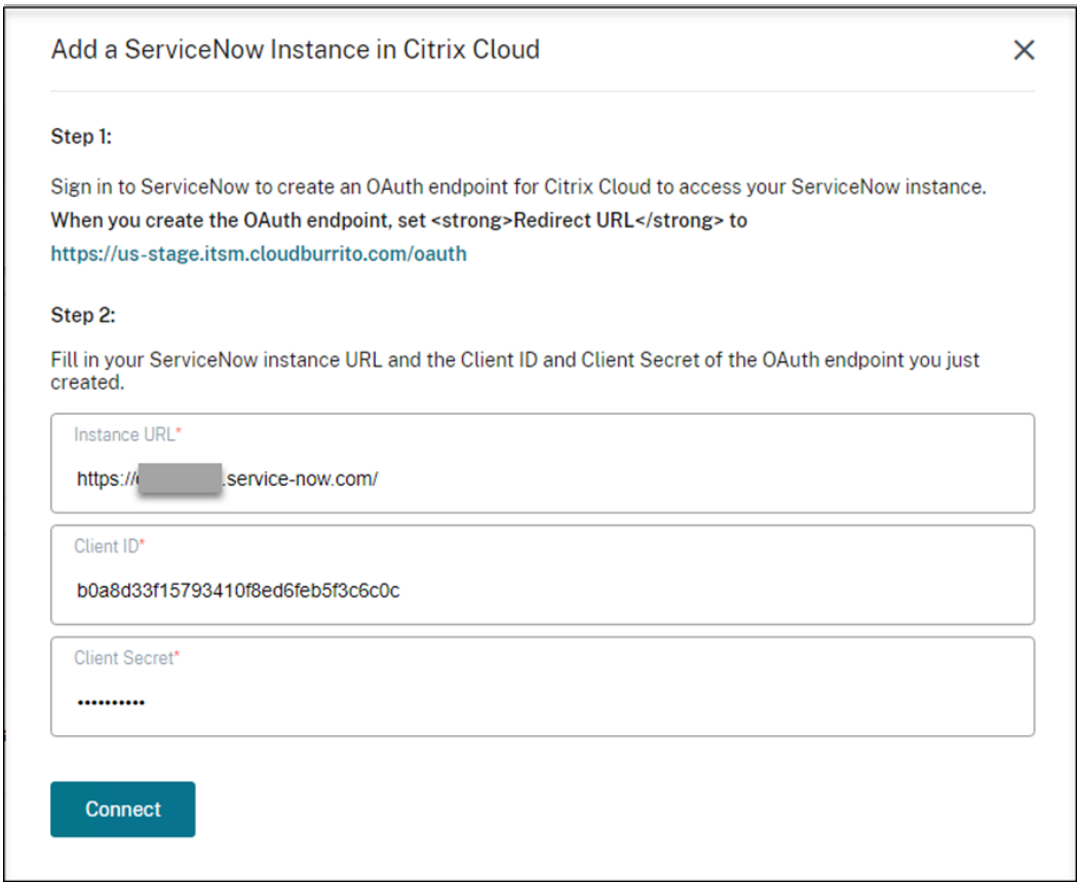


h) OAuth エンドポイント名をクリックして、詳細ページを開きます。

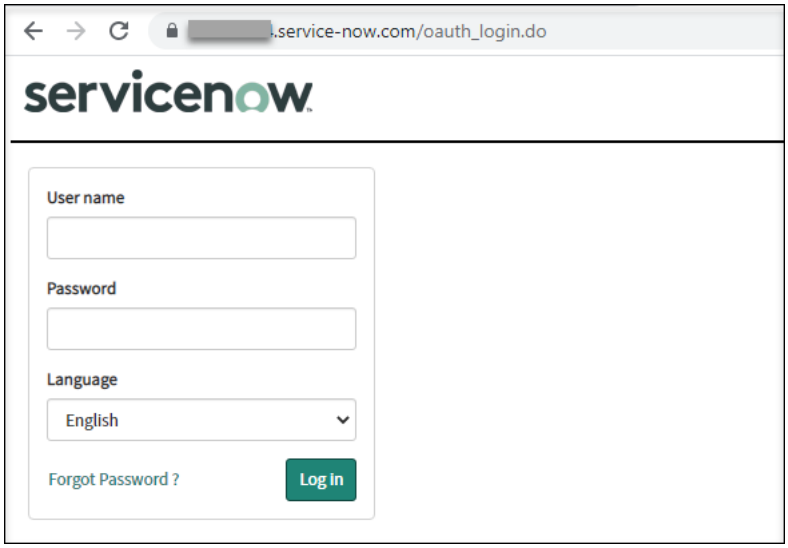


i) ServiceNow インスタンスの URL、および OAuth エンドポイントの［Client ID］と［Client Secret］を記録しておきます。

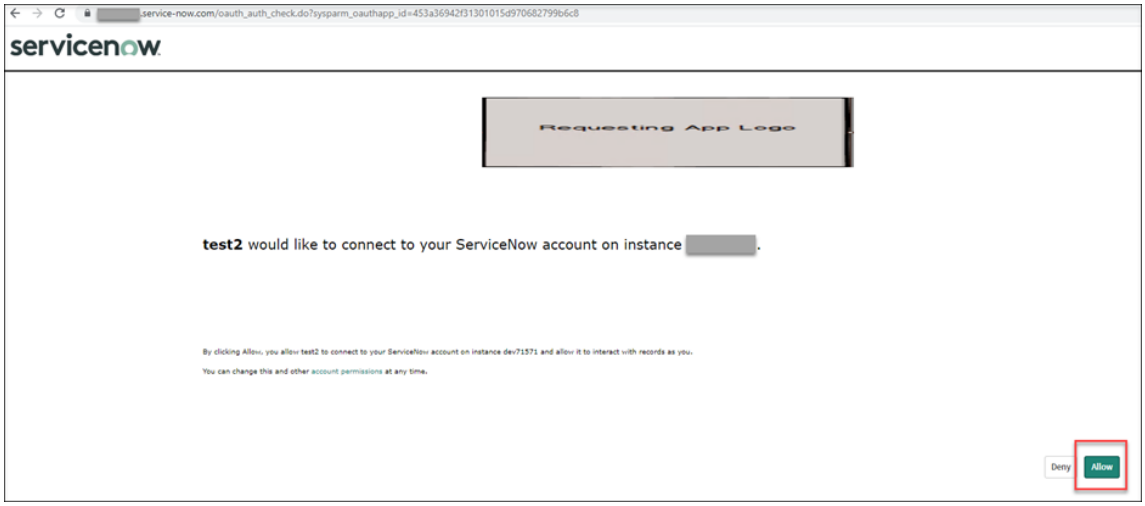
j) ［**Add a ServiceNow Instance in Citrix Cloud**］ダイアログボックスに戻ります。記録しておいた ServiceNow インスタンスの URL、クライアント ID、およびクライアントシークレットを入力します。



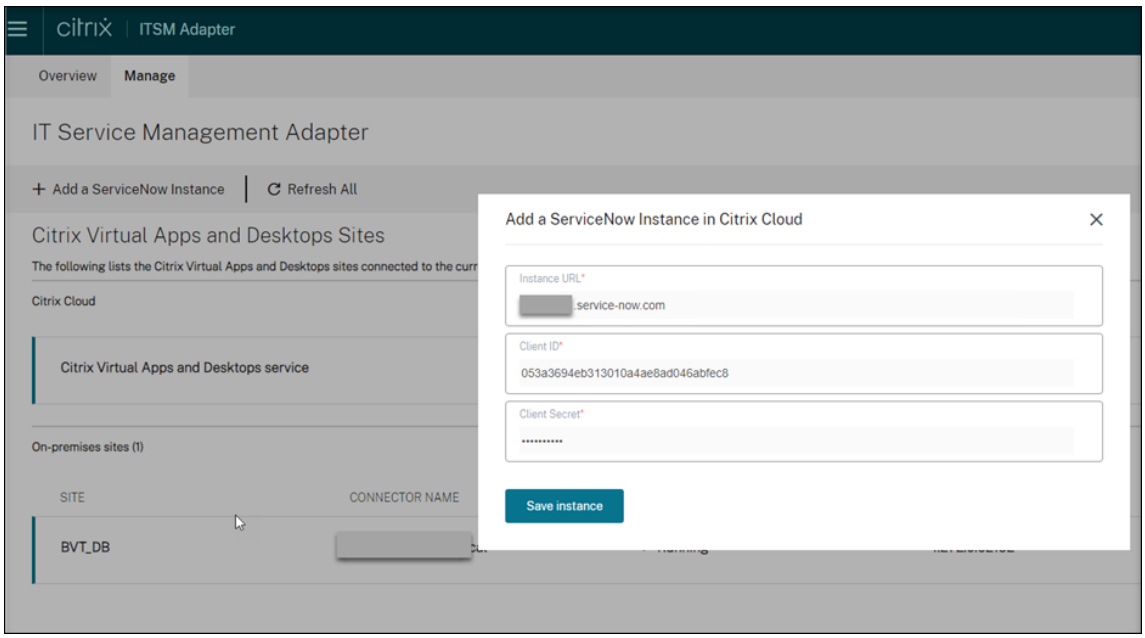
3. ［接続］をクリックします。インスタンスのログインページが開きます。



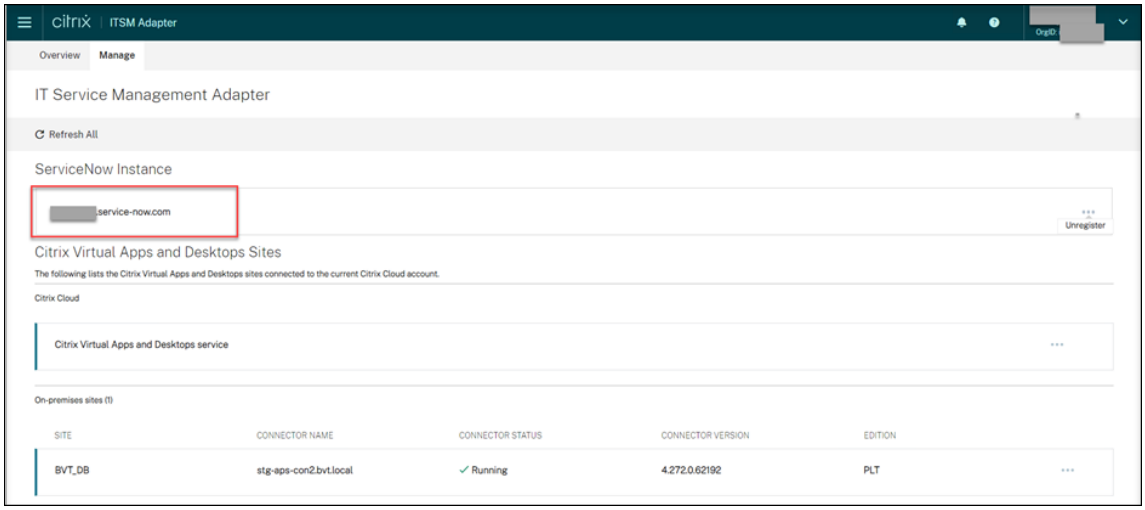
4. ServiceNow インスタンスの資格情報を入力し、［**Log in**］をクリックします。指定された ServiceNow インスタンスの ServiceNow アカウントに接続するために OAuth エンドポイントの許可を要求するページが表示されます。



5. [**Allow**] をクリックします。[**Add a ServiceNow Instance in Citrix Cloud**] ダイアログボックスに戻ります。



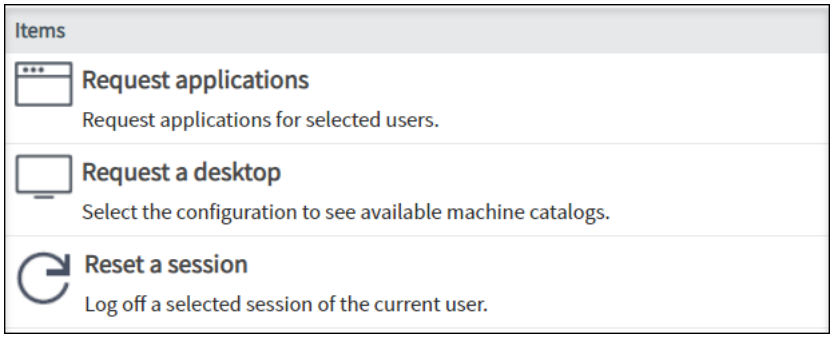
6. [**Save instance**] をクリックします。ITSM アダプターサービスは、ITSM コネクタとの接続のテストを開始します。テストが正常に完了すると、ServiceNow インスタンスの保存が開始されます。ServiceNow インスタンスが正常に保存されると、[**Add a ServiceNow Instance in Citrix Cloud**] ダイアログボックスが自動的に閉じます。



7. （オプション）ServiceNow インスタンスを変更するには、その横にあるドットメニューをクリックし、［**Unregister**］を選択します。その後、必要に応じて別の ServiceNow インスタンスを追加します。

手順 **5**：**ITSM** アダプターサービスを **ServiceNow** で公開する

手順 1～4 を完了すると、ユーザーおよびエンドユーザーは「**Citrix**」で検索して ServiceNow で ITSM アダプターサービスを見つけ、リクエストを送信できるようになります。ユーザーエクスペリエンスを向上させるために、簡単にアクセスできるよう、選択したサービスアイテムを ServiceNow ダッシュボードに公開することをお勧めします。例：

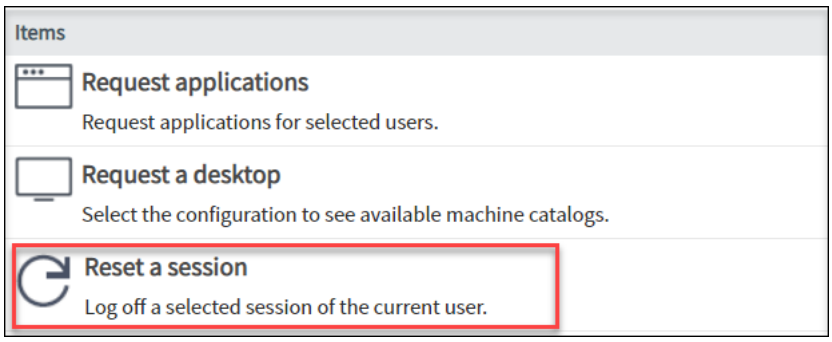


サンプルシナリオ

Reset a session

エンドユーザーの操作

1. ServiceNow インスタンスにログインします。
2. ［**Reset a session**］エントリを見つけます。例：



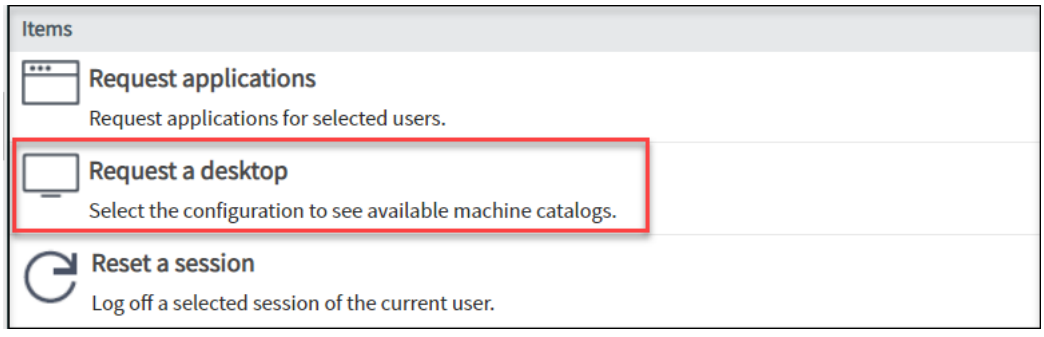
3. [**Reset a session**] ページで、現在のユーザーのデスクトップセッションまたはアプリセッションを選択し、[**Order Now**] をクリックしてセッションからログオフします。

> 注:
>
> プロビジョニングが管理者によるかユーザーによるかに関係なく、セッションで実行されているすべてのアプリケーションがリセットされます。

Request a desktop

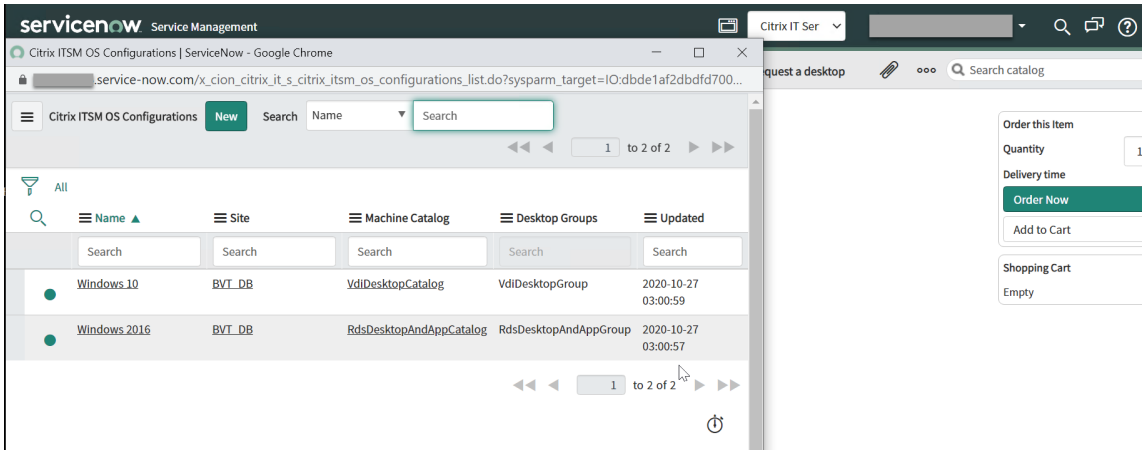
エンドユーザーの操作

1. ServiceNow インスタンスにログインします。
2. [**Request a desktop**] エントリを見つけます。例:



3. [デスクトップのリクエスト] ページで、[構成] エリアの検索ツールを使用して、使用可能なマシンカタログを探します。

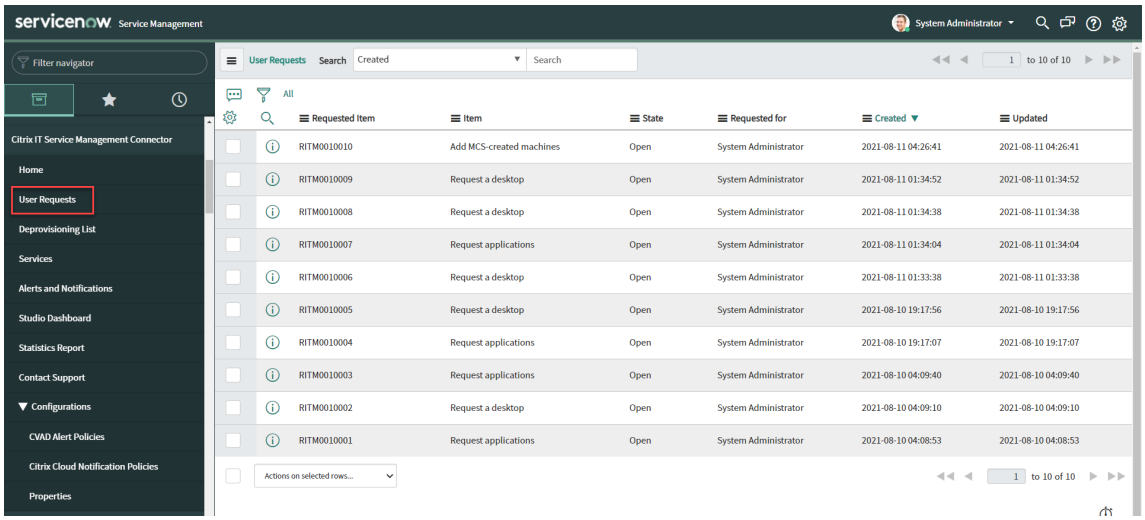
4. 対象のオペレーティングシステムを選択し、[**Quantity**] を設定します。[**Order Now**] をクリックします。



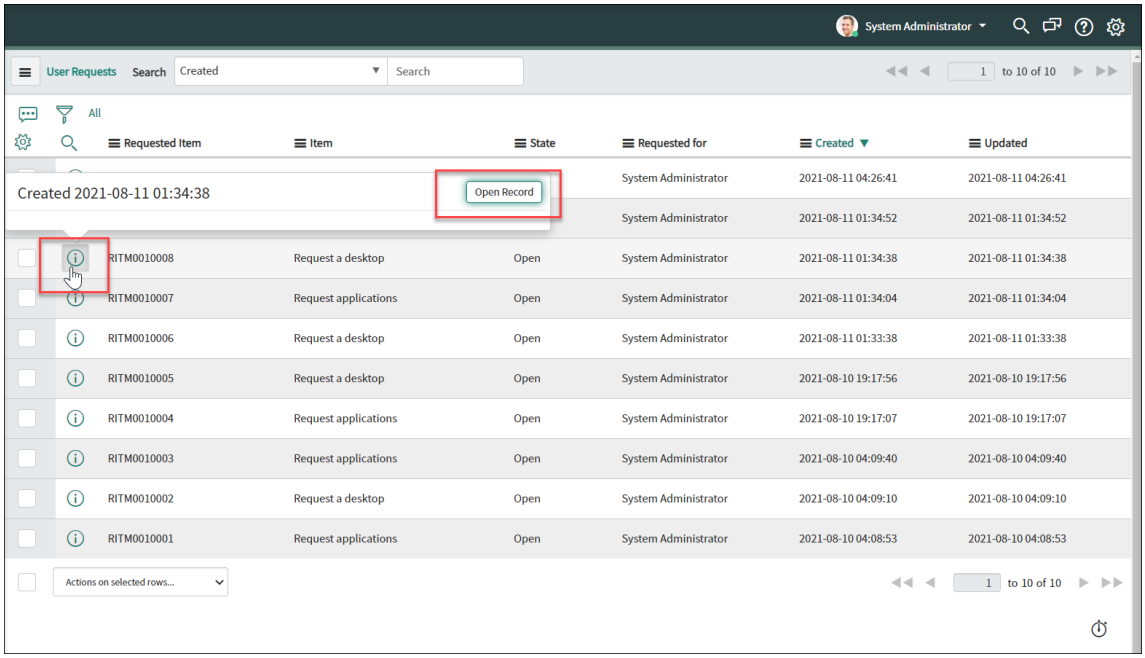
管理者の操作

1. ServiceNow ポータルにログインし、左側ペインの [**Citrix IT Service Management Connector**] に移動し、[**User Requests**] を選択します。

   [**User Requests**] ページにリクエストの一覧が表示されます。

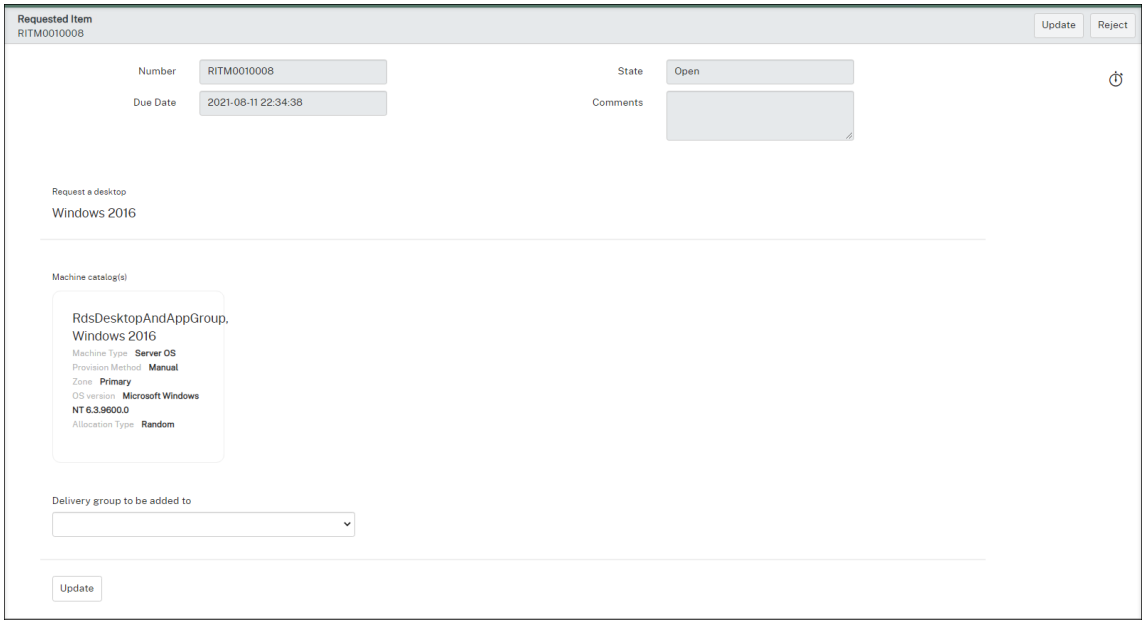


2. リクエスト ID の横にあるアイコン、［**Open Record**］の順にクリックします。リクエストの詳細が表示されます。



3. 最初にマシンカタログを選択してから、一覧からデリバリーグループを選択します。

   リクエストされたマシンカタログでマシンが不足している場合は、MCS を介してマシンをカタログに追加するよう求められます。ハイパーリンクをクリックして、マシン作成リクエストをすぐに作成するか、現在のデスクトップリクエストを閉じてから後でマシン作成リクエストを開始することができます。



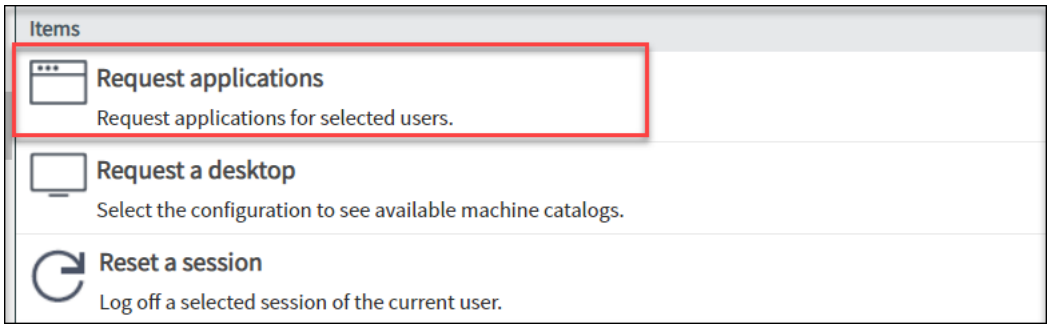
4. ［更新］をクリックします。

これで、リクエストされたデスクトップがプロビジョニングされ、ユーザーに割り当てられました。

Request applications

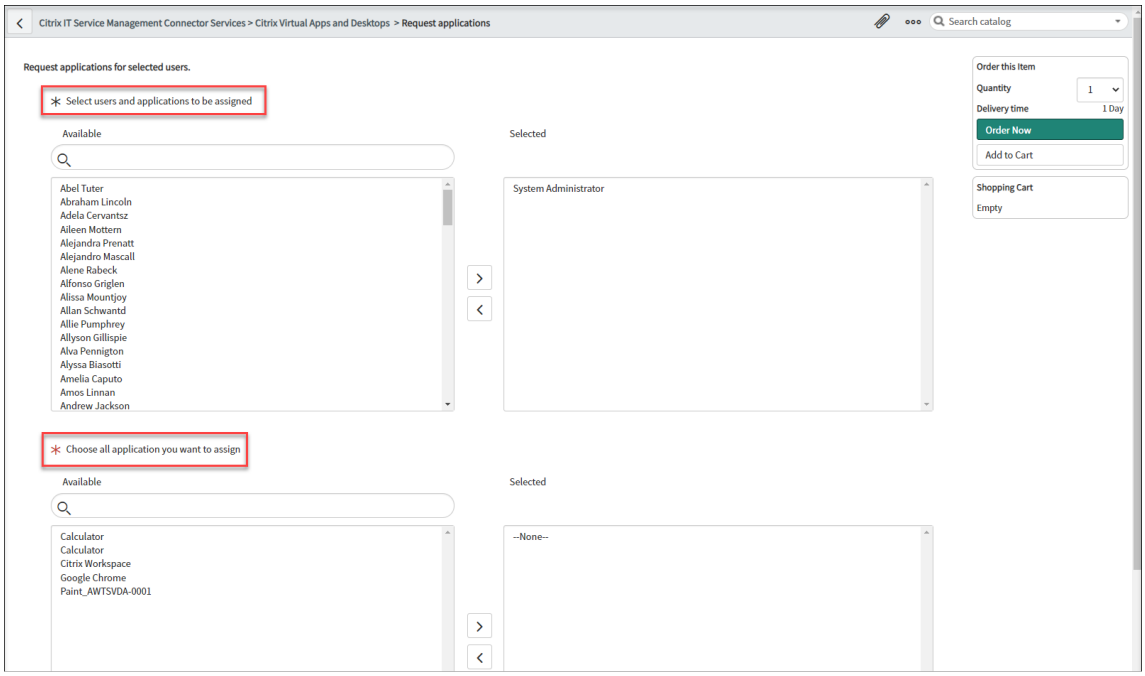
エンドユーザーの操作

1. ServiceNow インスタンスにログインします。
2. [**Request applications**] エントリを見つけます。例:



3. [**Request applications**] ページに、利用可能なユーザーとアプリケーションが一覧表示されます。選択して [**Order Now**] をクリックします。

> ヒント:
>
> 現在ログインしているユーザーがデフォルトで選択されています。



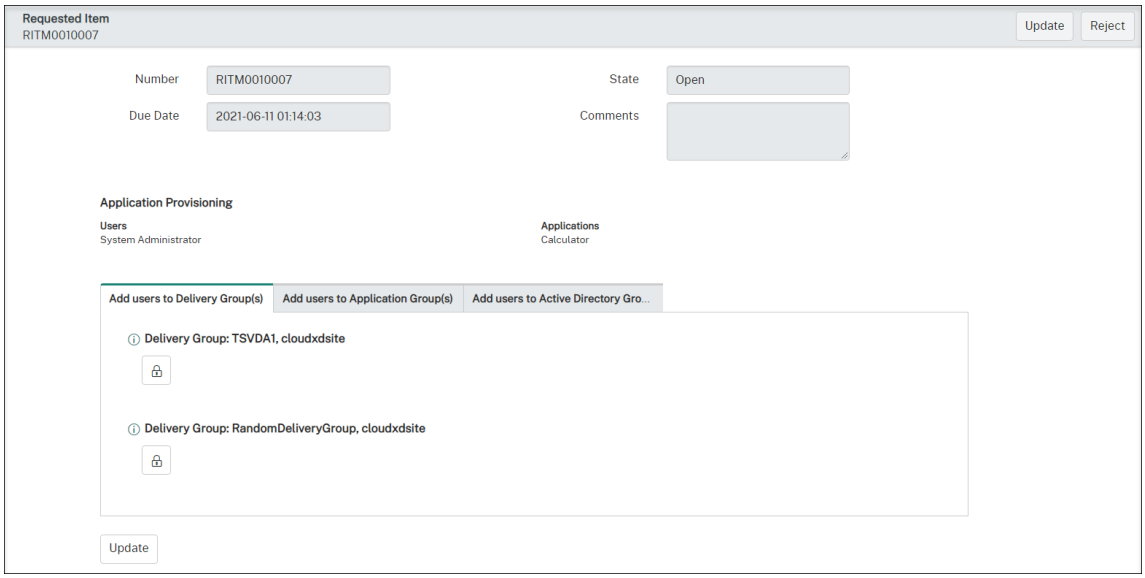
管理者の操作

1. [**User Requests**] ページにリクエストの一覧が表示されます。アプリケーションのリクエスト ID の横にあるアイコン、[**Open Record**] の順にクリックします。リクエストの詳細が表示されます。

> ヒント：
>
> ユーザーリクエストに使用できるアプリケーションを設定できるようになりました。詳しくは、本記事の「Studio ダッシュボード」を参照してください。

2. アプリのプロビジョニングを完了するには 3 つのオプションがあります：

   - ユーザーをデリバリーグループに追加：ロックアイコンをクリックしてユーザーを指定のデリバリーグループに追加し、［**Update**］をクリックします。
   - ユーザーをアプリケーショングループに追加：ロックアイコンをクリックしてユーザーを指定のアプリケーショングループに追加し、［**Update**］をクリックします。
   - ユーザーを **Active Directory** グループに追加：ロックアイコンをクリックしてユーザーを指定の Active Directory グループに追加して、［**Update**］をクリックします。

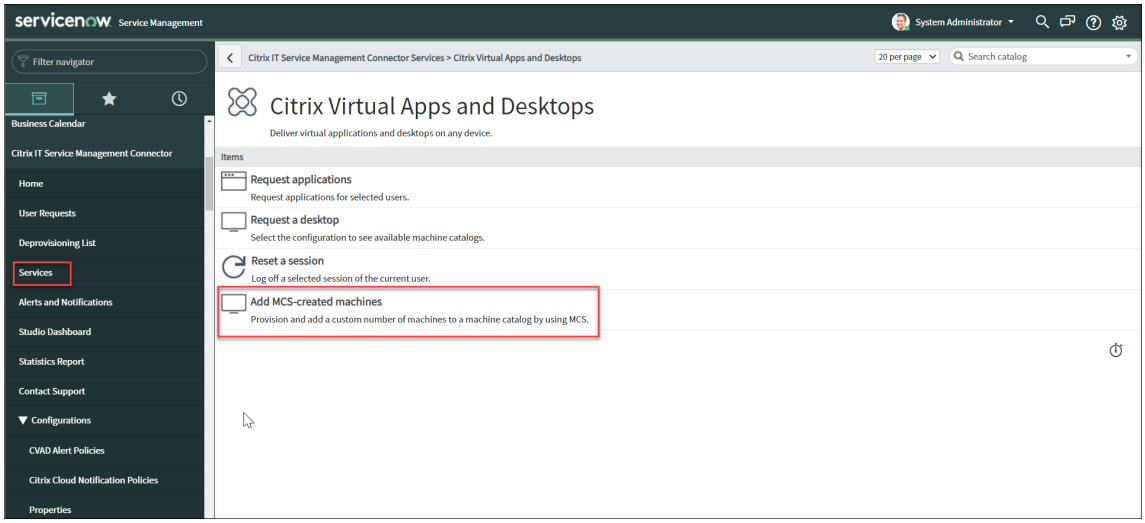


> 注：
>
> - ITSM コネクタは、Citrix Cloud からの構成を定期的に同期します。現在、同期サイクルは 1 時間です。各タブの内容は、Citrix Virtual Apps and Desktops で要求されたアプリケーションの関連設定を反映しています。たとえば、［**Add users to Active Directory Group(s)**］タブには、要求されたアプリケーションに関連するすべての AD グループが表示されます。
> - ［**Add users to Active Directory Group(s)**］タブが期待どおりに機能するようにするには、ServiceNow で［**Active Directory Automation**］ソリューションをアクティブ化して、Citrix ITSM コネクタが AD 自動化チャネルを多重化して AD または Azure AD にユーザーを設定できるようにします。

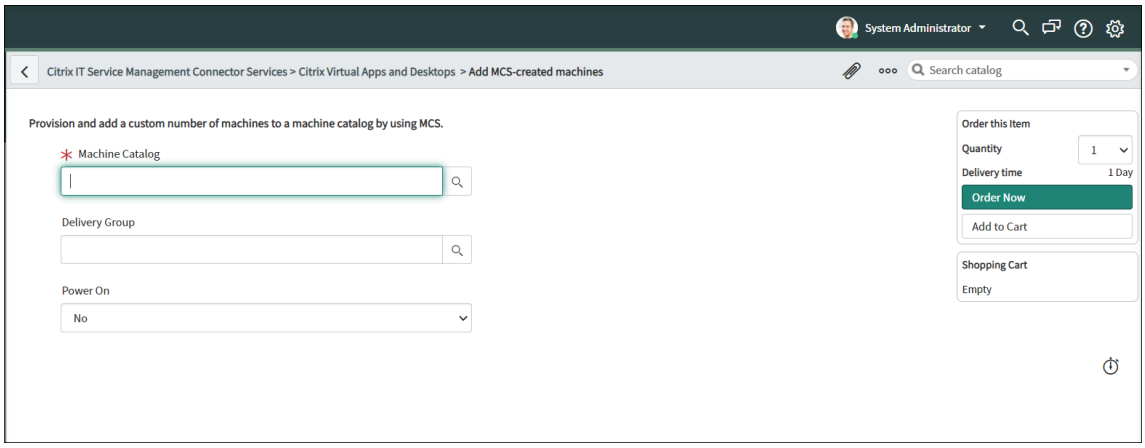
Add MCS-created machines

リクエストされたマシンカタログにマシンが不足している場合に、MCS で作成したマシンを追加できます。スケールアウトするマシンカタログは、Citrix Virtual Apps and Desktops サービスでホストされている必要があります。

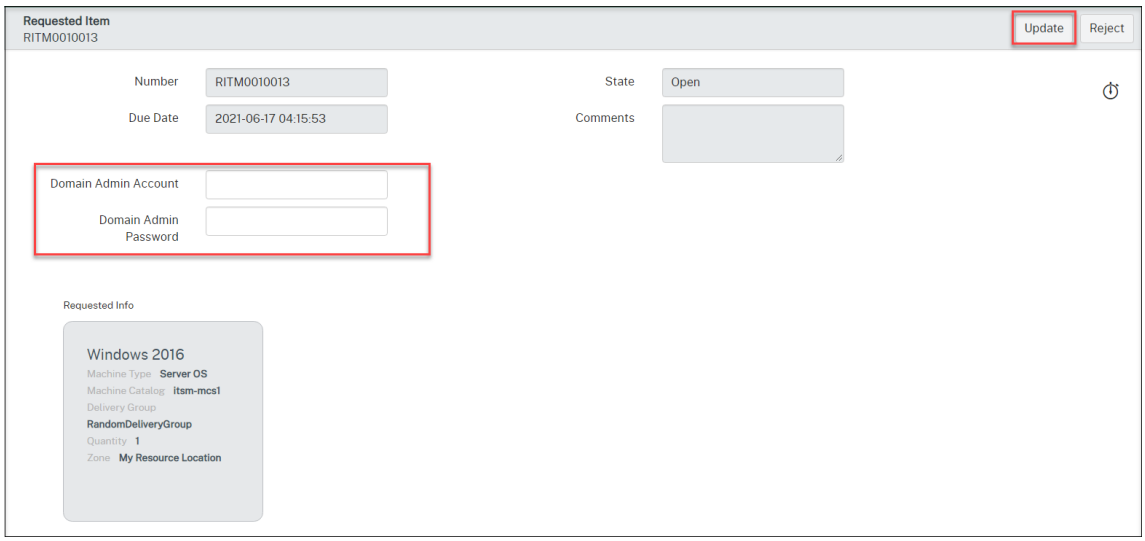
1. ServiceNow インスタンスにログインします。
2. 左ペインで **Citrix IT Service Management Connector** に移動し、[**Services**] を選択します。
3. [**Citrix IT Service Management Connector Services**] ページで、[**Citrix Virtual Apps and Desktops**] をクリックします。次のサービスが表示されます:
   - Request applications
   - Request a desktop
   - Reset a session
   - Add MCS-created machines



4. [**Add MCS-created machines**] を選択します。

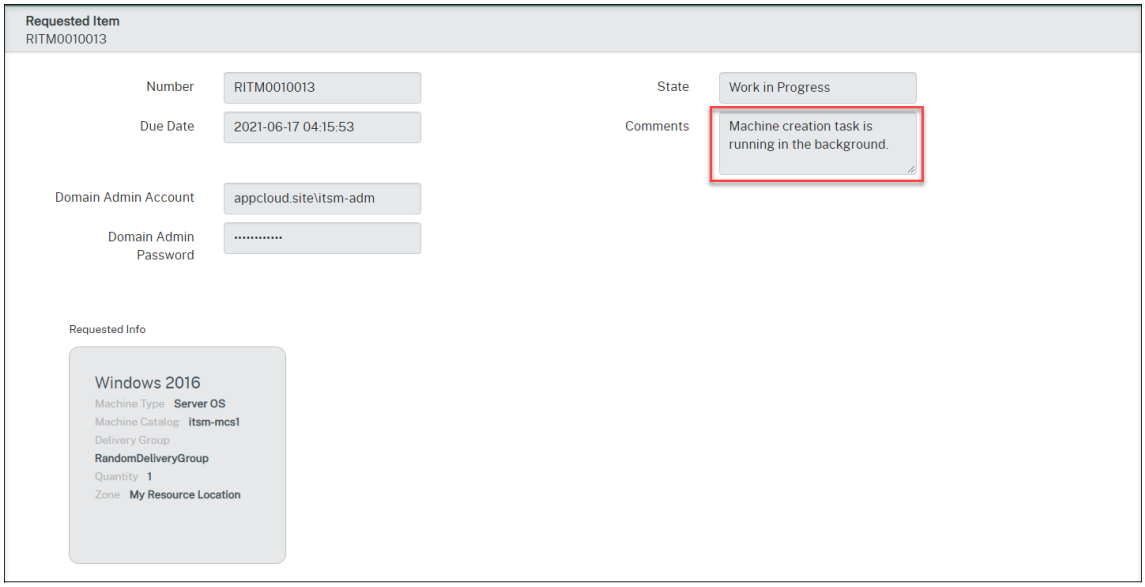


5. フィールドを設定し、作成するマシンの数を指定します。
6. [**Order Now**] をクリックします。
7. [**Requests**] ページに移動します。
8. マシン作成リクエストのレコードを開きます。



9. ドメインの資格情報を入力し、［更新］をクリックします。マシンの作成はバックグラウンドで実行されます。マシンの作成が完了するまで待ちます。

   入力するドメイン資格情報は、1 回限りの使用のみを目的としたものです。この資格情報は保存またはキャッシュされません。

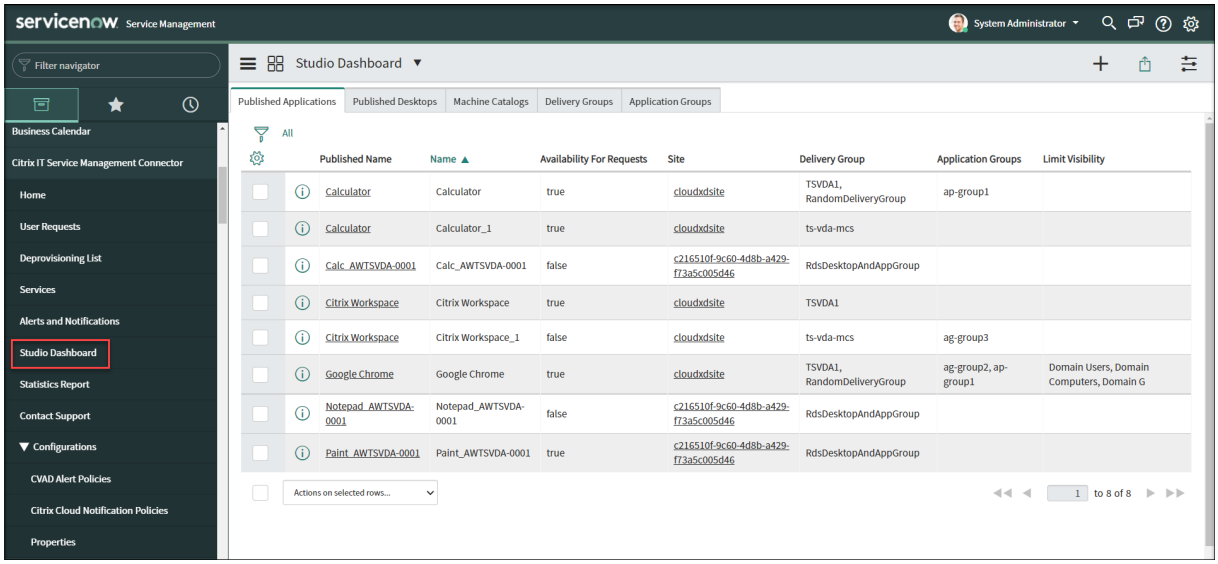


プロビジョニング解除一覧

2108.1.0 のリリース以降、Citrix Virtual Apps and Desktops サービスでホストされている VDI デスクトップから、アイドル状態のリソースを解放できるようになりました。詳しくは、「Studio ダッシュボード」セクションを参照してください。

Studio ダッシュボード

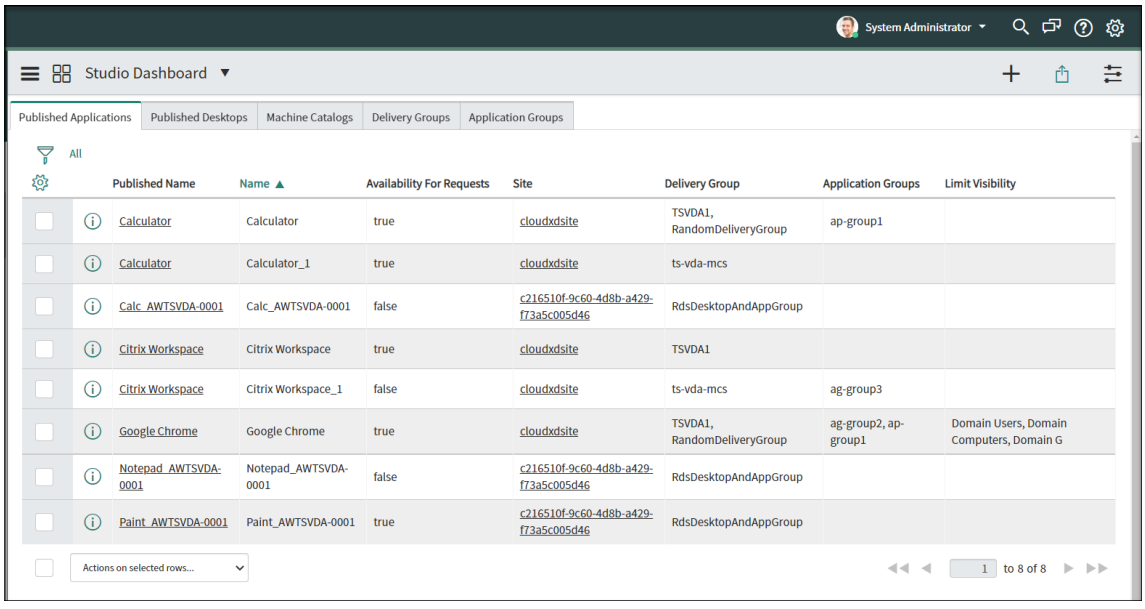
Studio ダッシュボードでは、公開アプリケーションとデスクトップ、マシンカタログ、デリバリーグループ、およびアプリケーショングループなど、Citrix Virtual Apps and Desktops（CVAD）の配信を一元的に管理できます。



このダッシュボードを使用して、ユーザーリクエストのアプリケーションの可用性を設定し、VDI デスクトップからアイドル状態のリソースを解放することもできます。

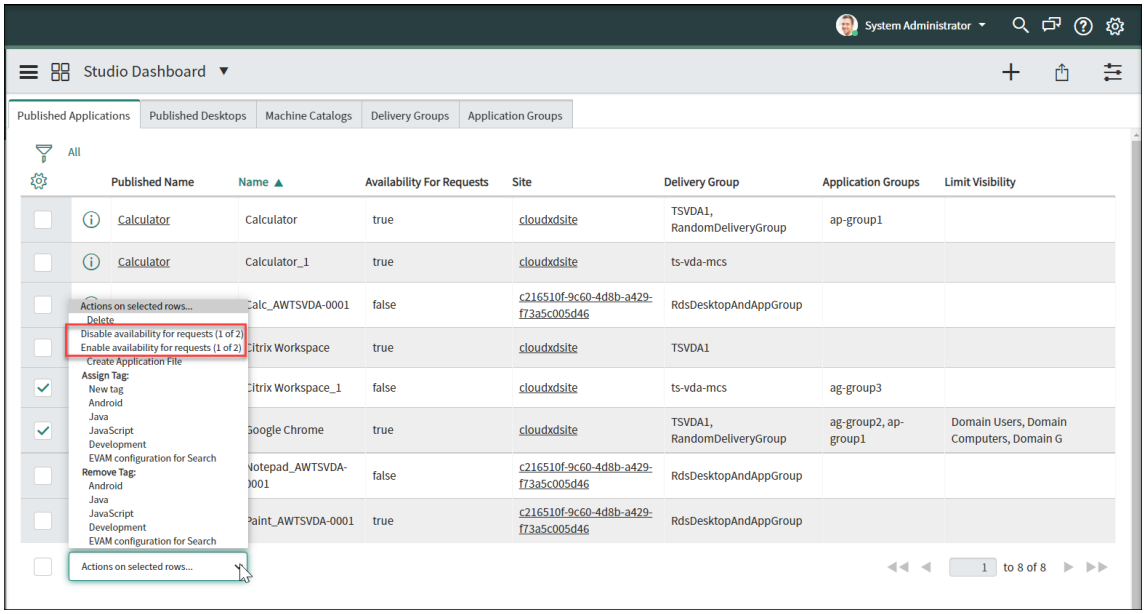
ユーザーリクエストのアプリケーションの可用性を設定するには、次の手順を実行します：

1. [**Published Applications**] タブを選択します。



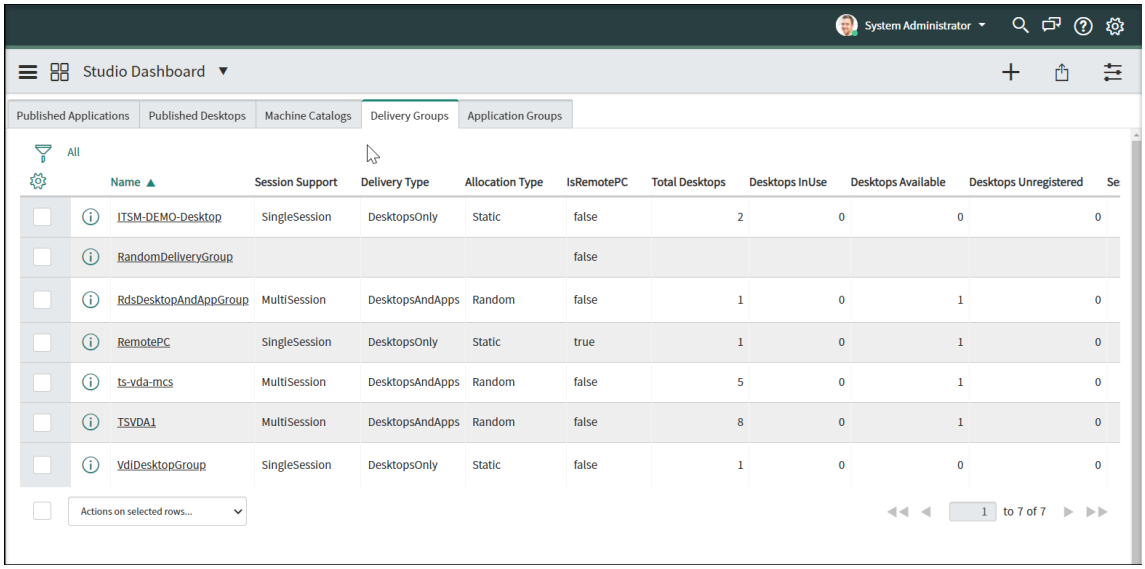
2. 1 つまたは複数のターゲットアプリケーションを選択します。
3. [**Actions on selected rows**] ドロップダウンリストで、[**Disable availability for requests**] または [**Enable availability for requests**] を選択し、選択したアプリケーションをリクエスト一覧で非表示に

するか、再び表示します。

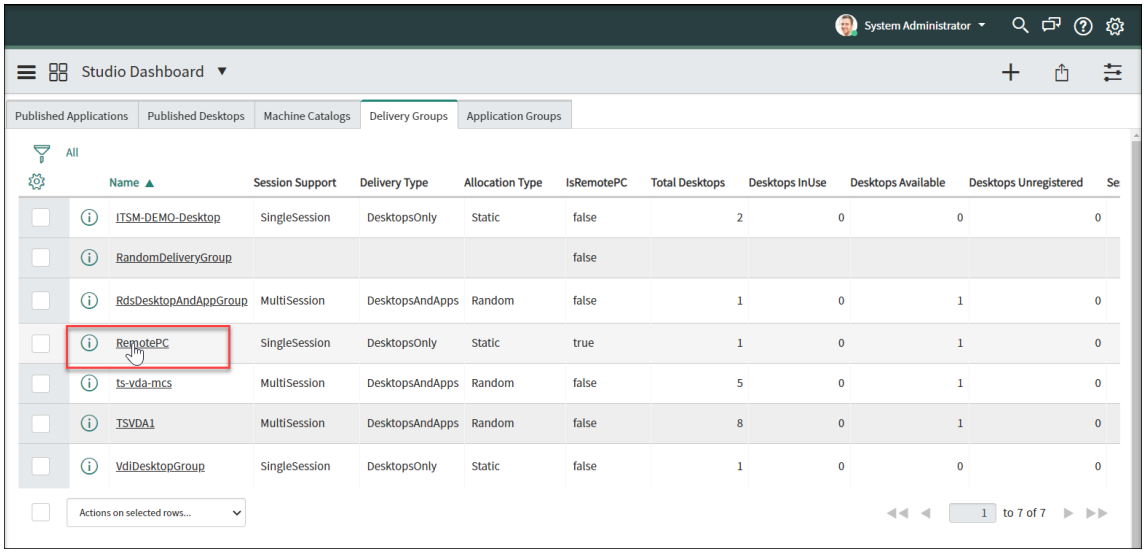


VDI デスクトップからアイドル状態のリソースを解放するには、次の手順を実行します:

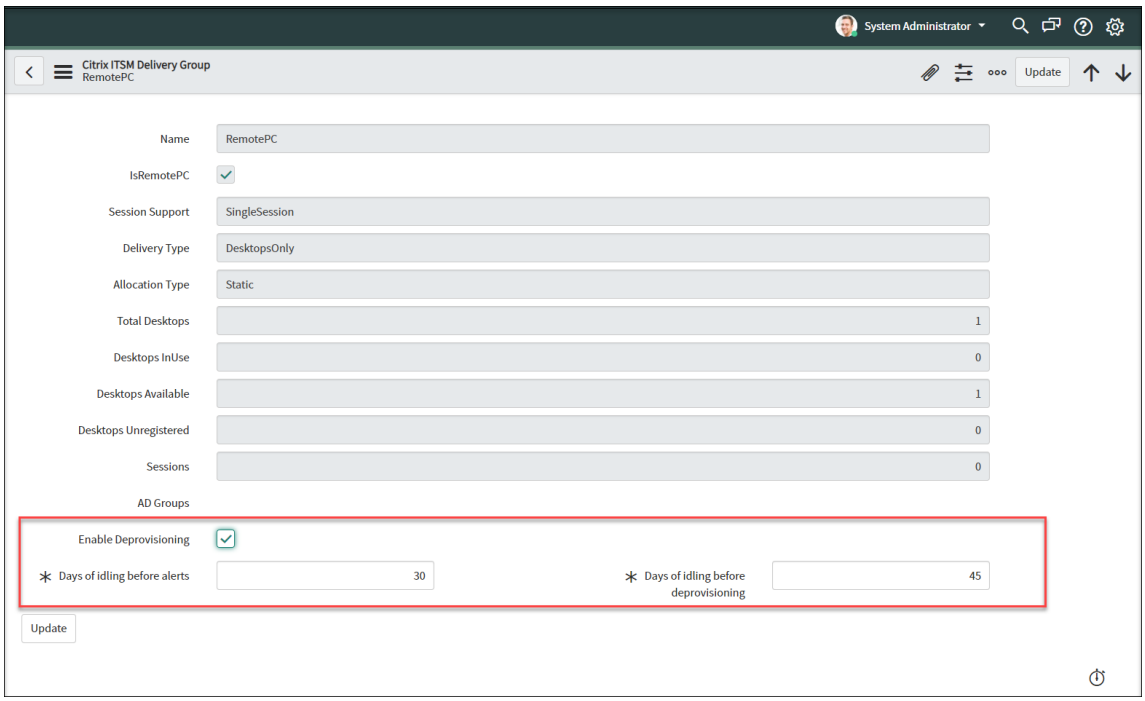
1. [**Delivery Groups**] タブを選択します。



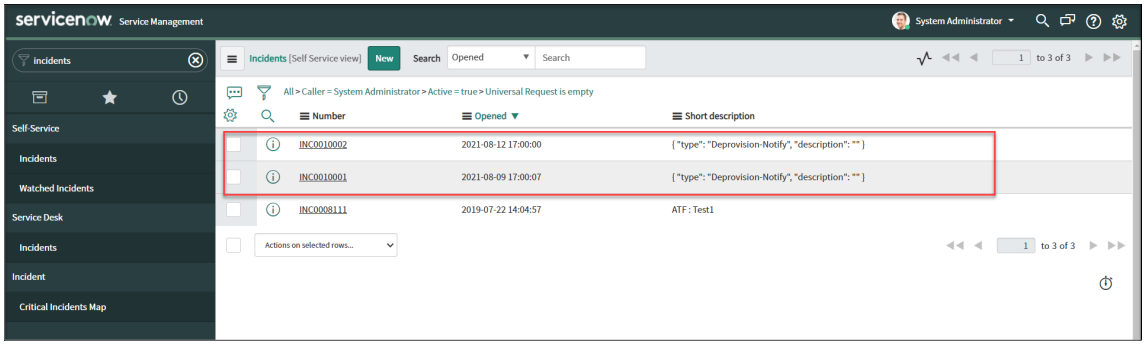
2. 割り当ての種類が ［**Static**］と表示されているターゲットデリバリーグループの名前をクリックします。



3. 選択したデリバリーグループのページで ［**Enable Deprovisioning**］を選択し、アラートとプロビジョニング解除までアイドル状態が続く日数を設定します。

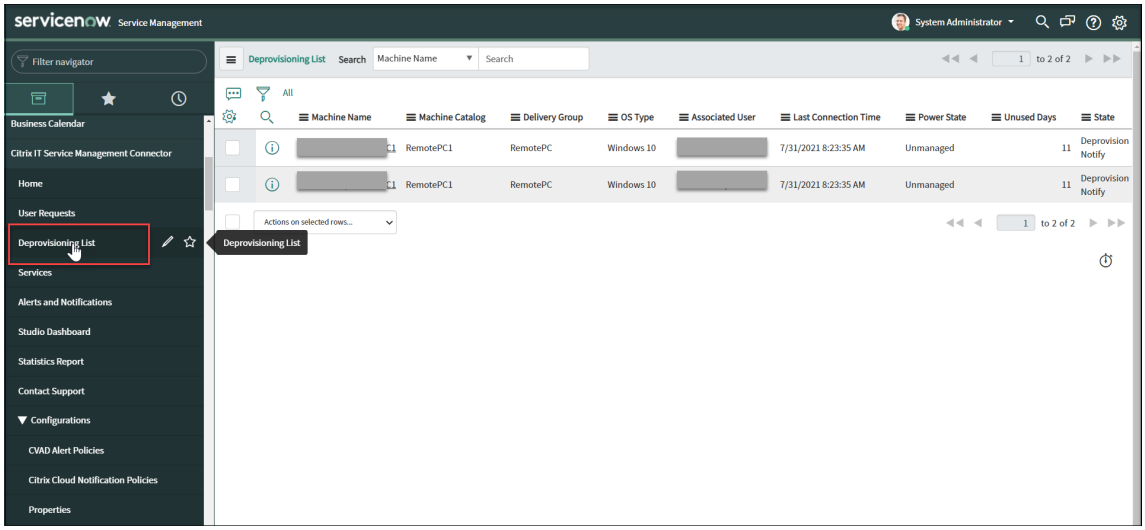


デリバリーグループ内のデスクトップのアイドル時間がアラートのしきい値を超えると、ServiceNow にインシデントがアラートとして作成されます。たとえば、以下のようになります：



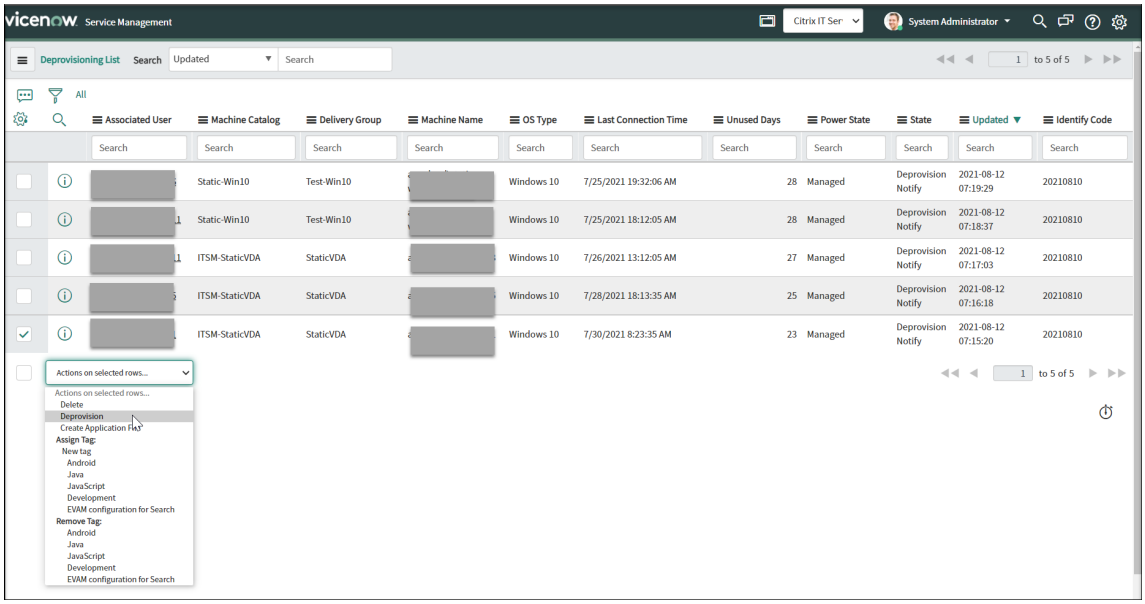
このようなインシデントの受信を回避するには、アラートまでアイドル状態が続く日数を「**0**」に設定します。

デリバリーグループ内のデスクトップのアイドル時間がプロビジョニング解除のしきい値を超えると、デスクトップがプロビジョニング解除一覧に表示され、プロビジョニング解除を決定できます。たとえば、以下のようになります:

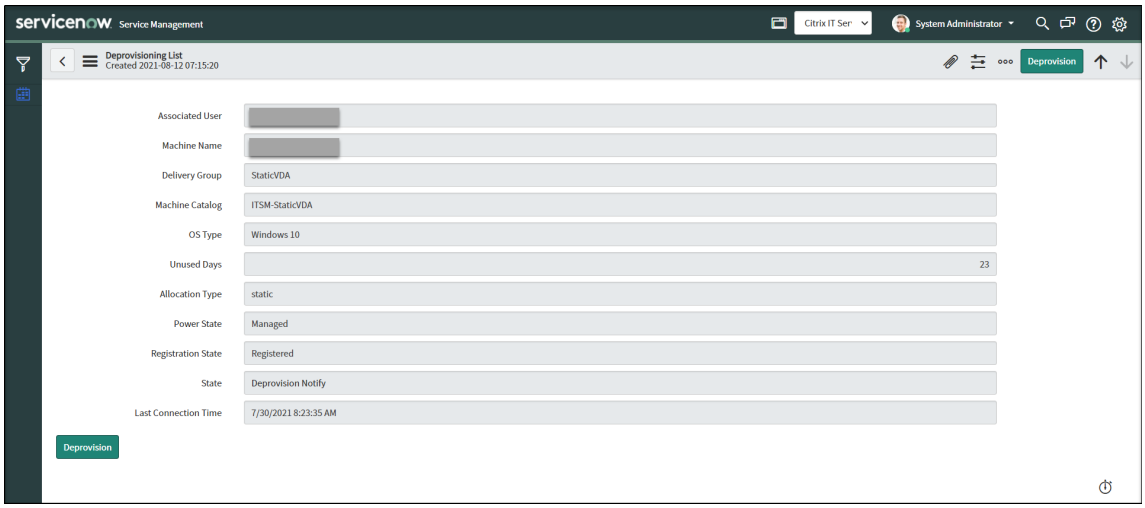


デスクトップのプロビジョニングを解除するには、デスクトップを選択し、[**Actions on selected rows**] で [**Deprovision**] を選択します。または、マシン名をクリックして別のページを開き、そのページの [**Deprovision**] をクリックします。

オプション 1: [**Actions on selected rows**] で [**Deprovision**] を選択する。



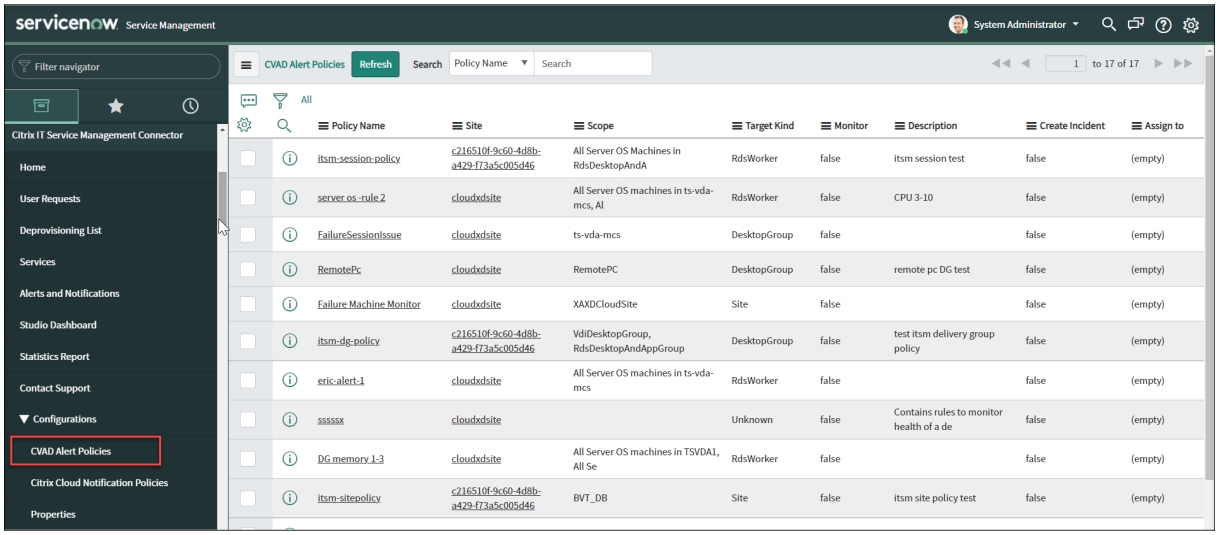
オプション 2：デリバリーグループの詳細ページで ［**Deprovision**］をクリックする。



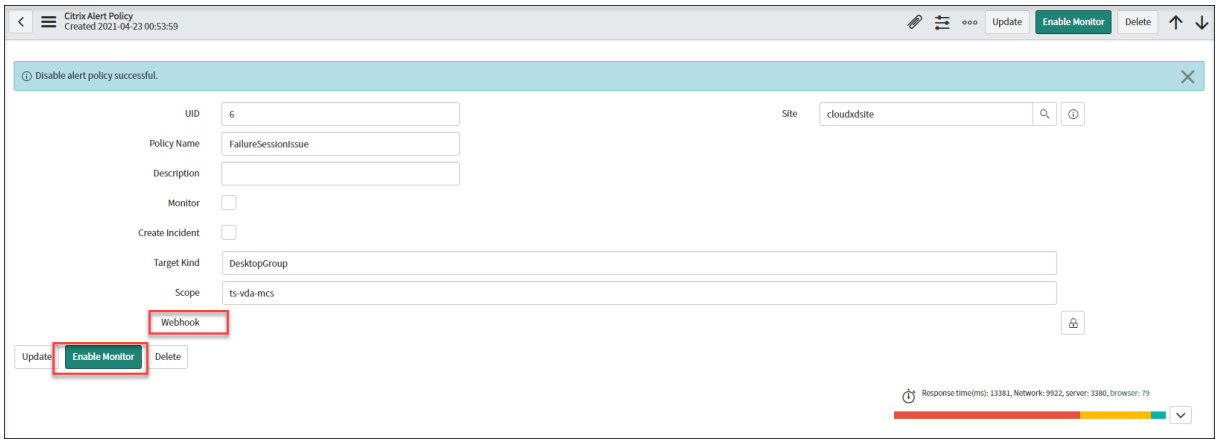
ServiceNow 内から **CVAD** アラートへのアクセス

アラートポリシーは、Citrix Director と、Citrix Virtual Apps and Desktops サービスポータルのモニターの両方で設定できます。詳しくは、Citrix Virtual Apps and Desktops のドキュメントとCitrix Virtual Apps and Desktops サービスのドキュメントを参照してください。

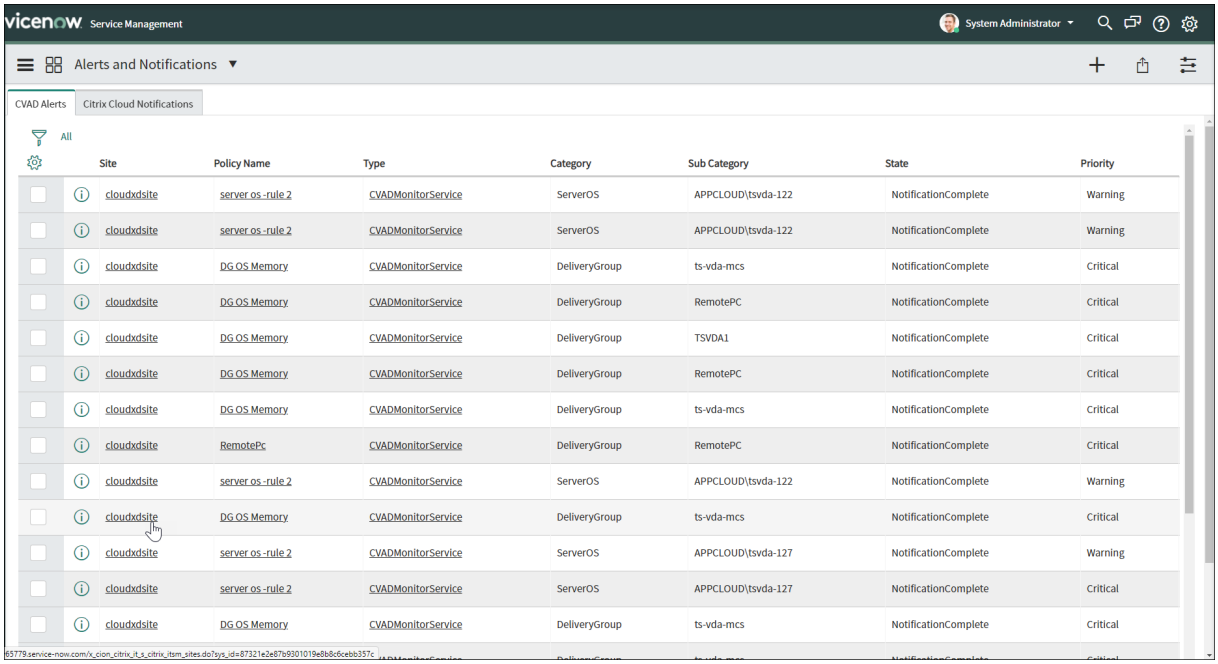
設定したアラートポリシーは、［**Citrix IT Service Management Connector**］**>** ［**Configurations**］**>** ［**CVAD Alert Policies**］の ServiceNow ポータルに定期的に同期します。現在、同期サイクルは 1 時間です。アラートポリシーをすぐに同期するには、［**Refresh**］をクリックします。



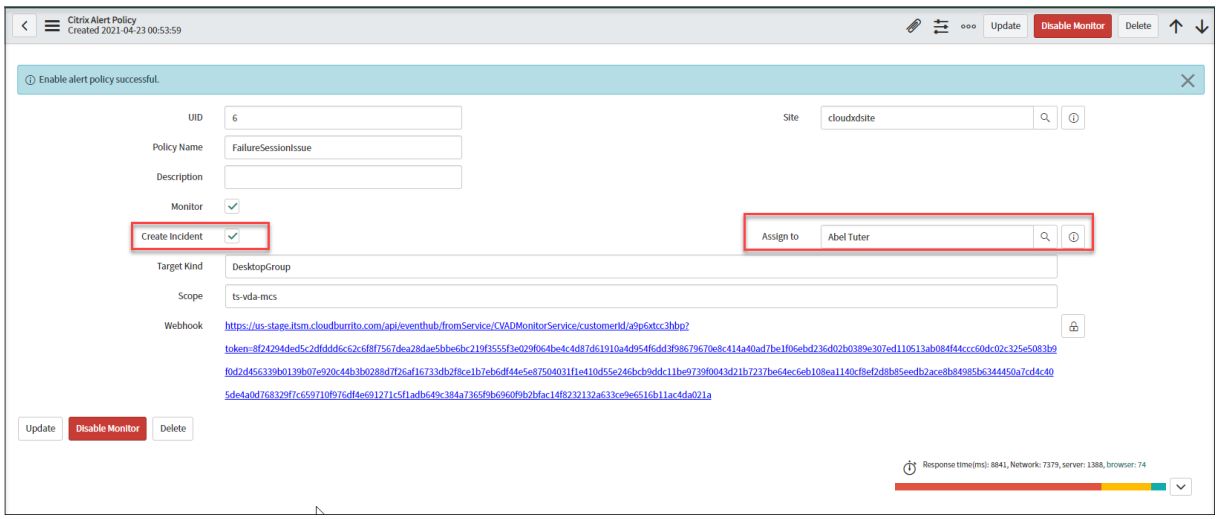
選択したアラートポリシーを開き、[**Enable Monitor**] をクリックできます。これによって、[**Citrix IT Service Management Connector**] > [**Alerts and Notifications**] の ServiceNow に、ポリシーを満たすアラートが表示されます。



次のスクリーンショットは、ServiceNow で表示されるアラートです。



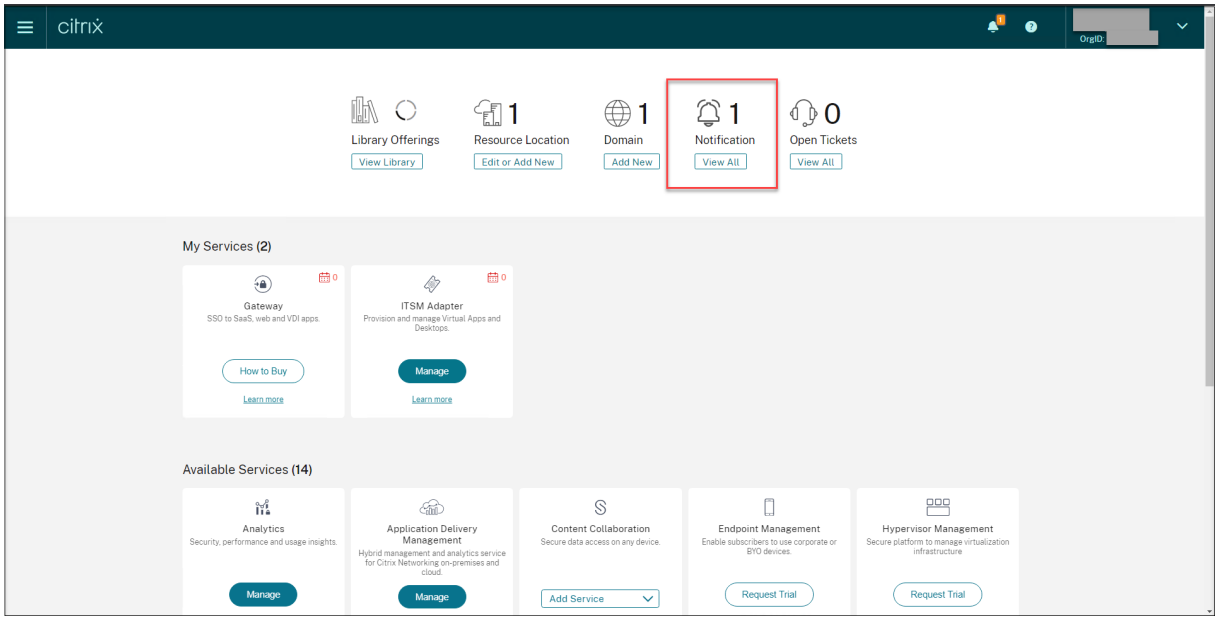
インシデントを作成し、アラート処理のために特定の担当者に割り当てることもできます。



監視が無効になっている場合、特定のポリシーを満たすアラートが ServiceNow に同期されません。

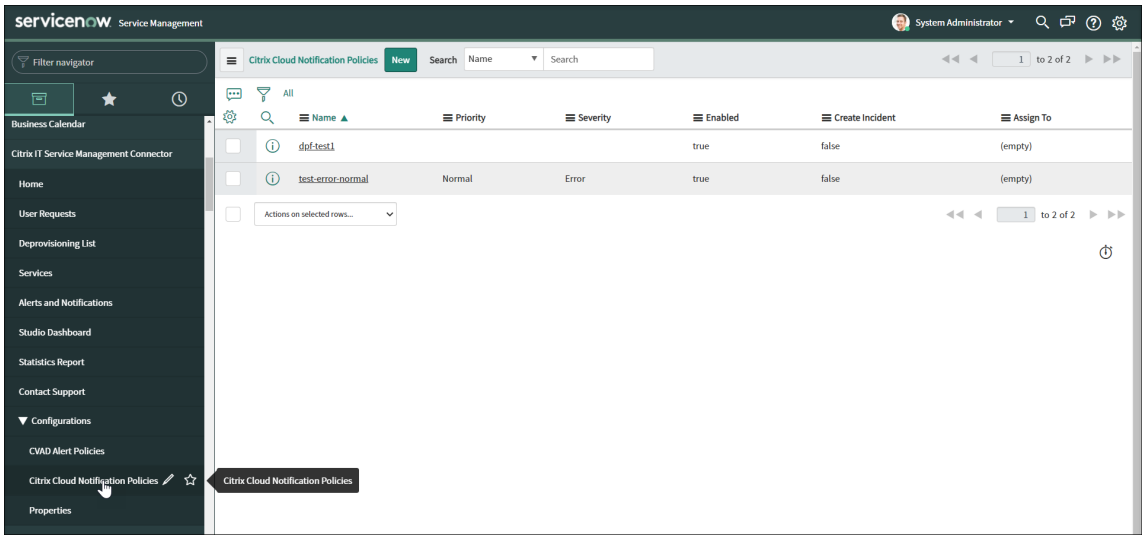
ServiceNow 内から **Citrix Cloud** 通知へのアクセス

通知は、Citrix Cloud 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 のすべてのサービスで使用できます。詳しくは、Citrix Cloud ドキュメントを参照してください。

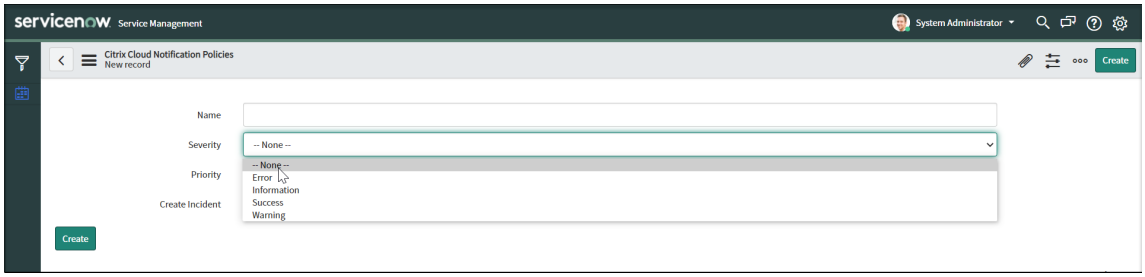


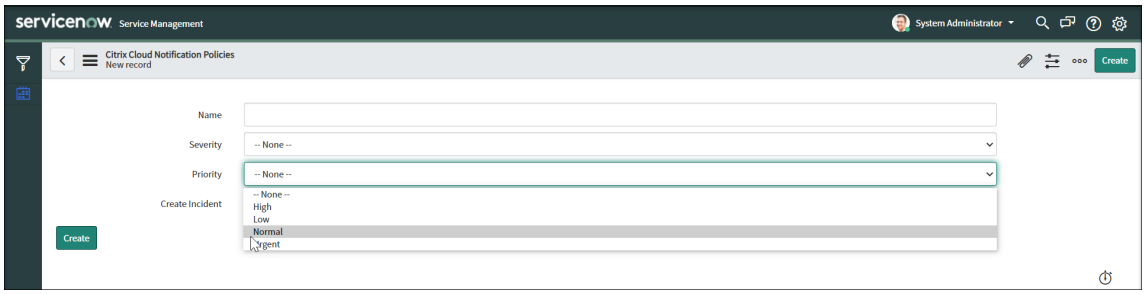
ServiceNow でポリシーを作成して、関心のある Citrix Cloud 通知から同期することができます。通知ポリシーを作成するには、次の手順を実行します:

1. 左側のナビゲーションから ［**Citrix IT Service Management Connector**］ > ［**Configurations**］ > ［**Citrix Cloud Notification Policies**］を選択します。

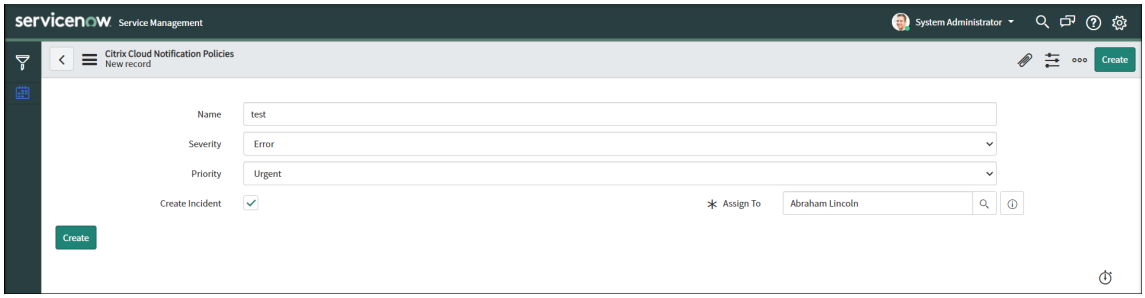


2. ［**New**］をクリックします。ポリシーに名前を付け、重大度や優先度などの通知フィルタリング条件を設定します。

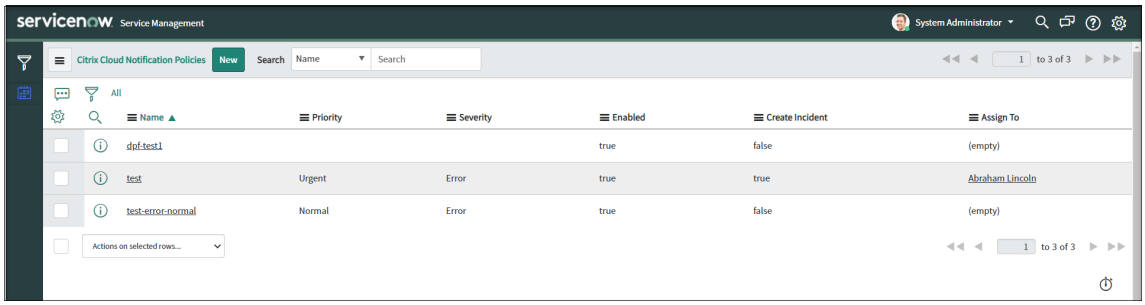




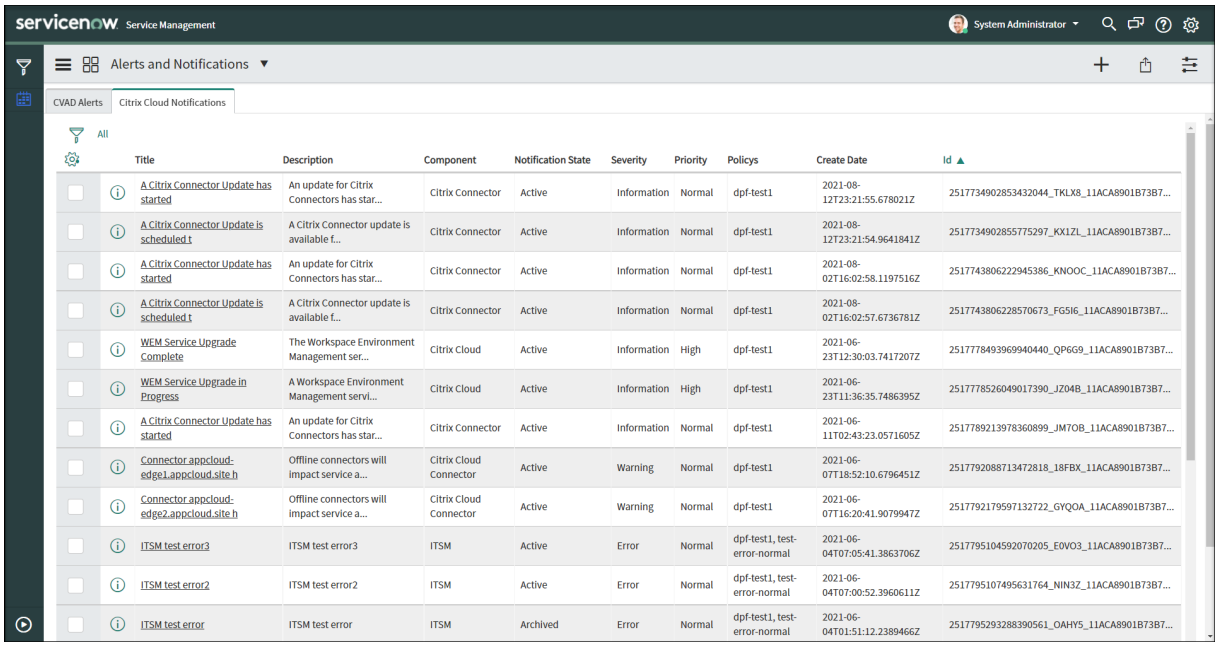
3. 条件を満たす通知に応じて ServiceNow でインシデントを作成し、それらのインシデントを特定の担当者に割り当てることを選択します。



4. [**Create**] をクリックします。作成したポリシーは、[**Citrix Cloud Notification Policies**] ページで更新されて表示されます。



ポリシーを設定すると、ポリシー設定の条件を満たす通知が Citrix Cloud から ServiceNow に同期されて［**Citrix IT Service Management Connector**］**>**［**Alerts and Notifications**］に表示されます。一度に複数の通知を選択し、［**Actions on selected rows**］で ［**Dismiss Notification**］を選択することができます。



MDX Service

September 17, 2021

MDX Service を使用すると、アプリコンテナテクノロジである MDX でアプリをラップすることで、iOS および Android モバイルアプリを準備することができます。MDX Service は、組織内で作成されたアプリをラップするために使用されます。このアプリは、Citrix Endpoint Management で管理できます。

MDX Service では、MDX 21.6.0 を使用してサードパーティ製アプリをラッピングできます。

お知らせ

- **WKWebView** の問題と **Citrix SSO**

  Apple が UIWebView を使用するアプリのサポートを終了した後、Citrix では業務用モバイルアプリのバージョン 20.11.x から WKWebView がサポートされるようになりました。WKWebView は、以前使用されていた UIWebView フレームワークに代わる Apple フレームワークです。技術的な制限と WKWebView の複雑さにより、一部の Web サイトでトンネリングの問題が発生する場合があります。

  Citrix では、分析を提供し、Web サイトをレンダリングする方法の変更をベストエフォートベースで提示する場合があります。ただし、問題が発生した場合は、VPN トンネルに Citrix SSO アプリを使用することをお勧めします。

Citrix SSO について詳しくは、「Citrix Gateway クライアント」を参照してください。

- モバイルアプリケーション管理（MAM）SDK は、iOS および Android プラットフォームがカバーできない MDX 機能の領域で代わりに使用されます。MAM SDK（Preview）について詳しくは、モバイルアプリケーション管理（MAM）SDKに関する Citrix Developer セクションを参照してください。詳細については、こちらのCitrix ブログの記事でも確認できます。

  Citrix ダウンロードページにサインオンして、SDK をダウンロードできます。

- MDX Toolkit は、2022 年 3 月に製品終了（EOL）になる予定です。エンタープライズアプリケーションの管理を続行するには、MAM SDK を使用する必要があります。
- MDX Service は、2021 年 9 月に製品終了（EOL）になる予定です。エンタープライズアプリケーションの管理を続行するには、MAM SDK を使用する必要があります。

iOS アプリのラッピングについて詳しくは、「iOS アプリをラップするには」を参照してください。

Android アプリのラッピングについて詳しくは、「Android アプリをラップするには」を参照してください。

MDX、MDX Toolkit を使用した従来の MDX ラッピング処理、必要なアセットの署名の説明については、以下を参照してください：

- MDX Toolkit について
- iOS モバイルアプリのラッピング
- Android モバイルアプリのラッピング

データ保持ポリシー

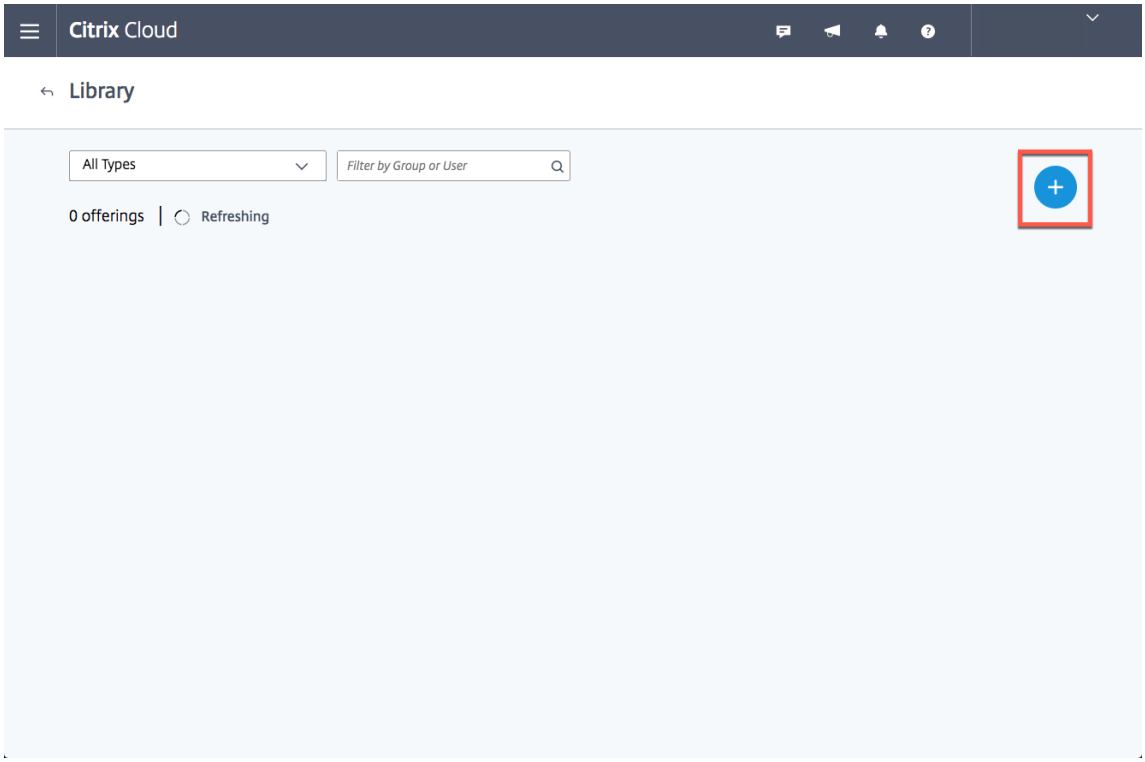
以下は、MDX Service のデータ保持ポリシーです：

- アプリのバイナリ（**IPA** ファイルと **APK** ファイル）： 90 日。
- ラップされたアプリ（**MDX** ファイル）： 90 日（ダウンロード可能）。
- 証明書とキーストアファイル：ラッピング後すぐに削除。
- **iOS** モバイルのプロビジョニングプロファイル：ラッピング後すぐに削除。

MDX Service の開始

MDX Service の使用を開始するには、以下の手順に従います。使用体験をフィードバックするには、Citrix ID を使用してMDX Service ディスカッションフォーラムに参加してください。

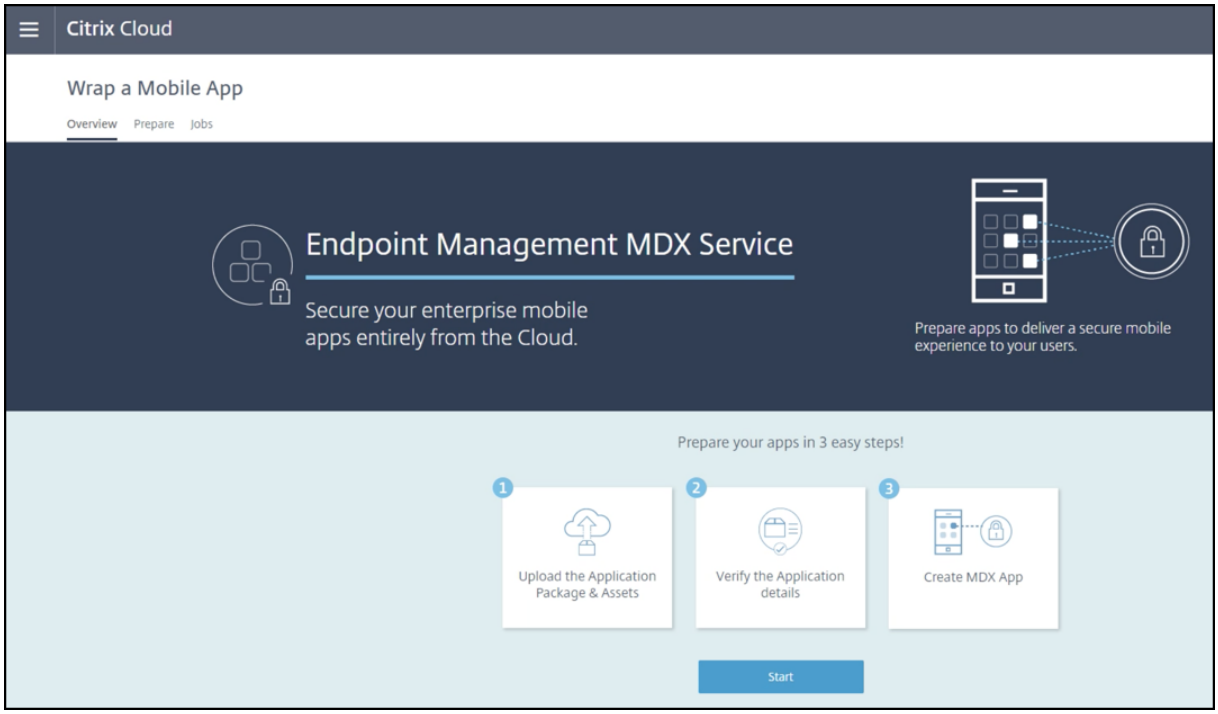
1. まだ Citrix Cloud アカウントがない場合は、トライアルをリクエストして Citrix Cloud に登録してください。登録について詳しくは、「Citrix Cloud への登録」を参照してください。
2. ページの右上隅にあるハンバーガーメニューをクリックしてから、［ライブラリ］をクリックします。
3. このページの右上に、プラス印（+）の入った青い円があります。このアイコンの上にマウスを置いて、［モバイルアプリをラップする］をクリックします。



MDX Service を使用するには

MDX Service を使用するには、アプリケーションパッケージバイナリと必要な署名アセットをアップロードします。次に、アプリの詳細を確認し、必要に応じて属性を変更します。これによって、ラップされたアプリケーションパッケージをダウンロードできます。

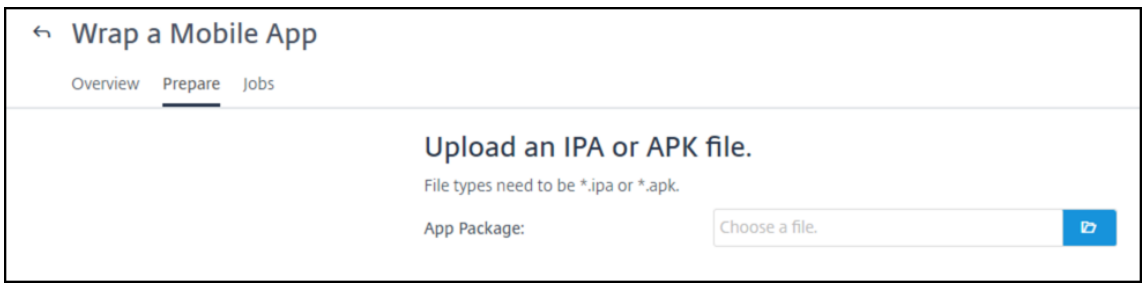
この手順を開始するには、MDX Service の［概要］ページで、画面の下部にある ［開始］をクリックします。



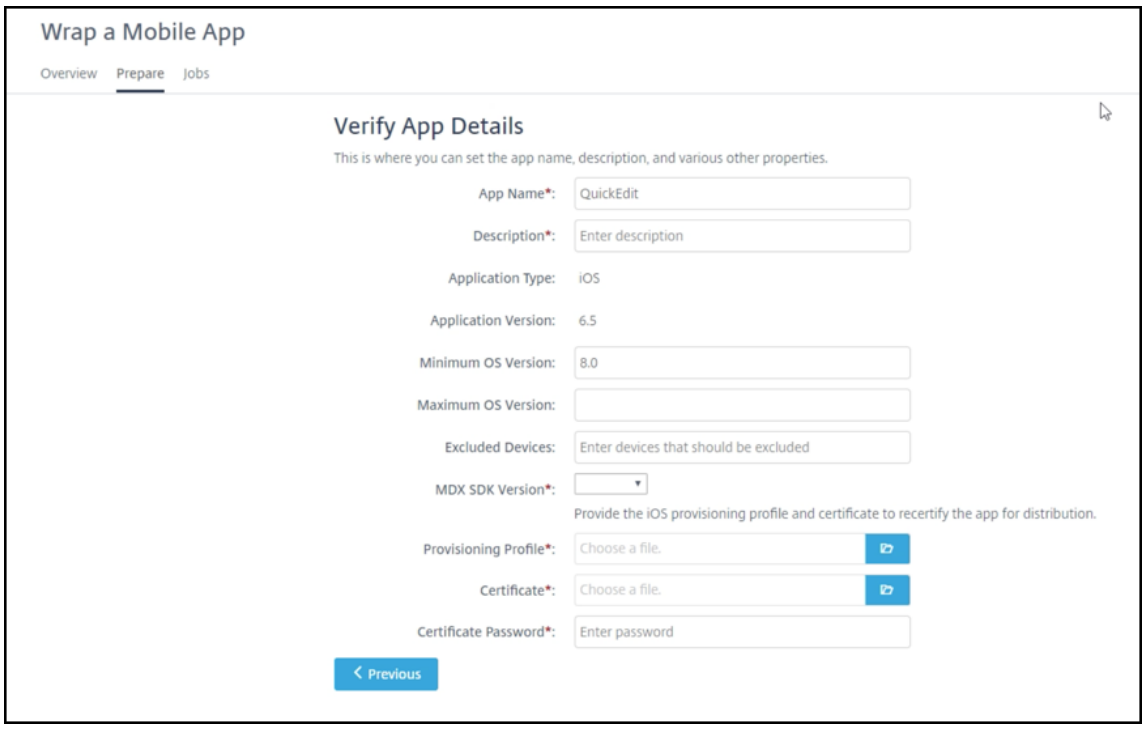
次に、以下の手順に従って、iOS アプリまたは Android アプリをラップします。

iOS アプリをラップするには

1. アプリの.ipa ファイルをアップロードします。アップロードに必要な時間はファイルサイズによって異なります。.ipa ファイルに許可されるファイルサイズの制限は 209MB です。この制限値を超えるアプリがある場合は、MDX Toolkit を使用してください。



.ipa ファイルがアップロードされ、正常に処理されると、[アプリケーションの詳細を確認]画面が表示されます。



2. ［アプリケーションの詳細を確認］画面で、次の情報を入力します:

   a) （オプション）［アプリ名］、［最小 **OS** バージョン］、［最大 **OS** バージョン］を変更します。

   b) ［説明］を入力します（必須）。

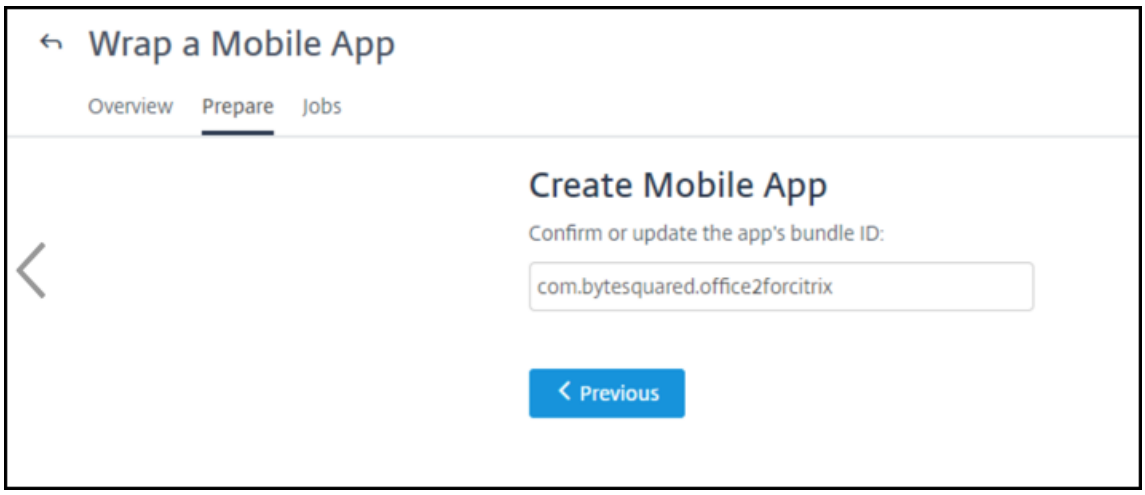
   c) アプリをラップする MDX SDK のバージョンを選択します。

   d) 次の iOS 署名アセットをアップロードします:

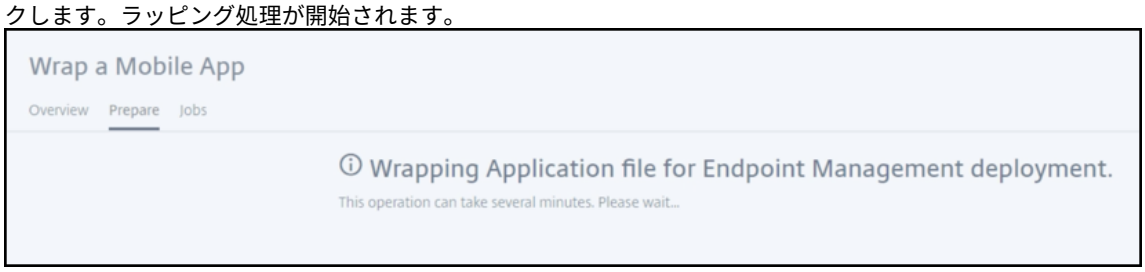
      - プロビジョニングプロファイル
      - 証明書
      - 証明書パスワード

      iOS のプロビジョニングプロファイルと証明書の情報の収集については、Endpoint Management ドキュメントの記事「証明書と認証」にある「Endpoint Management 証明書の管理」セクションの「MDX Service または MDX Toolkit」の項目を参照してください。

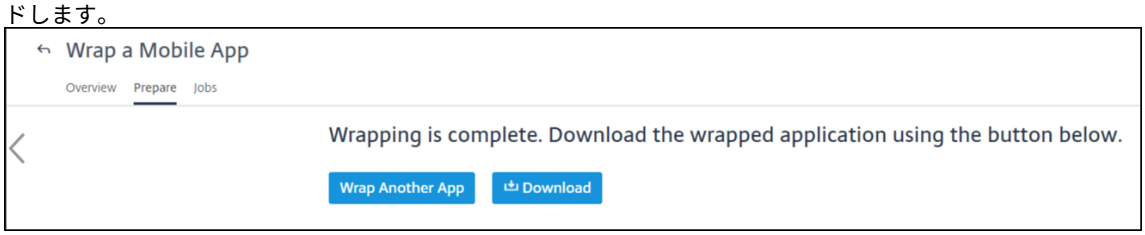
MDX Service で署名アセットを使用してアプリが変更されると、［モバイルアプリの作成］画面が表示されます。



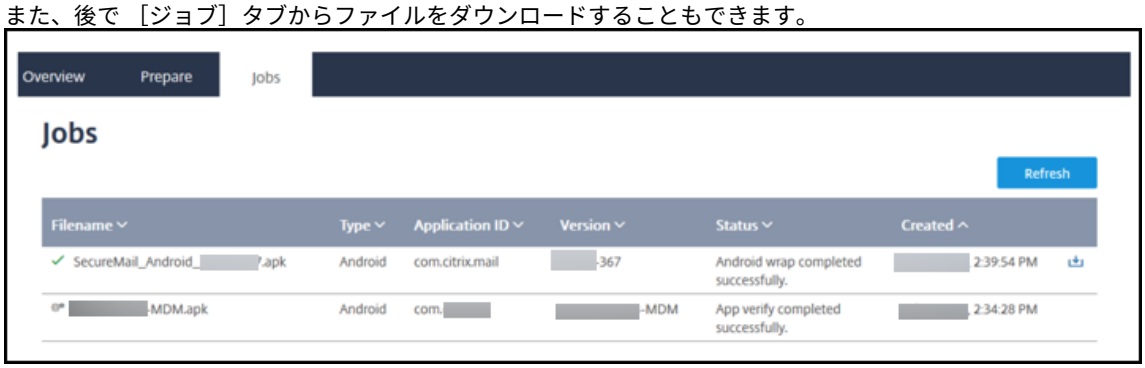
3. （オプション）［モバイルアプリの作成］画面で、モバイルアプリのバンドル ID を変更して、［次へ］をクリックします。ラッピング処理が開始されます。



4. ラッピング処理の完了後、ラップされた MDX アプリケーションパッケージ（.mdx ファイル）をダウンロードします。

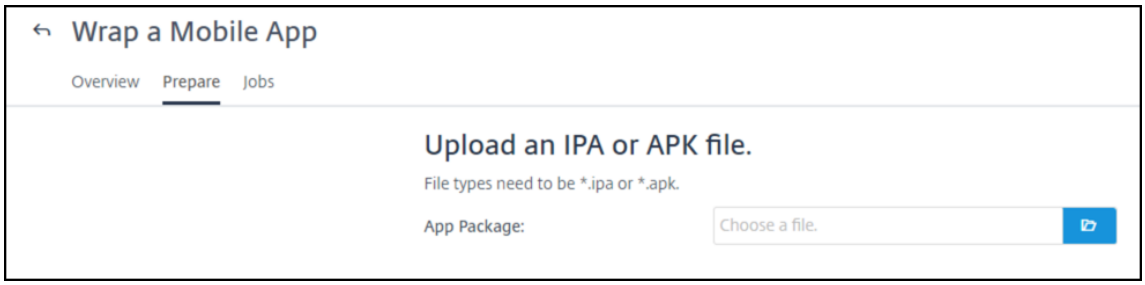


また、後で ［ジョブ］タブからファイルをダウンロードすることもできます。

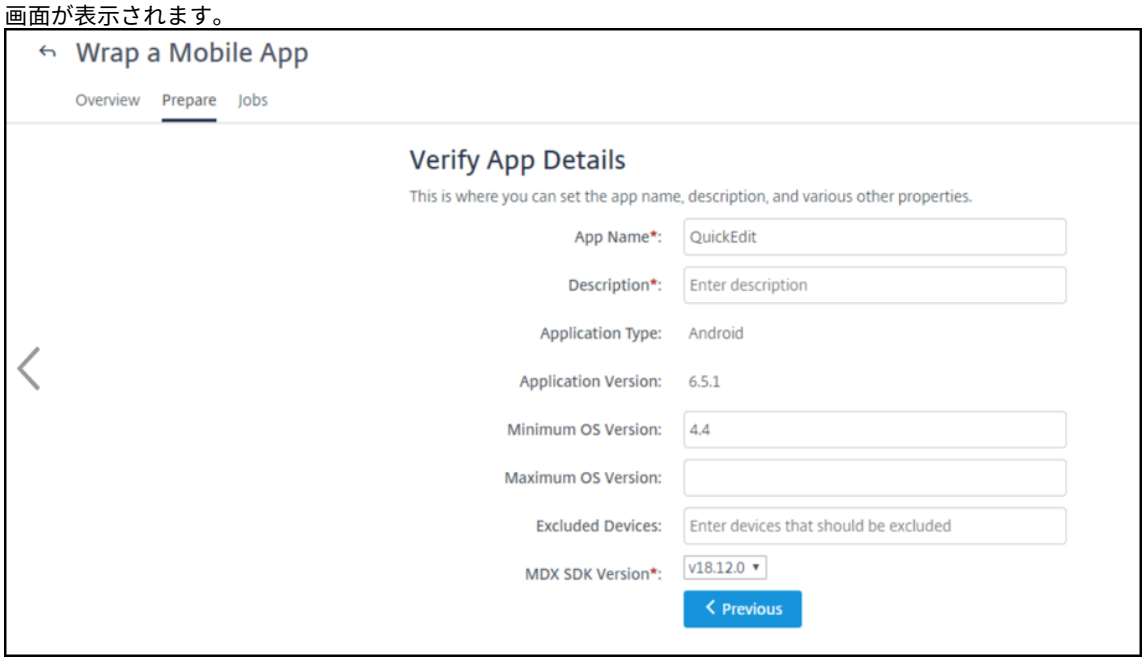


Android アプリをラップするには

1. アプリの.apk ファイルをアップロードします。アップロードに必要な時間はファイルサイズによって異なります。.ipa ファイルに許可されるファイルサイズの制限は 209MB です。この制限値を超えるアプリがある場合は、MDX Toolkit を使用してください。



2. .apk ファイルが MDX Service にアップロードされ、正常に処理されると、［アプリケーションの詳細を確認］画面が表示されます。

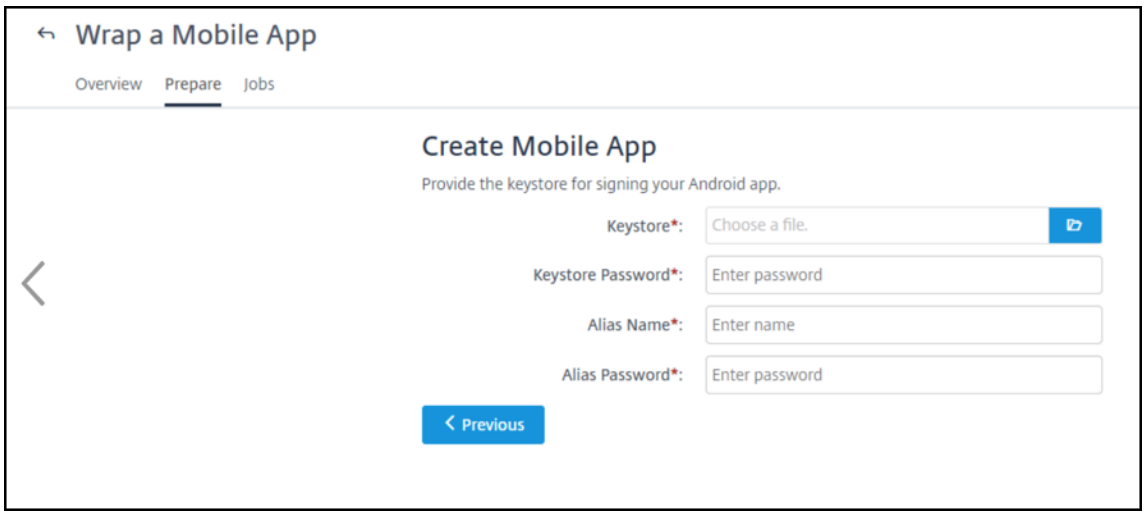


3. ［アプリケーションの詳細を確認］画面で、次の情報を入力します：

   a) （オプション）［アプリ名］、［最小 **OS** バージョン］、［最大 **OS** バージョン］を変更します。
   b) ［説明］を入力します（必須）。
   c) アプリをラップする MDX SDK のバージョンを選択します。

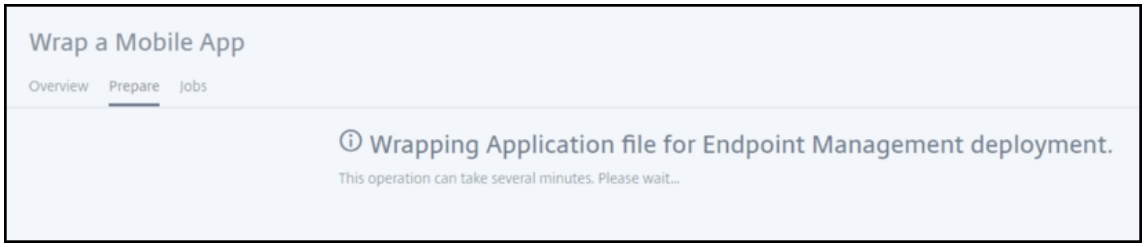
4. ［モバイルアプリの作成］画面で、次の Android 署名アセットをアップロードします：

   - キーストア
   - キーストアのパスワード
   - エイリアス名
   - エイリアスのパスワード



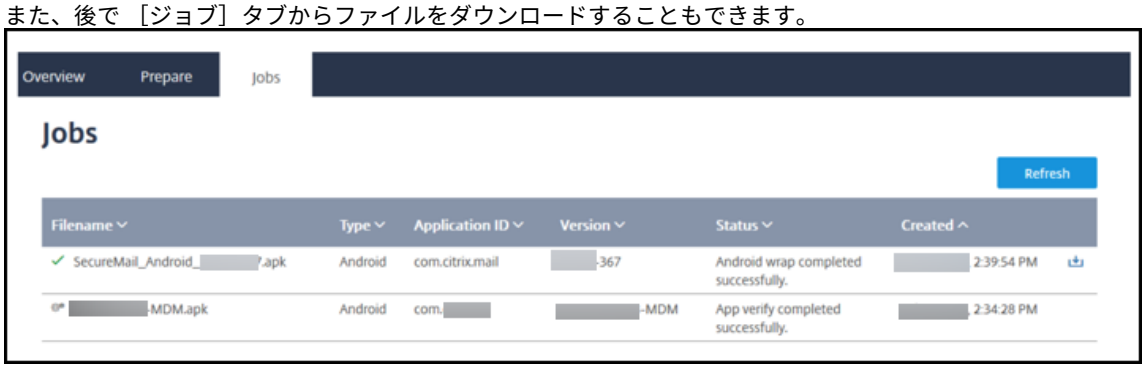
キーストアとエイリアス名の情報の収集については、CTX220480の手順に従います。

5. ［次へ］をクリックしてラッピング処理を開始します。



6. ラップされた MDX アプリケーションパッケージ（.mdx ファイル）をダウンロードします。

また、後で ［ジョブ］タブからファイルをダウンロードすることもできます。



既知の問題

MDX Service 20.10.5 の既知の問題

- macOS 10.14 以降で開発された iOS アプリは、MDX Service を使用してラップすることができません。MAM SDK または MDX 機能を備えた iOS アプリを追加するには、MAM SDK を使用してアプリを準備するか、オンプレミスの MDX Toolkit を使用してアプリをラップしてください。[CXM-90666]

Secure Browser サービス

June 15, 2021

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。管理者は、セキュアなブラウザーをすばやく展開することで、即時に価値を提供します。IT 管理者は、インターネット閲覧を分離することで、企業ネットワークのセキュリティを損なうことなく、エンドユーザーに安全なインターネットアクセスを提供します。

ユーザーは、Citrix Workspace（または Citrix Receiver）を使用してログオンし、構成済みの Web ブラウザーで Web アプリを開くことができます。Web サイトとユーザーデバイスとの間で閲覧データが直接転送されないため、ユーザー操作中のセキュリティが保護されます。

Secure Browser サービスを使って、次の用途に使用するセキュアなブラウザーを公開できます:

- 外部 **Web** アプリで共有パスコードを使用。共有パスコード認証を使用したブラウザーを公開する場合、ユーザーはアプリを起動するためにパスコードを入力する必要があります。
- 認証済みの外部 **Web** アプリ。認証済みの外部 Web アプリを公開し、Citrix Workspace を使用してこのアプリを起動する場合、少なくとも 1 つの Cloud Connector を含むリソースの場所が必要です（2 つ以上を推奨）。詳しくは、「Citrix Cloud Connector」を参照してください。認証済みアプリの場合、Citrix Cloud のライブラリを使用してユーザーを追加する必要があります。
- 認証されていない外部 **Web** アプリ。認証されていない外部 Web アプリを公開し、Citrix Workspace を使用してこのアプリを起動する場合、少なくとも 1 つの Cloud Connector を含むリソースの場所が必要です（2 つ以上を推奨）。詳しくは、「Citrix Cloud Connector」を参照してください。

  通常は推奨されませんが、認証されていない外部 Web アプリを単純な概念実証に使用することがあります。

詳しくは、「セキュアなブラウザーの公開」を参照してください。

Secure Browser サービスはまた、次の機能を提供します:

- 公開アプリの Citrix Workspace への統合
- 公開アプリのオンプレミス StoreFront への統合
- セキュリティのためのシンプルな URL 許可リスト機能

- 使用状況の監視
- クリップボードの使用、印刷、キオスクモード、リージョンフェールオーバー、クライアントドライブマッピングの管理

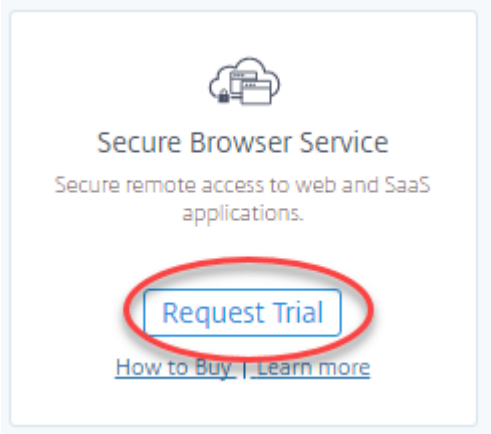
新機能

- 2021 年 3 月:
  - **Secure Browser** は、**Azure Active Directory** での認証をサポートします。ユーザーは、Azure Active Directory の資格情報を使用して、Citrix Workspace から Secure Browser アプリにサインインできるようになりました。詳しくは、「Citrix Workspace との統合」を参照してください。
  - **Secure Browser** を使用すると、ユーザーのアクティブなセッションを監視してログオフさせることができます。Secure Browser は、ユーザー名、セッション ID、クライアント IP、認証の種類、アプリケーション名、セッション開始時間、ユーザーのアクティブなセッションに関するセッション期間情報を提供します。アクティブな各セッションに関する基本情報を表示し、必要に応じてセッションを切断できます。詳しくは、「アクティブなセッションを監視」を参照してください。
- 2020 年のリリース：2020 年のすべてのリリースで、全体のパフォーマンスと安定性の向上に役立つ機能強化が行われています。

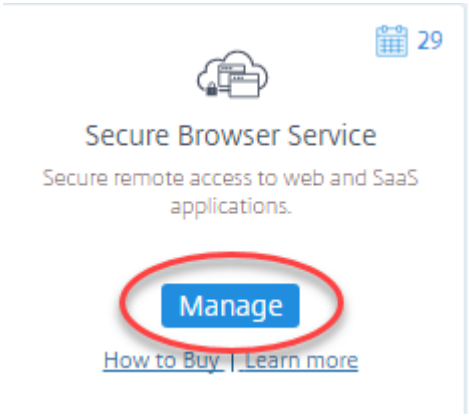
導入

以下のビデオでは、Secure Browser の使用開始について説明しています。

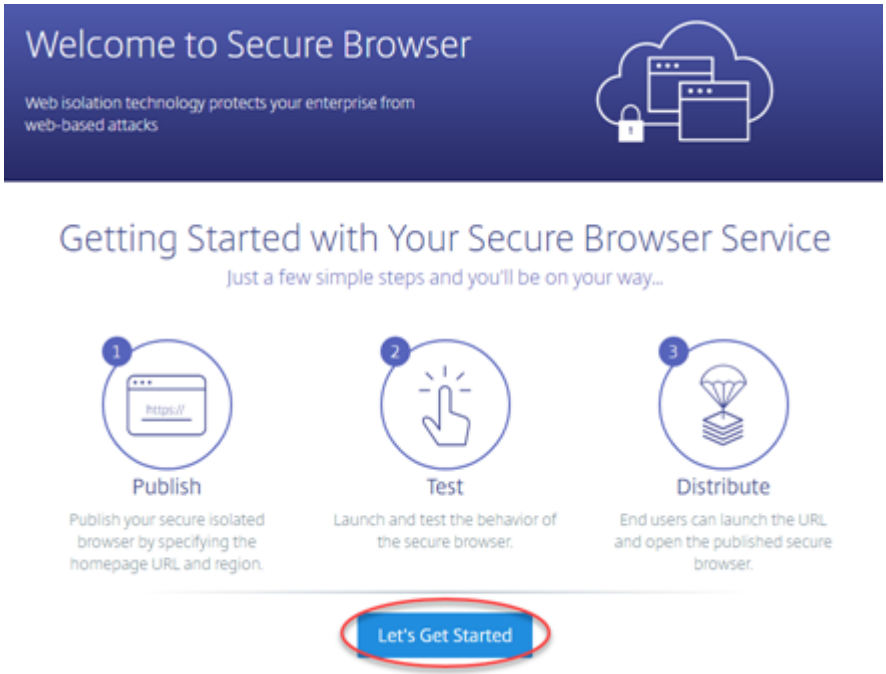
1. Citrix Cloud にサインインします。アカウントをお持ちでない場合は、「Citrix Cloud へのサインアップ」を参照してください。Citrix Secure Browser サービスの 30 日間トライアルをリクエストできます。
2. **Secure Browser** サービスのタイルで、［トライアルをリクエスト］をクリックします。



3. 数分後にメールが届きます。このメールは、Citrix Cloud アカウントに関連付けられています。メール内のサインインリンクをクリックします。
4. Citrix Cloud に再度サインインした後、**Secure Browser** サービスのタイルで ［管理］をクリックします。



5. [**Secure Browser** へようこそ] ページで、[使用を開始する] をクリックします。説明に従って、最初のセキュアなブラウザーを公開します。



Citrix Secure Browser サービスの購入について詳しくは、「https://www.citrix.com/ja-jp/products/citrix-secure-browser/」を参照してください。

Citrix Workspace との統合

Secure Browser は Citrix Workspace に統合できます。サービスが統合されていることを確認するには:

1. Citrix Cloudにサインインします。
2. 左上のメニューで、[ワークスペース構成] を選択します。
3. [サービス統合] タブを選択します。
4. Secure Browser サービスのエントリが有効になっていることを確認します。無効になっている場合は、省略記号メニューをクリックし、[有効化] を選択します。

認証は、Active Directory または Azure Active Directory を使用して実行できます。**Azure Active Directory** を選択した場合、Active Directory ドメインコントローラーを含むオンプレミスのドメインには、少なくとも 1 つ（2 つ以上を推奨）の Cloud Connector が含まれている必要があります。詳しくは、次のトピックを参照してください：

- ワークスペースへの認証の変更
- Azure Active Directory を Citrix Cloud に接続する

オンプレミス **StoreFront** と統合する

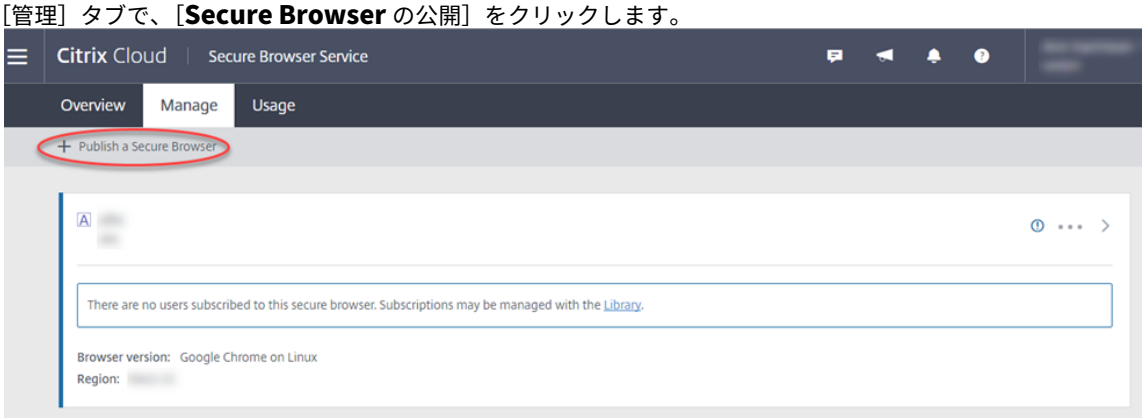
オンプレミス StoreFront を使用している Citrix Virtual Apps and Desktops の顧客は、Secure Browser サービスと簡単に統合することで次の利点が得られます：

- 公開されたセキュアなブラウザーを既存の Citrix Virtual Apps and Desktops アプリで集約して、統合ストア環境を実現します。
- ネイティブの Citrix Receiver を使用して、エンドユーザーエクスペリエンスを強化できます。
- StoreFront に統合された既存の多要素認証ソリューションを使用して、Secure Browser 起動時のセキュリティを強化できます。

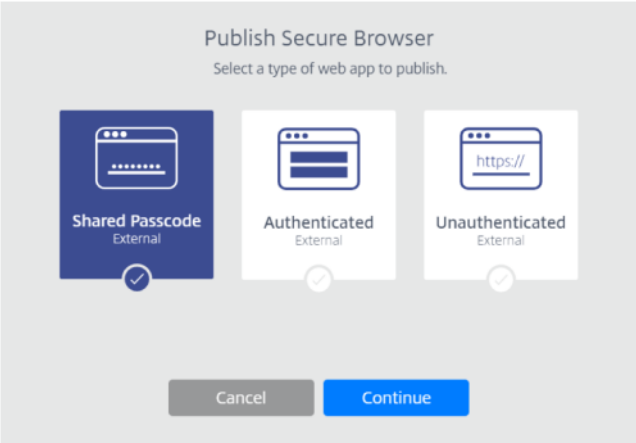
詳しくは、CTX230272および StoreFront の構成に関するドキュメントを参照してください。

セキュアなブラウザーの公開

1. Citrix Cloud にサインインします（まだサインインしていない場合）。**Secure Browser** サービスのタイルで、［管理］をクリックします。
2. ［管理］タブで、［**Secure Browser** の公開］をクリックします。



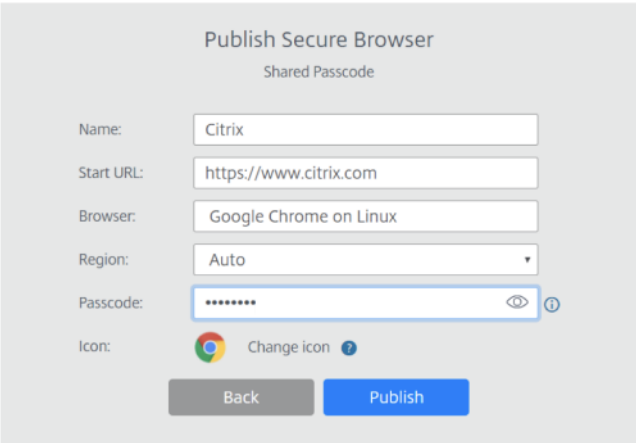
3. 公開するセキュアなブラウザーの種類を、［共有］、［パスコード］、［認証されている］、［認証されていない］から選択します。次に、［続行］をクリックします。



デフォルトでは、ユーザーは launch.cloud.com を使用して、共有パスコード認証でアプリケーションを起動する必要があります。Citrix Workspace および Citrix Cloud ライブラリは共有パスコード使用のアプリをサポートしません。

Citrix Workspace を使用するには、認証済みアプリを公開して Citrix Cloud ライブラリで利用者（ユーザー）やグループを明示的に割り当てる必要があります。認証されていないアプリは、ユーザー割り当てなしですべての Workspace 利用者が使用できます。

4. 次の設定を構成します：



- 名前：作成中のアプリの名前を入力します。
- 開始 **URL**：ユーザーがアプリを起動したときに開く URL を指定します。
- リージョン：サーバーの場所/リージョンを選択します。利用可能なリージョンは米国西部、米国東部、東南アジア、オーストラリア東部、西ヨーロッパです。

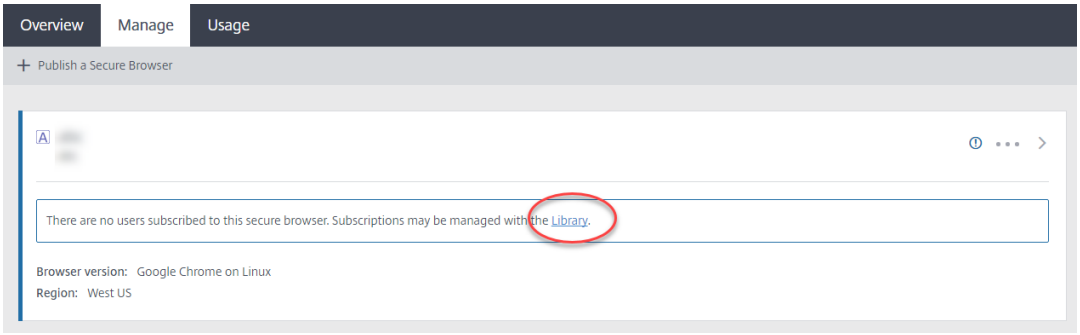
  ［自動］を選択すると、Secure Browser は地理位置情報に基づいて、最も近いリージョンに接続します。
- パスコード：共有パスコード認証のブラウザーを選択した場合は、アプリにアクセスするときのセキュリティを強化するために、パスコードを入力します。パスコードは、最低 8 文字の英数字にする必要があります。パスコードを保存したことを確認してから、ユーザーと共有します。launch.cloud.com を使用してアプリを起動したときに、ユーザーがパスコードを入力する必要があります。

- アイコン：デフォルトでは、Secure Browser を公開するときに使用される Google Chrome の実行可能ファイルのアイコンです。公開ブラウザーに、独自のアイコンを表示することもできるようになりました。

  ［アイコンの変更］**>** ［アイコンの選択］の順にクリックし、アイコンを選択してアップロードするか、［デフォルトのアイコンを使用］を選択し、既存の Google Chrome のアイコンを使用します。

5. 完了したら、［公開］をクリックします。公開が完了すると、［管理］タブには、公開したブラウザーの一覧が表示されます。

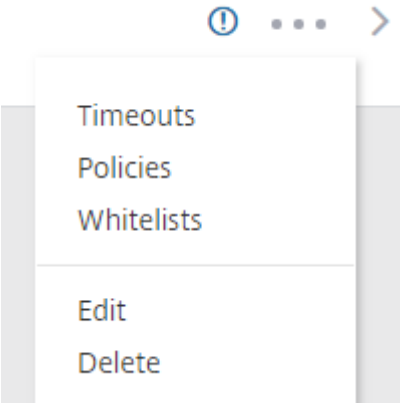
   - 認証済みのセキュア Web ブラウザーを公開した場合、Citrix Cloud のライブラリを使用してユーザーやグループを追加する必要があります。行末尾にある右矢印をクリックして、ライブラリへのリンクを含む詳細ペインを展開します。



   提供されたリンクをクリックし、説明に従って、作成したセキュアなブラウザーを含むライブラリ画面を表示します。セキュアなブラウザーを含むタイル内の省略記号をクリックし、［利用者を管理］をクリックします。利用者の追加について詳しくは、「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。

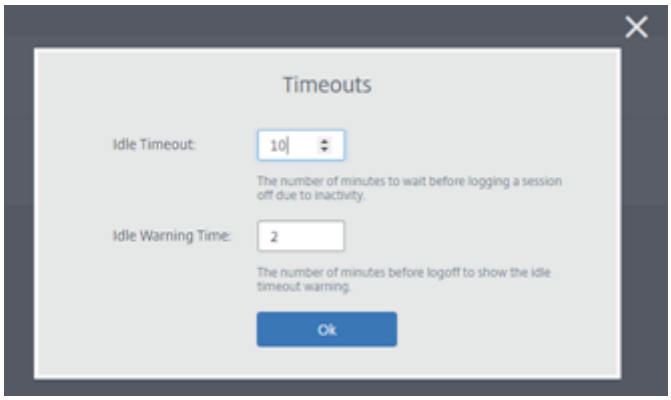
公開済みのセキュアなブラウザーの管理

［管理］タブに、公開済みのセキュアなブラウザーの一覧が表示されます。管理タスクを利用するには、項目の行末尾にある省略記号をクリックし、タスクを選択します。



メニュー項目を選択して変更せずに終了する場合は、ダイアログボックスの外側にある［**X**］をクリックして、選択をキャンセルします。

タイムアウト



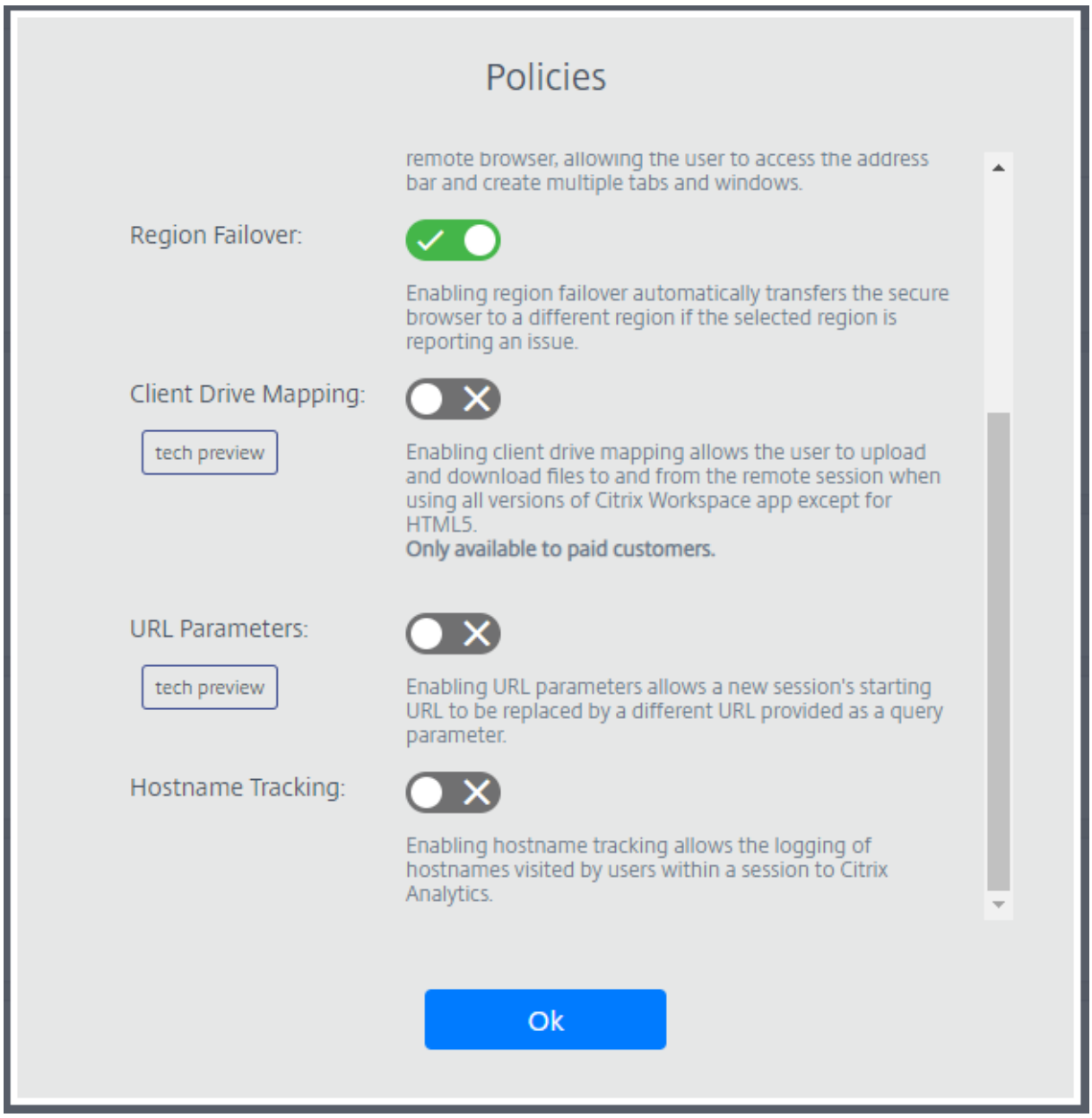
タイムアウト設定の種類は、次のとおりです：

- アイドルタイムアウト：非アクティブのセッションを終了する前にアイドル状態を維持できる時間（分）。
- アイドル警告の時間：警告メッセージがユーザーに送信されてからセッションが終了するまでの時間（分）。

たとえば、アイドルタイムアウトを「20」、アイドル警告の時間を「5」に設定した場合、セッションに 15 分間アクティビティがないと（20 − 5）、メッセージが表示されます。ユーザーが対応しないと、セッションは 5 分後に終了します。

設定を完了したら、［**OK**］をクリックします。

ポリシー

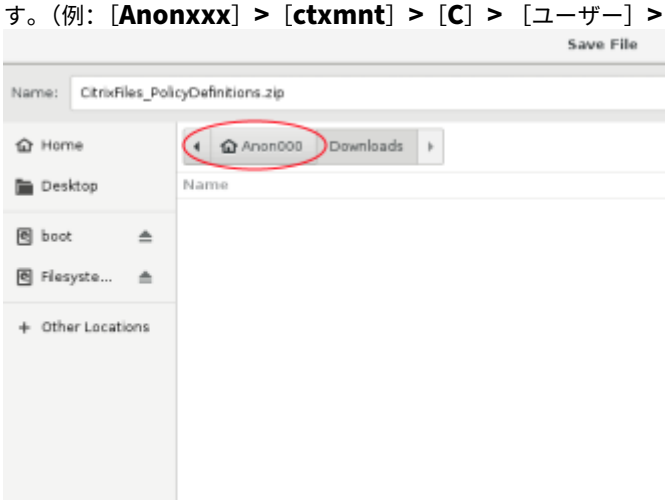


ポリシーページの設定により、次の項目を管理できます:

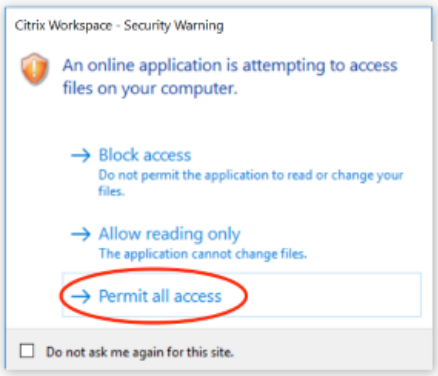
- クリップボード: クリップボードポリシーを有効にすると、リモートセッションとの間でコピーと貼り付けができるようになります。([クリップボード] ボタンが Citrix Workspace アプリのツールバーから削除されます。) デフォルトでは、この設定は無効になっています。
- 印刷: 印刷を有効にすると、リモート Web ページが PDF として保存され、ユーザーのデバイスに転送されます。ユーザーは、Ctrl+P キーを押して Citrix PDF プリンターを選択できます。デフォルトでは、この設定は無効になっています。
- 非キオスク: 非キオスクモードを有効にすると、インターフェイスがリモートブラウザーに復元されます。ユーザーは、ここでアドレスバーにアクセスして複数のタブとウィンドウを作成できます。(非キオスクモード

を無効にすると、リモートブラウザーの各ナビゲーションコントロールとアドレスバーが削除されます。）デフォルトでは、この設定は有効です（非キオスクモードがオンになっている）。

- リージョンフェールオーバー：現在のリージョンで問題が報告されている場合は、地域フェールオーバーポリシーにより、公開ブラウザーが自動的に別の地域に転送されます。オプトアウトするには、リージョンフェールオーバーポリシーを無効にします。リージョンの選択を ［自動］にして Web ブラウザーを公開すると、セキュアなブラウザーはポリシーに登録されたままになります。デフォルトでは、有効になっています。
- クライアントドライブマッピング：クライアントドライブマッピングポリシーを有効にすると、ユーザーは、リモートセッションとの間でファイルをアップロードおよびダウンロードできます。この機能は、Citrix Workspace アプリで開始されたセッションでのみ使用できます。デフォルトでは、この設定は無効になっています。
  - ダウンロードしたファイルは、必ず **Anonxxx**ディレクトリ内の**ctxmnt**ディスクに保存する必要があります。これを行うには、ユーザーはファイルを保存する場所を指定する必要があります。（例：［**Anonxxx**］**>** ［**ctxmnt**］**>** ［**C**］**>** ［ユーザー］**>**「ユーザー名」**>** ［ドキュメント］）



  - ダイアログボックスで、**ctxmnt**フォルダーへのすべてのアクセスを許可するか、読み取り/書き込みアクセスをどのように許可するかを指定します。



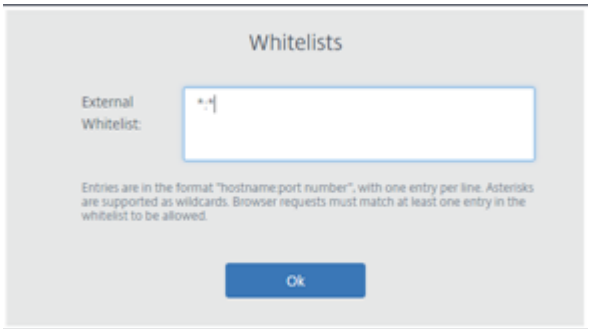
- **URL** パラメーター： URL パラメーターを有効にすると、ユーザーがアプリを起動した際に新しいセッションの開始 URL を変更できます。このポリシーを有効にするには、疑わしい Web サイトを特定し、それらを Secure Browser にリダイレクトするようローカルプロキシサーバーを構成します。デフォルトでは、この設定は無効になっています。詳しくは、「概念実証ガイド：Azure における Citrix ADC を使用した Secure

Browser への URL リダイレクト」を参照してください。

- ホスト名の追跡：ホスト名の追跡を使用して、ユーザーのセッション中に Secure Browser でホスト名をログに記録する機能を有効にします。このポリシーは、デフォルトでは無効になっています。この情報は、Citrix Analytics と共有されています。詳しくは、「Citrix Analytics」を参照してください。

設定を完了したら、[**OK**] をクリックします。

許可リスト



許可リストタスクでは、公開されたセキュアなブラウザーとのセッション内で、ユーザーが許可リストに登録された URL のみにアクセスできるように制限することができます。この機能は、外部認証済みの Web アプリで使用できます。

許可リストのエントリは「`hostname:port number`」の形式で入力します。1 行に 1 つずつ入力します。アスタリスクをワイルドカードとして使用できます。ブラウザーの要求は、許可リストの少なくとも 1 つのエントリと一致する必要があります。

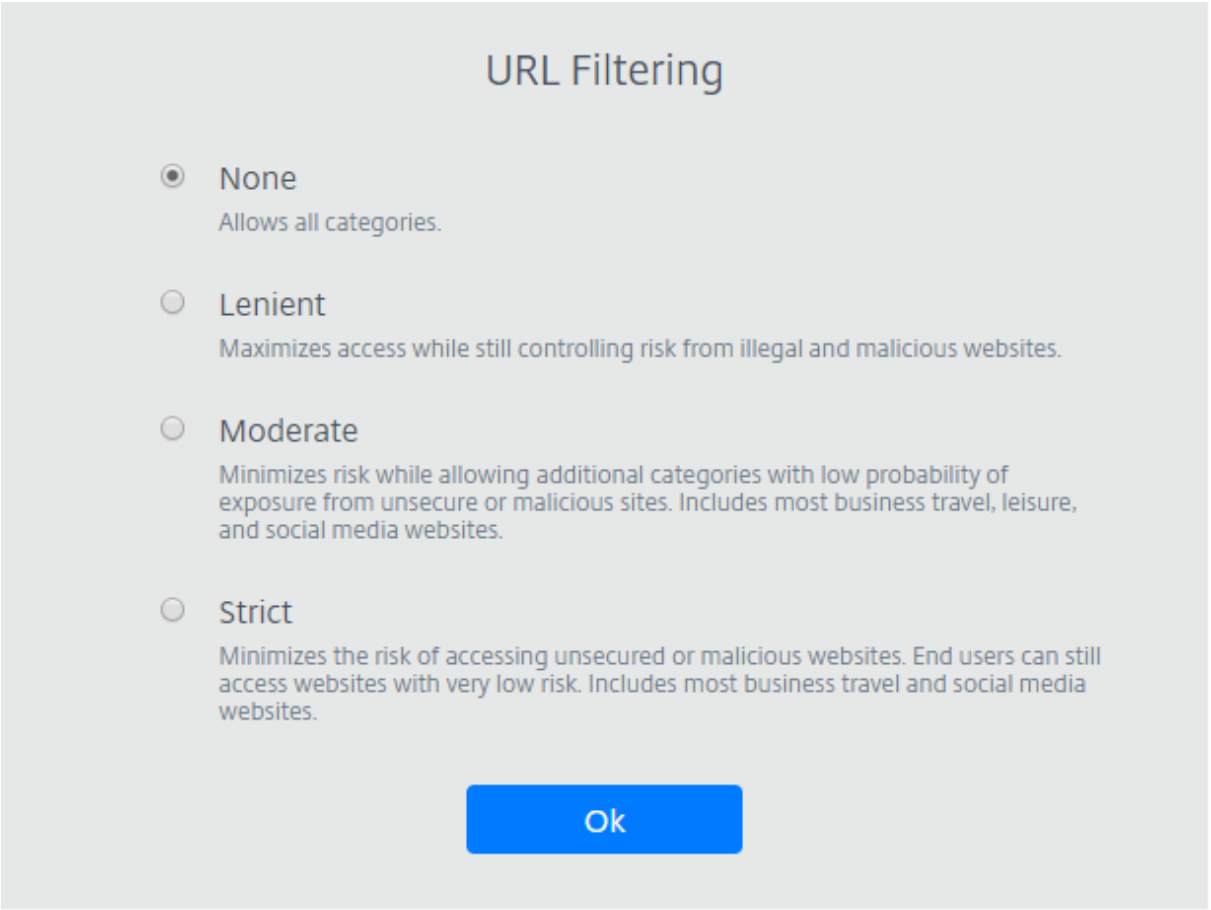
たとえば、許可された URL として`https://example.com`を設定するには:

- `example.com:*`と入力すると、任意のポートからこの URL に接続できます。
- `example.com:80`と入力すると、ポート 80 からのみこの URL への接続を許可します。
- `*:*`と入力すると、この URL への任意のポートからのアクセスと、ほかの URL やポートへの任意のリンクからのアクセスを許可します。「`*.*`」の形式で入力すると、公開アプリからすべての外部 Web アプリへのアクセスが許可されます。この形式は、Web アプリの外部の許可リストに指定するデフォルト設定です。

設定を完了したら、[**OK**] をクリックします。

アクセス制御サービスと統合すると、高度な Web フィルター機能が利用できます。詳しくは、「ユースケース：アプリへのアクセスを選択的に許可するアクセスポリシーを設定する」を参照してください。

URL フィルタリング



リスクモデルに関連した事前定義のカテゴリごとにアクセス方法を制御するよう URL フィルタリングを構成できます。以下は、URL フィルタリングオプションです:

- なし - すべてのカテゴリを許可します。
- 低 - 不正または悪意のある Web サイトによるリスクを管理しながら、Web サイトに最大限アクセスできるようにします。次のカテゴリが含まれます:
  - 成人：猟奇描写、性教育、ポルノ、ヌード、性的サービス、アダルト検索/リンク、水着と下着、アダルト雑誌とニュース、性的表現（テキスト）、フェチ、出会い系。
  - コンピューティングとインターネット：リモートプロキシ、プライベート IP アドレス、ピアツーピアのファイル共有、トレント。
  - ギャンブル：懸賞、賞品、宝くじ、ギャンブル全般。
  - 違法で有害：テロリズム、過激派、誹謗、中傷、武器、暴力、自殺、違法薬物、薬物、違法行為、マリファナ、主義主張全般。
  - マルウェアとスパム：ハッキング、マルウェア、スパム、スパイウェア、ボットネット、感染サイト、フィッシングサイト、キーロガー、モバイルマルウェア、電話ボット、悪意および危険がある Web サイト。
- 中 - リスクを最小限に抑えながら、セキュリティ保護されていない Web サイトや悪意のある Web サイトへ

の露出の可能性が低いカテゴリを許可します。次のカテゴリが含まれます:

- 成人：猟奇描写、性教育、ポルノ、ヌード、性的サービス、アダルト検索/リンク、水着と下着、アダルト雑誌とニュース、性的表現（テキスト）、フェチ、出会い系。
- ビジネスと産業：オークション。
- コンピューティングとインターネット：広告、バナー、リモートプロキシ、プライベート IP アドレス、ピアツーピアファイル共有、トレント。
- ダウンロード：モバイルアプリストア、ストレージサービス、ダウンロード、プログラムのダウンロード。
- メール： Web ベースのメールおよびメールサブスクリプション。
- 金融：暗号通貨。
- ギャンブル：懸賞、賞品、宝くじ、ギャンブル全般。
- マルウェアとスパム：ハッキング、マルウェア、スパム、スパイウェア、ボットネット、感染サイト、フィッシングサイト、キーロガー、モバイルマルウェア、電話ボット、悪意および危険がある Web サイト。
- メッセージング、チャット、電話：インスタントメッセージおよび Web ベースのチャット。
- ニュース、娯楽、社会： Wordpress（投稿とアップロード）、サポートされていない URL、オカルト、コンテンツなし、その他、ホロスコープ、占星術、運勢判断、飲酒、宗教、個人の Web ページ、ブログ、オンラインゲーム。
- ソーシャルネットワーク：写真の検索および共有サイト、IT 掲示板、掲示板。

- 高 - セキュリティ保護されていない Web サイトや悪意のある Web サイトにアクセスするリスクを最小限に抑えます。エンドユーザーは、引き続きリスクの低い Web サイトにアクセスできます。次のカテゴリが含まれます:
  - 成人：猟奇描写、性教育、ポルノ、ヌード、性的サービス、アダルト検索/リンク、水着と下着、アダルト雑誌とニュース、性的表現（テキスト）、フェチ、出会い系。
  - ビジネスと産業：オークション。
  - コンピューティングとインターネット：広告、バナー、動的 DNS、モバイルアプリ、パブリッシャー、パークドメイン、リモートプロキシ、プライベート IP アドレス、ピアツーピアファイル共有、トレント。
  - ダウンロード：モバイルアプリストア、ストレージサービス、ダウンロード、プログラムのダウンロード。
  - メール： Web ベースのメールおよびメールサブスクリプション。
  - 金融：暗号通貨と金融商品。
  - ギャンブル：懸賞、賞品、宝くじ、ギャンブル全般。
  - 違法で有害：テロリズム、過激派、誹謗、中傷、武器、暴力、自殺、違法薬物、薬物、違法行為、マリファナ、主義主張全般。
  - 求人と履歴書：雇用、キャリアアップ、LinkedIn（更新、メール、接続、ジョブ）。
  - マルウェアとスパム：ハッキング、マルウェア、スパム、スパイウェア、ボットネット、感染サイト、フィッシングサイト、キーロガー、モバイルマルウェア、電話ボット、悪意および危険がある Web サイト。
  - メッセージング、チャット、電話：インスタントメッセージおよび Web ベースのチャット。
  - ニュース、娯楽、社会： Wordpress（投稿とアップロード）、宿泊施設、旅行と観光、サポートされていない URL、政治、ファッションと美容、芸術と文化的イベント、リファレンス、レジャーと趣味、地

域社会、その他、飲酒、人気のトピック、特別なイベント、ニュース、社会と文化、オンライン雑誌、オンラインゲーム、ライフイベント、オカルト、コンテンツなし、星占い、占星術、運勢判断、有名人、ストリーミングメディア、娯楽、施設、アクティビティ、個人の Web ページとブログ、宗教。

- ソーシャルネットワーク：ソーシャルネットワーク全般、YikYak（投稿）、Twitter（投稿、メール、フォロー）、Vine（アップロード、コメント、メッセージ）、Google+（写真とビデオのアップロード、投稿、ビデオチャット、コメント）、Instagram （アップロードとコメント）、YouTube（共有とコメント）、Facebook（グループ、ゲーム、質問、ビデオのアップロード、写真のアップロード、イベント、チャット、アプリ、投稿、コメント、友達）、Tumblr（投稿、コメント、写真、ビデオのアップロード）、Pinterest（ピンとコメント）、IT 掲示板、掲示板。

設定を完了したら、［**OK**］をクリックします。

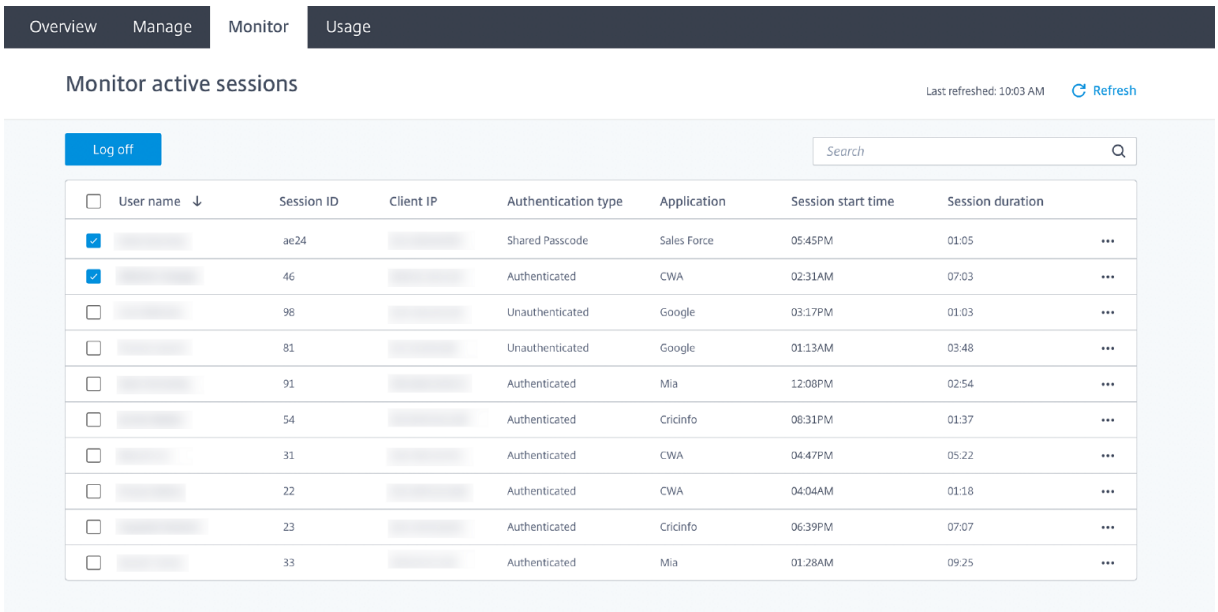
編集

編集タスクでは、公開されたブラウザーの名前、開始 URL、リージョン、またはパスコードを変更することができます。完了したら、［公開］をクリックします。

削除

削除タスクでは、公開されたセキュアなブラウザーを削除することができます。このタスクを選択すると、削除確認メッセージが表示されます。

アクティブなセッションを監視

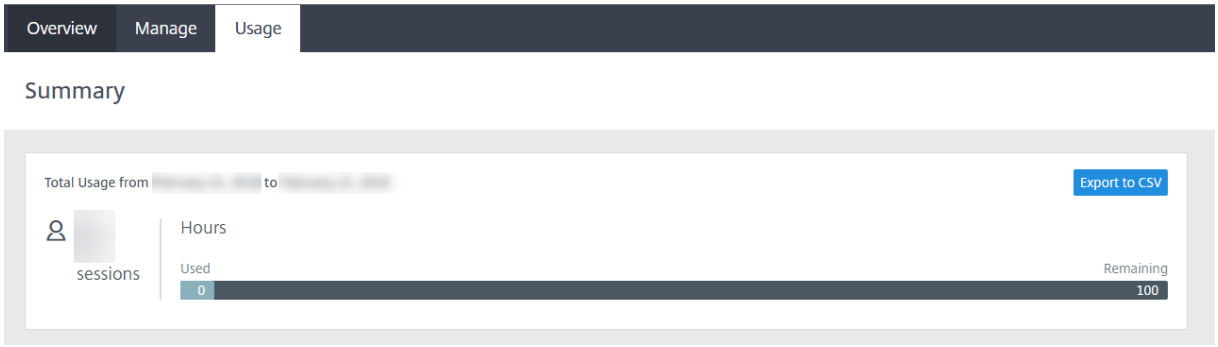


［監視］タブには、ユーザーのリアルタイムセッションに関する情報が表示されます。1 つまたは複数のアクティブなセッションを監視および切断できます。

単一のセッションを停止するには、セッションを選択し、エントリの行の最後にある省略記号メニューをクリックします。［セッションのログオフ］をクリックして、変更を確認します。

複数のセッションを切断するには、一覧からアクティブなセッションを選択し、ページ上部の ［ログオフ］ボタンをクリックします。変更を確認すると、Secure Browser は選択したすべてのセッションを直ちに切断します。

使用状況の監視



［使用状況］タブには以下の内容が表示されます：

- 開始セッション数
- 使用期間（時間）

使用状況の詳細を含むスプレッドシートを作成するには、［**CSV** にエクスポート］をクリックして、確認する期間を選択します。

セキュリティの技術概要

Secure Browser サービスは、シトリックスによって管理および運用される SaaS 製品です。このサービスを使用すると、クラウドでホストされている Web ブラウザーを介して Web アプリケーションにアクセスできます。

クラウドサービス

Citrix Secure Browser サービスは、Virtual Delivery Agents（VDA）上で実行される Web ブラウザーと、ユーザー管理とこれらの VDA へのユーザー接続を行う管理コンソールで構成されています。Citrix Cloud は、オペレーティングシステム、Web ブラウザー、および Citrix コンポーネントのセキュリティおよびパッチ適用など、これらのコンポーネントの運用を管理します。

Secure Browser サービスを使用している間、ホストされている Web ブラウザーはユーザーの閲覧履歴を追跡し、HTTP 要求のキャッシュを実行します。固定プロファイルが使用されているため、閲覧セッションが終了するとこのデータは確実に削除されます。

Secure Browser サービスには、HTML5 対応の Web ブラウザーでアクセスします。このサービスでは、ダウンロード可能なクライアントは使用しません。使用するブラウザーとクラウドサービスの間のすべてのトラフィックは、業界標準の TLS で暗号化されています。Secure Browser は、TLS 1.2 のみをサポートしています。

Secure Browser の出力トラフィックは、指定の IP アドレスを使用して内部ネットワークを保護します。受け入れる IP アドレスのリストについては、Knowledge Center の記事「CTX286379」を参照してください。

Web アプリケーション

Citrix Secure Browser サービスは、顧客またはサードパーティの Web アプリケーションを配信するために使用されます。Web アプリケーションの所有者にはセキュリティを管理する責任があり、Web サーバーとアプリケーションの脆弱性に対するパッチ適用などを行います。

Secure Browser と Web アプリケーション間のトラフィックのセキュリティは、Web サーバーの暗号化設定によって異なります。インターネット上でこのトラフィックを保護するため、管理者は HTTPS の URL を公開します。

詳細情報

セキュリティ情報について詳しくは、次のリソースを参照してください:

- シトリックスセキュリティサイト: https://www.citrix.com/security
- Citrix Cloud ドキュメント: セキュリティで保護された Citrix Cloud プラットフォームの展開ガイド

そのほかの情報の入手先

開発者向け: Secure Browser Service の API（Tech Preview）

Citrix Virtual Apps Essentials

June 15, 2021

Citrix Virtual Apps Essentials を使用すると、Microsoft Azure の Windows アプリケーションおよびホストされた共有デスクトップを、あらゆるデバイス上のあらゆるユーザーに配信できます。本サービスは、業界トップクラスの Citrix Virtual Apps サービスと、Microsoft Azure の機能および柔軟性を組み合わせたものです。Virtual Apps Essentials により、Windows Server デスクトップを公開することもできます。

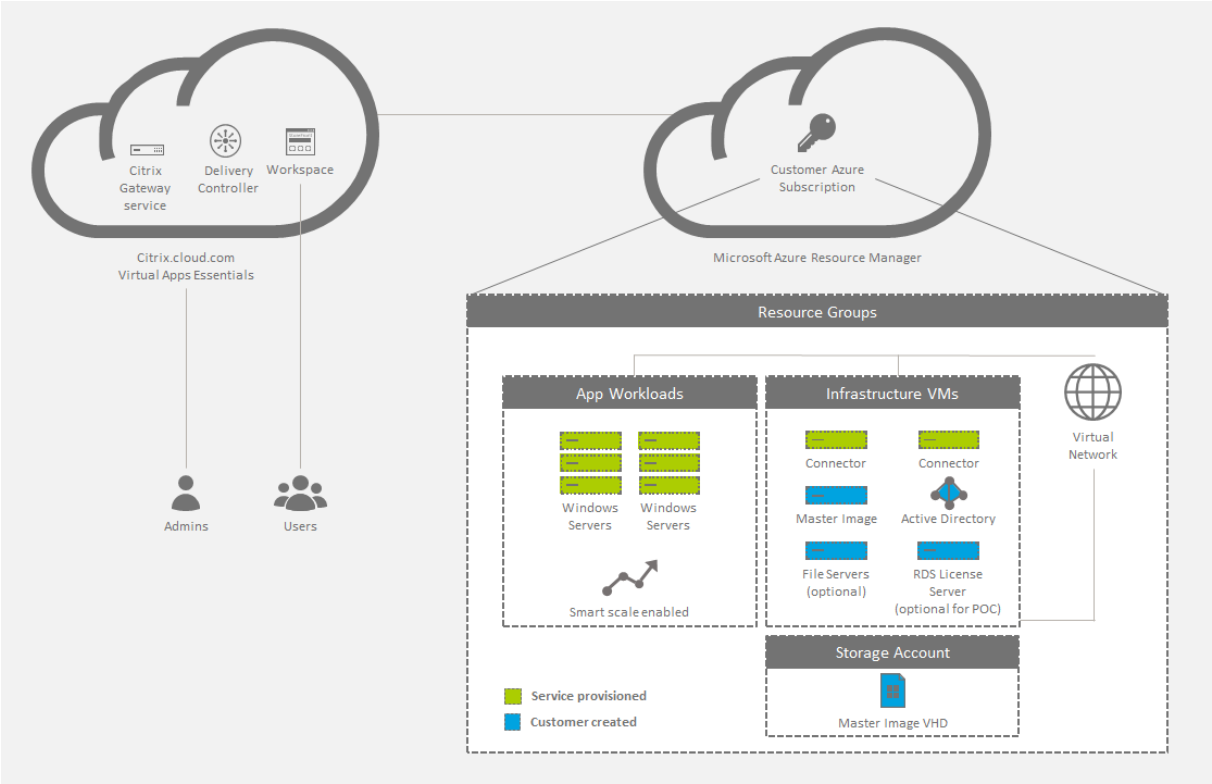
サーバー OS マシンは、単一マシン上で複数のセッションを実行して、同時に接続する複数のユーザーに複数のアプリケーションとデスクトップを配信します。各ユーザーは、単一のセッション内ですべてのアプリケーションを実行します。

本サービスは Citrix Cloud を通じて提供されるものであり、アプリワークロードを Azure サブスクリプション内へ簡単に展開できます。ユーザーがワークスペース環境からアプリケーションを開くと、アプリケーションは、見かけ上はユーザーのコンピューター上でローカルに実行されます。ユーザーは、場所を問わず任意のデバイスからアプリに安全にアクセスできます。

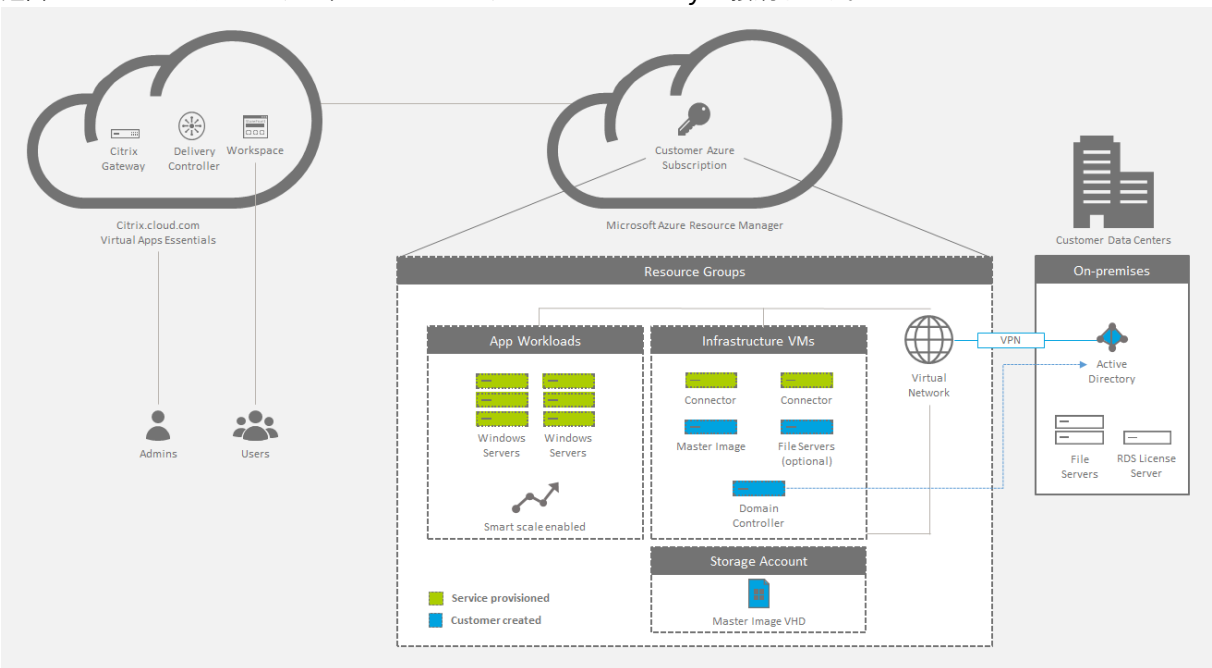
Virtual Apps Essentials には、コア管理サービスに加え、ワークスペース環境とCitrix Gateway サービスが含まれています。アプリワークロードは、Azure サブスクリプション内で実行されます。

展開アーキテクチャ

次の図に、基本的な Virtual Apps Essentials のクラウド展開アーキテクチャの概要を示します:



オンプレミスデータセンターにユーザーが接続できるようにすることも可能です。Azure クラウドとオンプレミスデータセンター間の接続は、VPN 接続を介して行われます。ユーザーは Virtual Apps Essentials を通じ、VPN 接続経由でライセンスサーバー、ファイルサーバー、Active Directory に接続します。



展開の要約

Citrix Virtual Apps Essentials を展開するには、次の手順を実行します:

- Azure Marketplace で Citrix Virtual Apps Essentials を購入します。
- Azure サブスクリプションを準備して関連付けます。
- マスターイメージを作成してアップロードします。
- カタログの展開、アプリとデスクトップの公開、および利用者の割り当て

新機能

- 2018 年 12 月: クラウドホスト **StoreFront** が削除されました

  クラウドホスト StoreFront は、Virtual Desktops Essentials で使用できなくなりました。2017 年 12 月以前に Virtual Desktops Essentials（XenDesktop Essentials の新名称）を購入したお客様は、この記事で説明しているように、Citrix Workspace を使用して、利用者にデスクトップアクセスを提供できます。

- 2018 年 8 月: 新しい製品名

  一定期間シトリックスのお客様かパートナーだった経験がある方は、製品や製品ドキュメントに新しい名前が使用されていることにお気付きになるかもしれません。このシトリックス製品を初めてお使いになる場合、製品またはコンポーネントで異なる名前が表示されることがあります。

  新しい製品名とコンポーネント名は、シトリックスの製品ラインとクラウド戦略の拡大によるものです。ここでは、次の名前を使用します。

  - **Citrix Virtual Apps Essentials**: XenApp は、多くの種類のアプリを希望する場所に集約して、ここから業務用ツールにアクセスできるようにするという、シトリックスのワークスペース戦略の一部です。XenApp Essentials は、統一された状況に応じた安全なワークスペースの一環として、Citrix Virtual Apps Essentials になりました。
  - **Citrix Workspace** アプリ: Citrix Workspace アプリには、既存の Citrix Receiver テクノロジやその他の Citrix Workspace クライアントテクノロジが組み込まれています。エンドユーザーに最高の作業を実行するために必要なすべての作業アプリ、ファイル、およびデバイスと対話できる統合されたコンテキスト上のエクスペリエンスをエンドユーザーに提供するための追加機能を提供するように拡張されました。
  - **Citrix Gateway**: NetScaler Unified Gateway は、Citrix Gateway になっています。Citrix Gateway を使うと、最高の作業を行うために必要なアプリやデータに安全かつコンテキストに応じたアクセスが可能になります。

  製品内のコンテンツには、以前の名前が含まれている場合があります。たとえば、コンソールのテキスト、メッセージ、ディレクトリ名またはファイル名に以前の名前が含まれている場合があります。既存のお客様のスクリプトの破損を防ぐために、コマンドや MSI などの一部のアイテムでは、以前の名前を引き続き保持できます。

関連する製品ドキュメント、その他の情報（ビデオやブログの投稿など）、その他のサイト（Azure Marketplace など）には以前の名前が含まれている可能性があります。この移行の間はご迷惑をおかけしますが、何卒ご容赦願います。新しい名前について詳しくは、https://www.citrix.com/about/citrix-product-guide/を参照してください。

- 2018 年 5 月：**Virtual Apps Essentials** のインターフェイスから追加のイメージを作成する

  Azure Resource Manager インターフェイスで実稼働環境用のイメージを作成した後、必要に応じて、Azure で追加のイメージを作成できます。新機能として、追加のイメージを Azure インターフェイスで作成する代わりに、Virtual Apps Essentials インターフェイスで新しいマスターイメージを作成できるようになりました。詳しくは、「マスターイメージの準備とアップロード」を参照してください。

- 2018 年 5 月：モニター表示の機能拡張

  ［モニター］画面に、アプリケーションおよび使用頻度の高いユーザーに関する使用状況の情報が表示されるようになりました。詳しくは、「サービスを監視する」を参照してください。

システム要件

Microsoft Azure

Citrix Virtual Apps Essentials のマシンの構成は、Azure Resource Manager を介してのみ行うことができます。

Azure Resource Manager は次の目的に使用します：

- 仮想マシン（VM：Virtual Machine）、ストレージアカウント、仮想ネットワークなどのリソースの展開
- リソースグループ（グループとして管理するリソースのコンテナ）の作成および管理

Microsoft Azure にリソースをプロビジョニングし展開するには、次のものが必要です：

- Azure アカウント
- Azure Resource Manager サブスクリプション
- 使用するサブスクリプションに関連付けられているディレクトリの Azure Active Directory グローバル管理者アカウント。ユーザーアカウントには、リソースのプロビジョニングに使用する Azure サブスクリプションの所有者権限が設定されている必要があります。Azure Active Directory テナントの設定方法について詳しくは、「How to get an Azure Active Directory tenant」を参照してください。

Citrix Cloud

Virtual Apps Essentials は Citrix Cloud を通じて提供されるため、オンボードプロセスを完了するには Citrix Cloud アカウントが必要になります。Azure Marketplace にアクセスしてトランザクションを完了する前に、Citrix Cloud への登録ページで Citrix Cloud アカウントを作成できます。

既存の Citrix Virtual Apps and Desktops サービスまたは Citrix Virtual Desktops Essentials サービスのアカウントに Citrix Cloud アカウントをリンクすることはできません。

Virtual Apps Essentials コンソール

Virtual Apps Essentials 管理コンソールは、次の Web ブラウザーで開くことができます:

- Google Chrome
- Internet Explorer

既知の問題

Virtual Apps Essentials には、次の既知の問題があります:

- Windows Server 2019 VDA では、構成中およびユーザーのワークスペースに、一部のアプリケーションアイコンが正しく表示されない場合があります。回避策として、アプリケーションの公開後に、正しく表示される別のアイコンを割り当てる ［アイコンの変更］機能を使用します。
- Azure AD Domain Services を使用する場合：ワークスペースのログオン UPN（User Principal Name: ユーザープリンシパル名）には、Azure AD Domain Services の有効化時に指定したドメイン名を含める必要があります。作成したカスタムドメインをプライマリとして指定している場合でも、ログオンにカスタムドメインの UPN を使用することはできません。
- カタログのユーザーを構成してドメインを選択すると、Builtin\Users グループのユーザーを表示および選択できます。
- 指定した仮想マシンサイズが選択したリージョンで利用できない場合、カタログを作成できません。お客様のリージョンで利用可能な仮想マシンを確認するには、Microsoft の Web サイトでリージョン別の利用可能な製品の図を参照してください。
- 同じアプリの複数のインスタンスを一度に［スタート］メニューから作成し公開することはできません。たとえば、［スタート］メニューから Internet Explorer を公開したとします。その後、指定した Web サイトを起動時に開く Internet Explorer の 2 番目のインスタンスを公開するとします。これを行うには、2 番目のアプリは、［スタート］メニューではなくアプリのパスを使用して公開します。
- Virtual Apps Essentials では、Azure Active Directory ユーザーアカウントを使用したサブスクリプションのリンクをサポートしています。Live.com 認証アカウントはサポートされません。
- VDA に既存のリモートデスクトッププロトコル（RDP：Remote Desktop Protocol）セッションがある場合、ユーザーはアプリケーションを起動できません。この現象は、VDA に他のユーザーがログオンしていないときに RDP セッションが開始された場合にのみ発生します。
- server.domain.subdomain よりも長いライセンスサーバーアドレスは入力できません。
- 容量管理に対して複数の更新を連続して行うと、更新後の設定が VDA に正しく反映されない可能性があります。
- 英語以外の Web ブラウザーを使用する場合、テキストは英語とブラウザーの言語を組み合わせて表示されます。

サービスの購入方法

> 注:
>
> このセクションの情報をPDFでダウンロードすることもできます。PDF には、以前の製品名が含まれています。

Citrix Virtual Apps Essentials は、Microsoft Azure アカウントを使ってAzure Marketplaceから直接購入します。Citrix Virtual Apps Essentials には、少なくとも 25 人のユーザーが必要です。

このサービスは Citrix Cloud を通じて提供されるため、オンボードプロセスを完了するには Citrix Cloud アカウントが必要になります。詳しくは、「システム要件」の「Citrix Cloud」セクションを参照してください。

Citrix Virtual Apps Essentials の購入時は、注文が迅速に処理されるように、アドレスを含むすべての情報が正しく入力されていることを確認してください。Virtual Apps Essentials を構成する前に、Azure Marketplace で次の操作を完了していることを確認します:

- 連絡先情報と会社の詳細を入力します。
- 請求情報を提供します。
- サブスクリプションを作成します。

顧客（ユーザー）と価格を設定するには:

1. ［ユーザーの選択］で、顧客の名前を選択します。
2. ［価格設定］で、［ユーザー数］に Virtual Apps Essentials にアクセスできるユーザー数を入力します。
3. ［月額］で、同意書のチェックボックスをオンにして ［作成］をクリックします。

概要ページが開き、リソースの詳細が表示されます。

アカウントがプロビジョニングされたら、［**Citrix Cloud** による管理］をクリックします。

> 重要:
>
> Microsoft Azure によるサービスのプロビジョニングが完了するまで待ってください。プロビジョニングが完了するまでは、［**Citrix Cloud** による管理］をクリックしないでください。このプロセスには最大 4 時間かかります。

リンクをクリックすると、Web ブラウザで Citrix Cloud が開き、以下で説明する構成プロセスを開始できます。

Azure サブスクリプションの準備

VDA および関連リソースのホスト接続に使用する Azure サブスクリプションを選択します。これらのリソースについては、使用状況に基づいて課金されることがあります。

> 注:
>
> 本サービスを利用するには、Azure Active Directory アカウントでログオンする必要があります。live.com などの他の種類のアカウントはサポートされません。

Azure サブスクリプションの準備をするには、Azure Resource Manager で以下の構成を行います:

1. リソースグループを作成して次を指定します:
    - リソースグループ名

- サブスクリプション名
- 位置情報

2. Azure Resource Manager で、仮想ネットワークをリソースグループに作成して名前をつけます。他のすべての設定についてはデフォルト値のままで構いません。ストレージアカウントはマスターイメージの作成時に作成します。

3. ドメインコントローラーは既存のものを使用するか、新しく作成します。ドメインコントローラーを作成する場合は次の手順を実行します:

   a) 作成したリソースグループおよび仮想ネットワーク内に、A3 標準サイズまたはその他のサイズの Windows Server 2012 R2 仮想マシンを作成します。この仮想マシンがドメインコントローラーになります。ドメインコントローラーを複数作成する場合は、可用性セットを作成し、すべてのドメインコントローラーをこのセットに配置します。
   b) プライベート静的 IP アドレスを仮想マシンのネットワークアダプターに割り当てます。アドレスの割り当ては Azure Portal で行います。詳しくは、Microsoft 社のドキュメント Web サイトで「Configure private IP addresses for a virtual machine using the Azure portal」を参照してください。
   c) [オプション]Active Directory のユーザーおよびグループと Active Directory ログを保存する新規データディスクを仮想マシンに接続します。詳しくは、「Azure portal を使用して Windows VM にマネージドデータディスクを接続する」を参照してください。ディスクを接続するときには、すべてのオプションをデフォルト設定のままにします。
   d) ドメインコントローラー仮想マシンのプライベート IP アドレスを仮想ネットワーク DNS サーバーに追加します。詳しくは、「Manage DNS servers used by a virtual network (Classic) using the Azure portal (Classic)」を参照してください。
   e) Microsoft DNS サーバーに加えて、パブリック DNS サーバーを追加します。この 2 番目の DNS サーバーの IP アドレスには、168.63.129.16 を使用します。
   f) ドメインコントローラー仮想マシンに、Active Directory Domain Services の役割を追加します。この手順が完了したら、ドメインコントローラー仮想マシンをドメインコントローラーと DNS に昇格させます。
   g) フォレストを作成し、Active Directory ユーザーを追加します。詳しくは、「Install a new Active Directory forest on an Azure virtual network」を参照してください。

ドメインコントローラーの代わりに Azure Active Directory Domain Services を使用する場合は、Microsoft Web サイトの「Azure Active Directory Domain Services for Beginners」を参照することをお勧めします。

Azure サブスクリプションを関連付ける

Citrix Cloud で、Citrix Virtual Apps Essentials を Azure サブスクリプションにリンクします。

1. Citrix Cloudにサインインします。左上のメニューで、［マイサービス］**>** ［**Virtual Apps and Desktops**］を選択します。
2. ［管理］タブで ［**Azure** サブスクリプション］をクリックします。
3. ［サブスクリプションの追加］をクリックします。Azure Portal が開きます。

4. グローバル管理者の Azure 資格情報で、Azure サブスクリプションにログオンします。
5. ［同意する］をクリックして、Virtual Apps Essentials で Azure アカウントにアクセスできるようにします。ログオンしたアカウントで利用可能なサブスクリプションが一覧表示されます。
6. 使用するサブスクリプションを選択し、［リンク］をクリックします。
7. Virtual Apps Essentials コンソールに戻り、選択したサブスクリプションがリンク状態になっていることを確認します。

Azure サブスクリプションを Virtual Apps Essentials にリンクしたので、次にマスターイメージをアップロードします。

マスターイメージの準備とアップロード

カタログの作成時には、マスターイメージを使用して、アプリケーションとデスクトップが含まれる VM を展開します。このマスターイメージには、お客様が用意しアプリケーションおよび VDA をインストールしたイメージ、またはシトリックスが作成したイメージを使用できます。実稼働環境では、お客様自身のマスターイメージを準備して使用することをお勧めします。シトリックスが作成したイメージは、パイロット展開およびテスト展開のみを目的としています。

最初の実稼働環境用イメージは、Azure Resource Manager インターフェイスで準備する必要があります。以降は、必要に応じて Azure で追加のイメージを作成できます。

追加のイメージを Azure インターフェイスで作成する代わりに、Virtual Apps Essentials インターフェイスで新しいマスターイメージを作成することも可能です。

- この方法では、作成済みのマスターイメージを使用します。ネットワーク設定については、既存のカタログから取得することも、手動で指定することもできます。
- 既存のマスターイメージを使用して新規イメージを作成したら、そのイメージを接続し、アプリを追加したり、テンプレートからコピーしたアプリを削除するなどしてカスタマイズします。VDA はインストール済みのため、再度インストールする必要はありません。
- この方法は Essentials サービスに留まったまま行うことができます。Azure にアクセスして新しいイメージを作成し、Essentials サービスに戻ってイメージをインポートする必要はありません。

たとえば、複数の HR アプリが含まれるマスターイメージを使用する、HR という名前のカタログがあるとします。最近、新しいアプリが公開されたので、このアプリを HR カタログユーザーに公開します。Virtual Apps Essentials のイメージ作成機能を使用して、現在のマスターイメージをテンプレートとして選択し、新しいマスターイメージを作成します。また、新しいマスターイメージで同じネットワーク接続設定を使用するように、HR カタログも選択します。最初のイメージができたら、このイメージに新しいアプリをインストールします。テスト後、新しいマスターイメージで HR カタログを更新し、更新後の HR カタログをカタログユーザーに公開します。元の HR マスターイメージは、再び必要になる場合があるため、［マイイメージ］リストに保持されます。

次のセクションでは、Azure インターフェイスで、マスターイメージを準備してアップロードする方法について説明します。Virtual Apps Essentials でイメージを作成する方法について詳しくは、「Virtual Apps Essentials でマスターイメージを準備する」を参照してください。

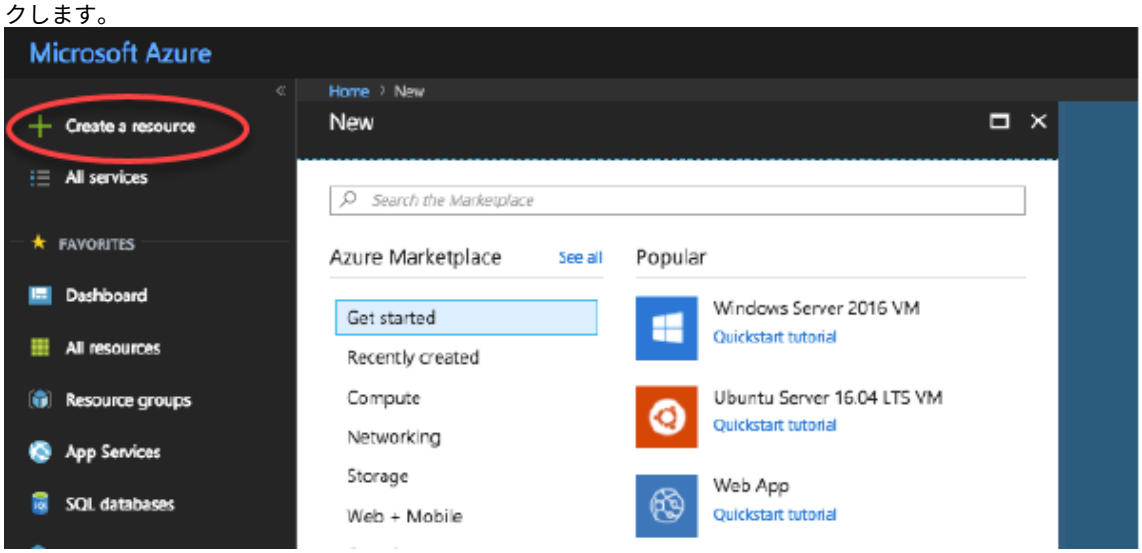
手順の概要

1. Azure または Virtual Apps Essentials でマスターイメージ VM を準備します。
2. マスターイメージにアプリをインストールします。
3. マスターイメージに Citrix VDA をインストールします。
4. マスターイメージを Azure Resource Manager から Virtual Apps Essentials にアップロードします（必要な場合）。

サーバー VDA の最新リリース（CR：Current Release）かサーバー VDA 7.15 の長期サービスリリース（LTSR：Long Term Service Release）の最新の累積更新プログラム（CU：Cumulative Update）を、Windows Server 2016 マシンまたは Windows Server 2012 R2 マシンにインストールすることをお勧めします。Windows Server 2008 R2 を使用する場合は、サーバー VDA 7.15 LTSR（最新の CU を推奨）をインストールする必要があります。この VDA はダウンロードページでも入手できます。CR および LTSR VDA のライフサイクルポリシーについては、「Lifecycle Policy for Citrix Cloud Virtual Apps and Desktops Service」を参照してください。

Azure でマスターイメージ **VM** を作成する

1. Azure ポータルにサインインします。
2. ナビゲーションペインで ［リソースの作成］ をクリックします。Windows Server 2008 R2、Windows Server 2012 R2、または Windows Server 2016 のエントリを選択するか、検索します。［作成］ をクリックします。

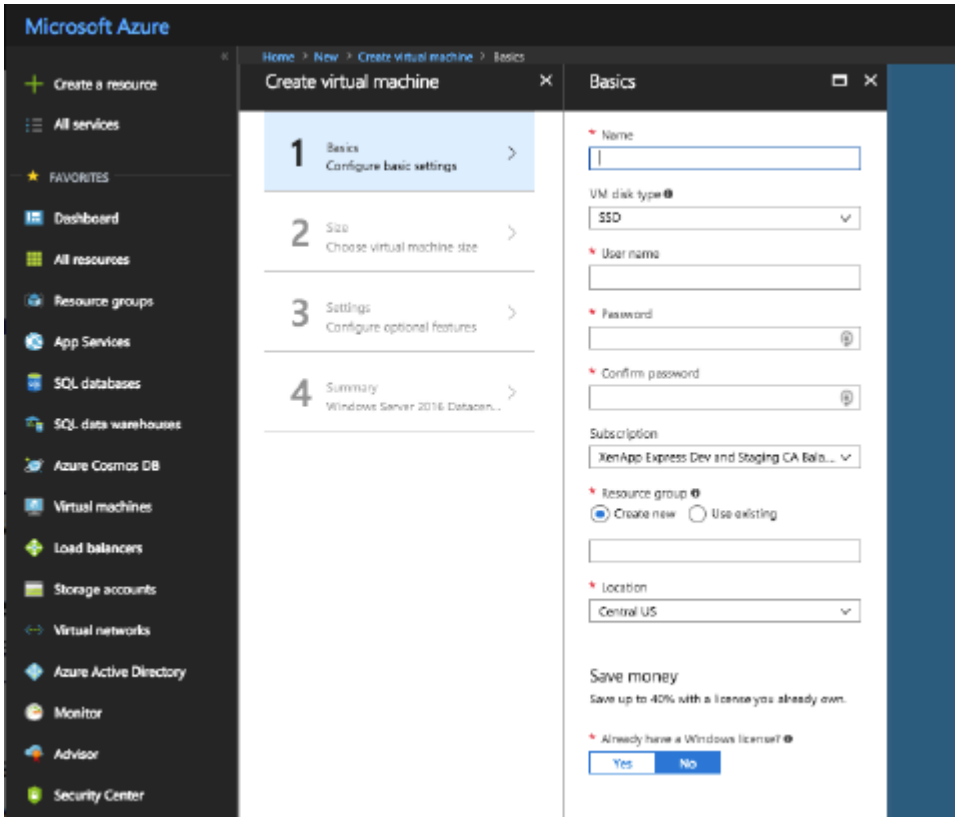


3. ［仮想マシンの作成］ページの ［1 基本］ パネルで次の操作を行います：
   a) VM の名前を入力します。
   b) VM ディスクの種類を選択します（オプション）。標準ディスクを作成します。
   c) ローカルユーザーの名前とパスワード、および確認用のパスワードを入力します。
   d) サブスクリプションを選択します。
   e) 新しいリソースグループを作成するか、既存のリソースグループを選択します。
   f) 場所を選択します。

g) リソースグループと場所を選択します。

h) 既に所有している Windows ライセンスを使用するかどうかを選択します。

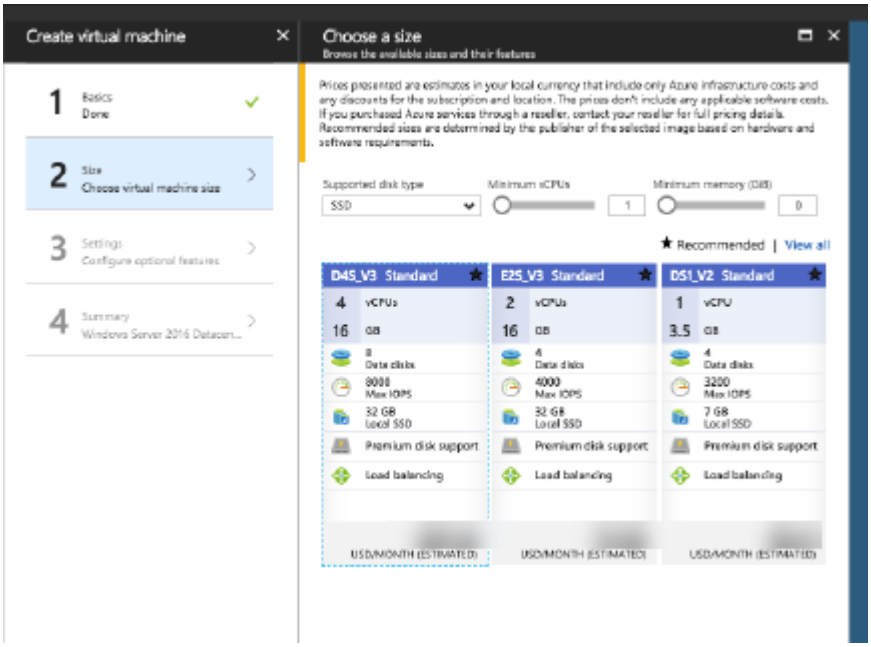
i) [**OK**] をクリックします。



4. [仮想マシンの作成] ページの [2 サイズ] パネルで、仮想マシンのサイズを選択します:

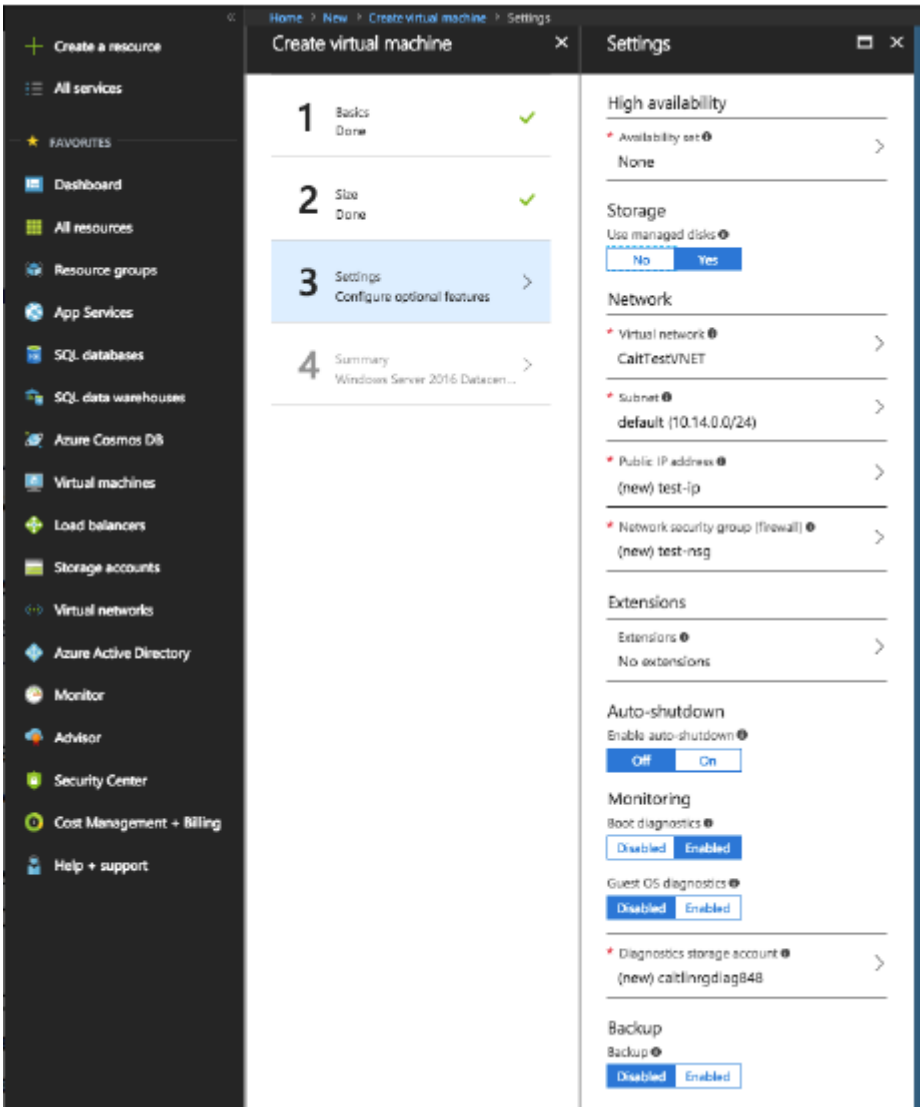
a) VM の種類を選択し、vCPU の最小数と最小メモリを指定します。推奨される選択肢が表示されます。すべての選択肢を表示することも可能です。

b) サイズを選び、[選択] をクリックします。



5. [仮想マシンの作成] ページの [3 設定] パネルで次の操作を行います:

   a) 高可用性を使用するかどうかを指定します。
   b) 仮想ネットワーク名、サブネット、パブリック IP アドレス、ネットワークセキュリティを指定します。
   c) 必要に応じて、拡張機能を選択します。
   d) 自動シャットダウンおよび監視の各オプション（ブート診断、ゲスト OS 診断、診断ストレージアカウント）を有効または無効にします。
   e) バックアップを有効または無効にします。
   f) [**OK**] をクリックします。



6. [4 概要] パネルで [**OK**] をクリックし、VM の作成を開始します。

Sysprep は使用しないでください。

マスターイメージにアプリをインストールする

作成したマスターイメージ VM に、ワークスペース URL にログオンしたユーザーに対して公開するアプリを追加します（後ほどこのマスターイメージを使用するカタログを作成してから、これらのアプリのうちのどれを指定したユーザーに公開するかを厳密に指定します）。

1. 作成したマスターイメージ VM の実行中にこの VM に接続します。
2. アプリケーションをインストールします。

マスターイメージに **VDA** をインストールする

1. マスターイメージ VM に接続します（まだ接続していない場合）。
2. ナビゲーションバーの ［ダウンロード］リンクから、VDA for Server OS をダウンロードします。または、Web ブラウザーで、Citrix Virtual Apps and Desktops サービスダウンロードページに移動します。VDA for Server OS を VM にダウンロードします（VDA のバージョン情報については上記のガイダンスを参照してください）。
3. ダウンロードしたファイルをダブルクリックして、VDA インストーラーを起動します。インストールウィザードが起動します。
4. ［環境］ページで、［マスター **MCS** イメージを作成する］を選択して ［次へ］をクリックします。
5. ［コアコンポーネント］ページで ［次へ］をクリックします。
6. ［**Delivery Controller**］ページで、［**Machine Creation Services** で自動的に指定する］を選択して ［次へ］をクリックします。
7. ［追加コンポーネント］、［機能］、［ファイアウォール］の各ページの設定については、シトリックスから別途指示がない限りデフォルトのままにします。各ページで ［次へ］をクリックします。
8. ［概要］ページで ［インストール］をクリックします。前提条件のインストールが始まります。再起動を求められたら、同意します。
9. VDA のインストールは自動的に再開されます。前提条件のインストールが完了すると、コンポーネントと機能がインストールされます。［**Call Home**］ページの設定は、シトリックスから別途指示がない限りデフォルトのままにして、［次へ］をクリックします。
10. ［完了］をクリックします。マシンが自動的に再起動します。
11. 正常に構成されたことを確認するため、インストールしたアプリケーションを 1 つ以上起動します。
12. 仮想マシンをシャットダウンします。Sysprep は使用しないでください。

マスターイメージをアップロードする

この手順では、マスターイメージを Azure Resource Manager から Virtual Apps Essentials にアップロードします。

1. まだCitrix Cloudにサインインしていない場合は、サインインします。左上のメニューで、［マイサービス］**>** ［**Virtual Apps and Desktops**］を選択します。
2. ［管理］タブで ［マスターイメージ］をクリックします。
3. ［マスターイメージの追加］をクリックします。
4. ［イメージの追加］ページで、サブスクリプション、リソースグループ、ストレージアカウント、VHD、およびリージョンを選択してイメージの場所を指定します。
5. マスターイメージの名前を入力します。
6. ［保存］をクリックします。

マスターイメージの検証が行われます。検証後、アップロードしたイメージが ［マスターイメージ］**>** ［マイイメージ］に表示されます。

ヒント：マスターイメージをアップロードしてからカタログを作成するのではなく、カタログの作成時に Azure

Resource Manager からマスターイメージをインポートすることもできます。

Virtual Apps Essentials でマスターイメージを準備する

この方法では、既存のマスターイメージをテンプレートとして（オプションで既存のカタログの接続詳細も）使用して、新しいマスターイメージを作成します。新しいマスターイメージは、作成後カスタマイズできます。この手順はすべて、Virtual Apps Essentials インターフェイス内のみで行います。

1. まだCitrix Cloudにサインインしていない場合は、サインインします。左上のメニューで、［マイサービス］**>** ［**Virtual Apps and Desktops**］を選択します。
2. ［管理］をクリックし、［マスターイメージ］タブを選択します。
3. ［イメージの作成］をクリックします。
4. ［イメージの作成］ページの ［イメージの選択］パネルで、マスターイメージを選択します。新しいイメージの名前を指定します。［次へ］をクリックします。
5. ［ネットワーク接続設定の指定］パネルで、既存のカタログの設定を流用するか、設定を指定するかを選択します。設定項目は、サブスクリプション、仮想ネットワーク、リージョン、サブネット、ドメイン、および VM インスタンスの種類です（カタログがない場合は、設定を入力する必要があります）。

   ［カタログから設定をコピー］を選択した場合は、コピーするカタログを選択します。ネットワーク接続の設定が表示されるので、新しいマスターイメージで使用する設定かどうかを目視で確認します。ドメインに参加する場合は、サービスアカウントのユーザー名とパスワードを入力します。［保存］をクリックします。

   ［新しい設定を入力］を選択した場合は、該当する設定フィールドの値を選択します。ドメインに参加する場合は、サービスアカウントのユーザー名とパスワードを入力します。［保存］をクリックします。
6. ［プロビジョニングの開始］をクリックします。
7. 新しいイメージが作成され、［管理］**>** ［マスターイメージ］リストに ［入力してください］ステータスで表示されます。［**VM** に接続］をクリックします。RDP クライアントがダウンロードされます。RDP を使用して、新しく作成した VM に接続します。アプリケーションやその他のソフトウェアを追加または削除して、新しいイメージをカスタマイズします。すべてのマスターイメージと同様、Sysprep は使用しないでください。
8. 新しいイメージのカスタマイズが完了したら、［管理］**>** ［マスターイメージ］ページに戻り、そのイメージの［完了］をクリックします。新しいイメージの検証プロセスが開始されます。
9. 検証プロセスが完了すると、新しいイメージが ［マイイメージ］リストに ［準備完了］ステータスで表示されます。

後でカタログを作成するときに、［マスターイメージの選択］ページで ［既存のイメージをリンクする］を選択すると、この新しいイメージが ［イメージ名］リストに表示されます。

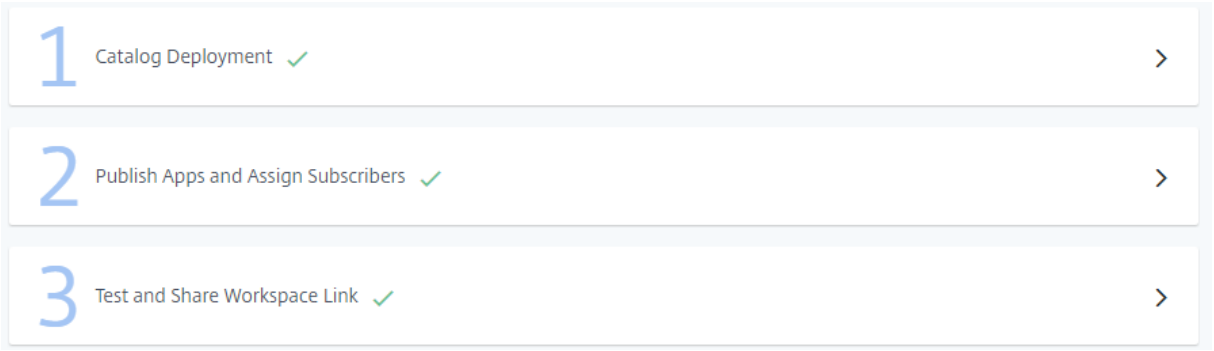
カタログの展開、アプリとデスクトップの公開、および利用者の割り当て

カタログでは、選択したユーザーと共有するように選択したアプリとデスクトップが一覧表示されます。

他のシトリックスのアプリおよびデスクトップ配信製品で例えると、本サービスのカタログは、マシンカタログとデリバリーグループを組み合わせたようなものです。ただし、本サービスでは、他のサービスのマシンカタログおよびデリバリーグループの作成ワークフローは利用できません。

カタログの展開および利用者とのアプリの共有は、複数の段階に分けて行います。

- カタログを作成する
- アプリを公開してカタログの利用者を割り当てる
- 利用者が使用するワークスペースリンクをテストして共有する

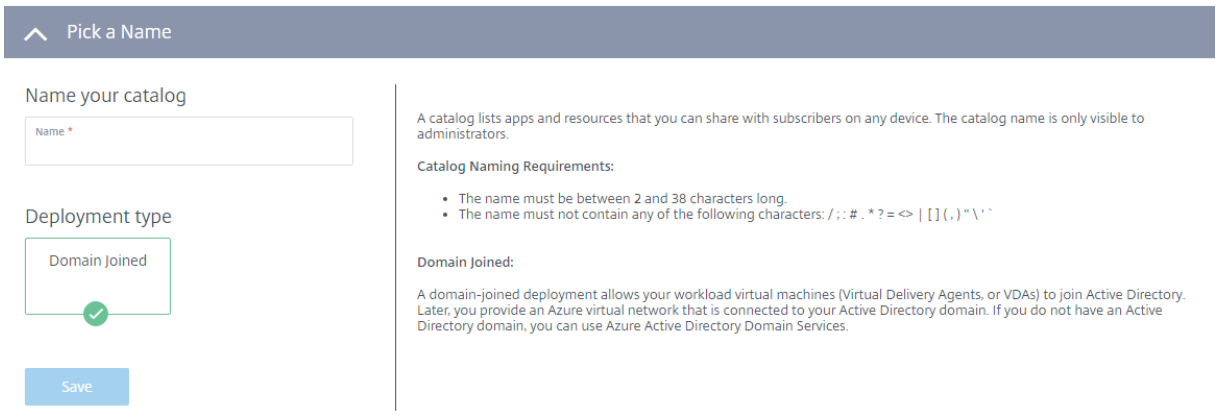


カタログを作成する

カタログを作成するときには、Azure Active Directory アカウントの資格情報およびサブスクリプション名を用意してください。

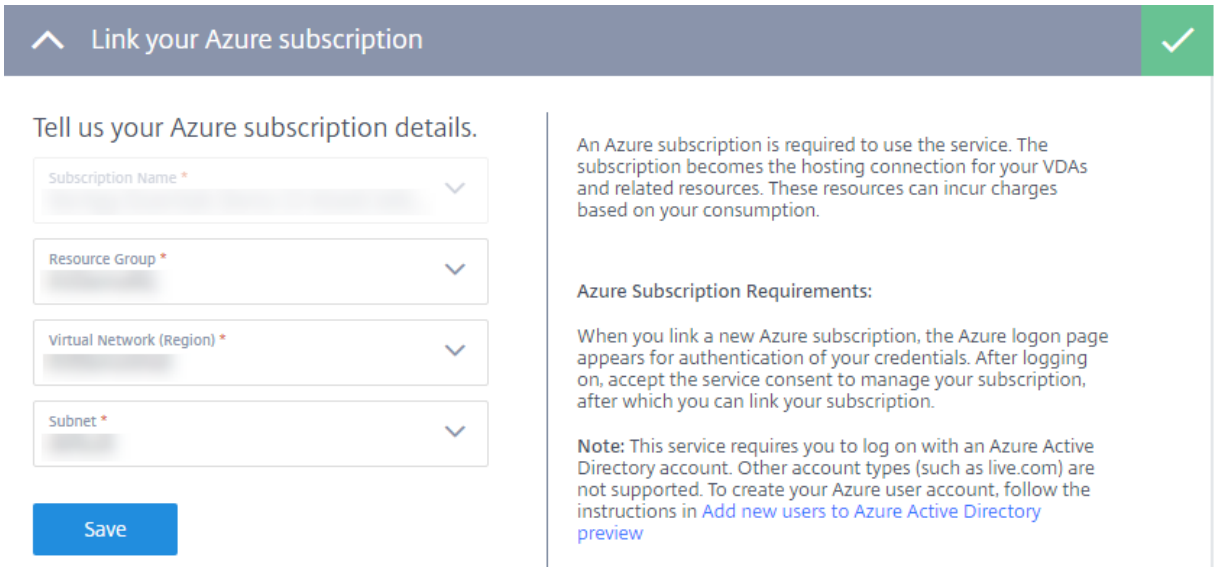
1. まだCitrix Cloudにサインインしていない場合は、サインインします。左上のメニューで、[マイサービス] > [**Virtual Apps and Desktops**] を選択します。
2. [管理] タブで、[カタログ]、[カタログを追加] の順にクリックします。
3. 以下の各パネルで情報を入力します。各パネルで入力が完了したら、[保存] をクリックします。必須情報が入力されていないか無効である場合、パネルのヘッダーに警告サインが表示されます。情報に不備がない場合はチェックマークが表示されます。

名前を選択する



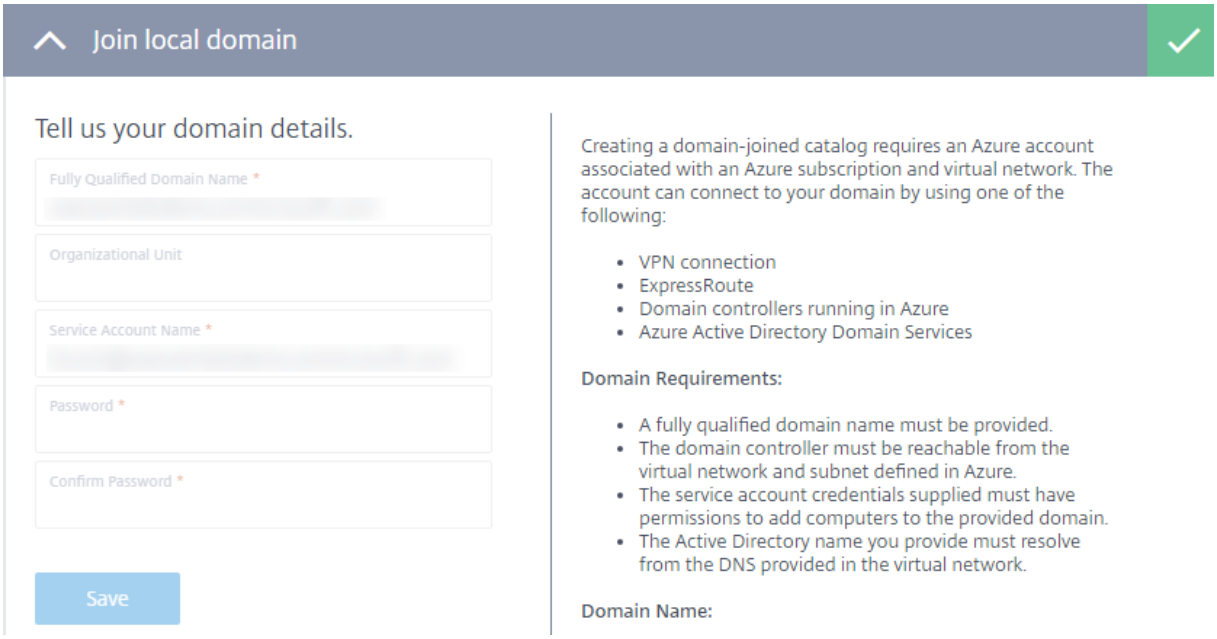
1. カタログの名前を 2～38 文字で入力します（英数字のみ、特殊文字は使用不可）。この名前は管理者にのみ表示されます。
2. ［ドメイン参加済み］が選択されていない場合は、選択します。展開をドメインに参加させると、VDA を Active Directory に追加できるようになります。後で、ドメインに接続する Azure 仮想ネットワークを指定します。ドメインがない場合は、Azure Active Directory Domain Services を使用できます。
3. ［保存］をクリックします。

Azure サブスクリプションを関連付ける



1. リンクする Azure サブスクリプションを選択します。新しい Azure サブスクリプションをリンクすると、Azure 資格情報の認証を行う Azure のサインインページが表示されます。サインイン後、本サービスがサブスクリプションを管理することに同意します。これで、サブスクリプションをリンクすることができます。Virtual Apps Essentials を利用するには、Azure Active Directory アカウントでログオンする必要があります。他のアカウントタイプ（live.com など）はサポートされません。
2. リソースグループ、仮想ネットワーク（VNET）、サブネットを選択します。選択した VNET により、リソースの展開先となる Azure リージョンが決まります。サブネットは、使用するドメインコントローラーに到達できる必要があります。
3. ［保存］をクリックします。

ローカルドメインに参加する



1. ドメイン情報を入力します:
   - 完全修飾ドメイン名: ドメイン名を入力します。この名前は、仮想ネットワークで提供される DNS で解決できるものである必要があります。
   - 組織単位:（オプション）指定した組織単位が Active Directory に含まれるようになります。このフィールドを空白のままにすると、マシンはデフォルトの Computers コンテナに配置されます。
   - [サービスアカウント名]、[パスワード]、[パスワードの確認]: ドメインへのコンピューターの追加権限を持つアカウントのユーザープリンシパル名（UPN）を入力します。次に、そのアカウントのパスワードを入力し、確認用にもう一度入力します。
2. [保存] をクリックします。

指定した仮想ネットワーク経由で接続できるかどうか、Azure サブスクリプションに VM を作成してテストします。この VM は、カタログの展開に使用するのと同じリソースグループ、仮想ネットワーク、およびサブネット内に配置する必要があります。VM がインターネットに接続できることを確認します。また、VM をドメインに参加させることで、このドメインにアクセスできることも確認します。テストは、このカタログの展開に使用したものと同じ資格情報を使用して行うことができます。

リソースの場所に接続する

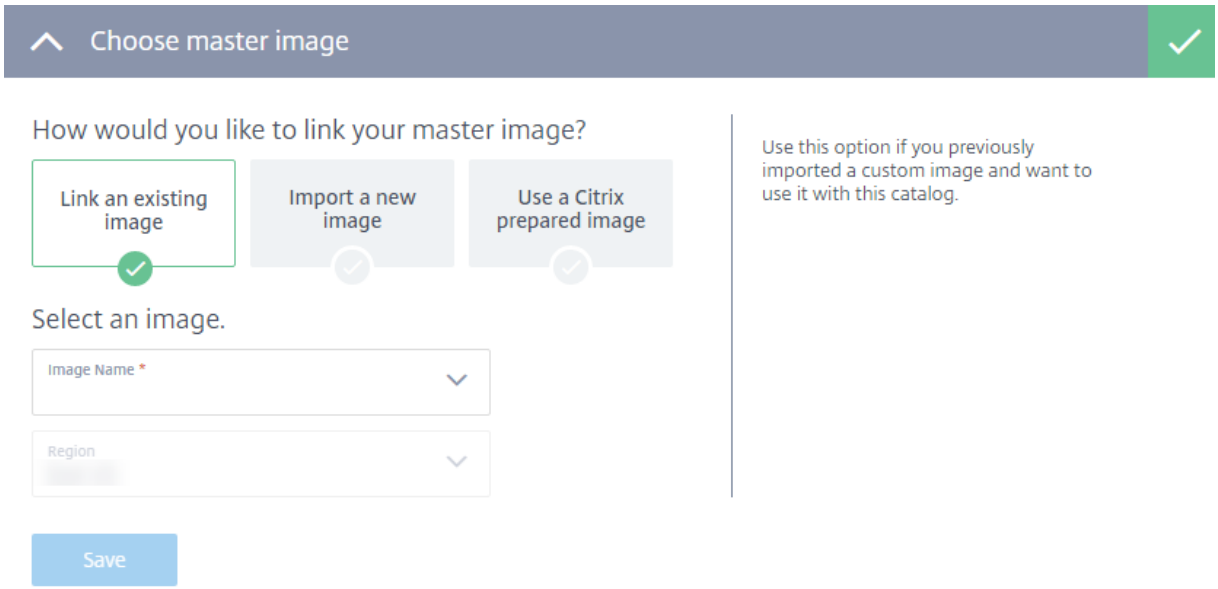
各リソースの場所には、Citrix Cloud と通信する Cloud Connector を 2 つ以上用意する必要があります。Cloud Connector の展開は、カタログの展開時に本サービスにより自動で行われます。Azure Resource Manager に Windows Server VM が 2 つ作成され、各サーバーに Cloud Connector が自動でインストールされます。
選択したリソースの場所が利用可能な場合、自動的に接続が行われます。[保存] をクリックします。
リソースの場所を作成する場合は、その名前を入力します。

- 特定の Azure リソースグループ内に Cloud Connector を作成するには、[**Azure** リソースグループ] の横

にある ［編集］をクリックして、リソースの場所を変更します。変更を行わない場合、Azure サブスクリプションをリンクしたときに指定したリソースグループが使用されます。

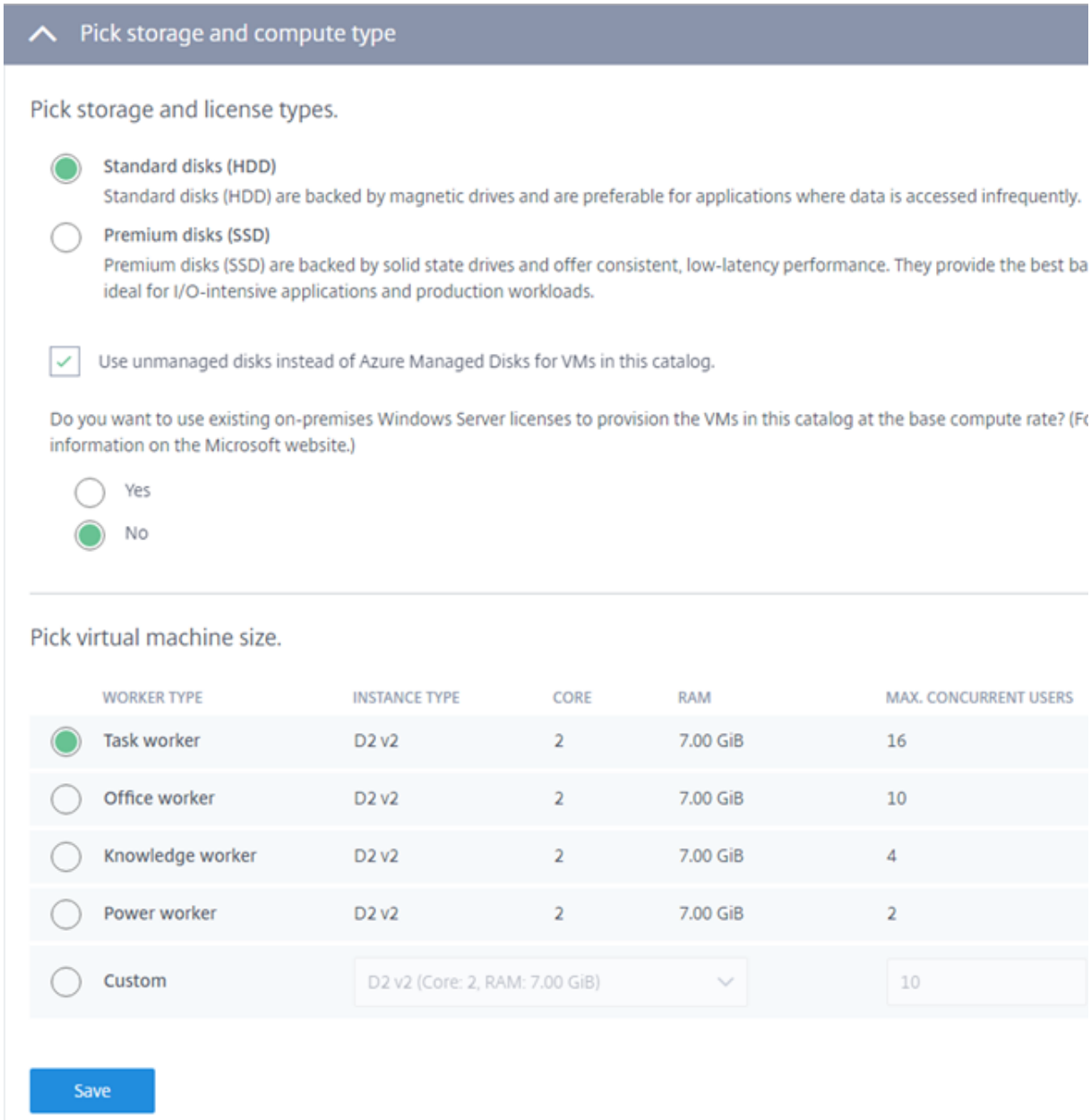
- Cloud Connector を別の組織単位に配置するには、［組織単位］の横にある ［編集］をクリックして組織単位を変更します。変更を行わない場合、Azure サブスクリプションをリンクしたときに指定したリソースグループが使用されます。

マスターイメージを選択する



1. 次のいずれかを選択します：
    - 既存のイメージをリンクする：カスタムイメージをインポート済みでありこのカタログでそのイメージを使用する場合は、このオプションを選択します。イメージを選択し、オプションでリージョンを選択します。
    - 新しいイメージをインポートする：まだインポートしていないカスタムイメージをこのカタログで使用する場合は、このオプションを選択します。サブスクリプション、リソースグループ、ストレージアカウント、VHD を選択します。マスターイメージのわかりやすい名前を入力します。
    - **Citrix** 提供イメージを使用する：独自のカスタムイメージを使用せずにサービスのテストを行う場合は、このオプションを選択します。提供イメージはデモ環境にのみ適しており、実稼働環境には推奨されません。提供されたイメージを選択します。
2. ［保存］をクリックします。

ストレージとコンピューティングの種類を選択する



1. 次の項目を構成します:

   - 標準ディスクまたはプレミアムディスク：標準ディスク（HDD）は磁気ドライブでサポートされています。頻繁にデータにアクセスしないアプリケーションに適しています。プレミアムディスク（SDD）はソリッドステートドライブでサポートされています。I/O 集約型アプリケーションに最適です。
   - **Azure Managed Disks** または非管理ディスクの使用： Azure Managed Disks について詳しくは、https://docs.microsoft.com/en-us/azure/virtual-machines/windows/managed-disks-overviewを参照してください。
   - **Azure Hybrid Use Benefit**：既存のオンプレミス Windows Server ライセンスを使用するかどうかを選択します。この機能を有効にして既存のオンプレミス Windows Server イメージを使用すると、

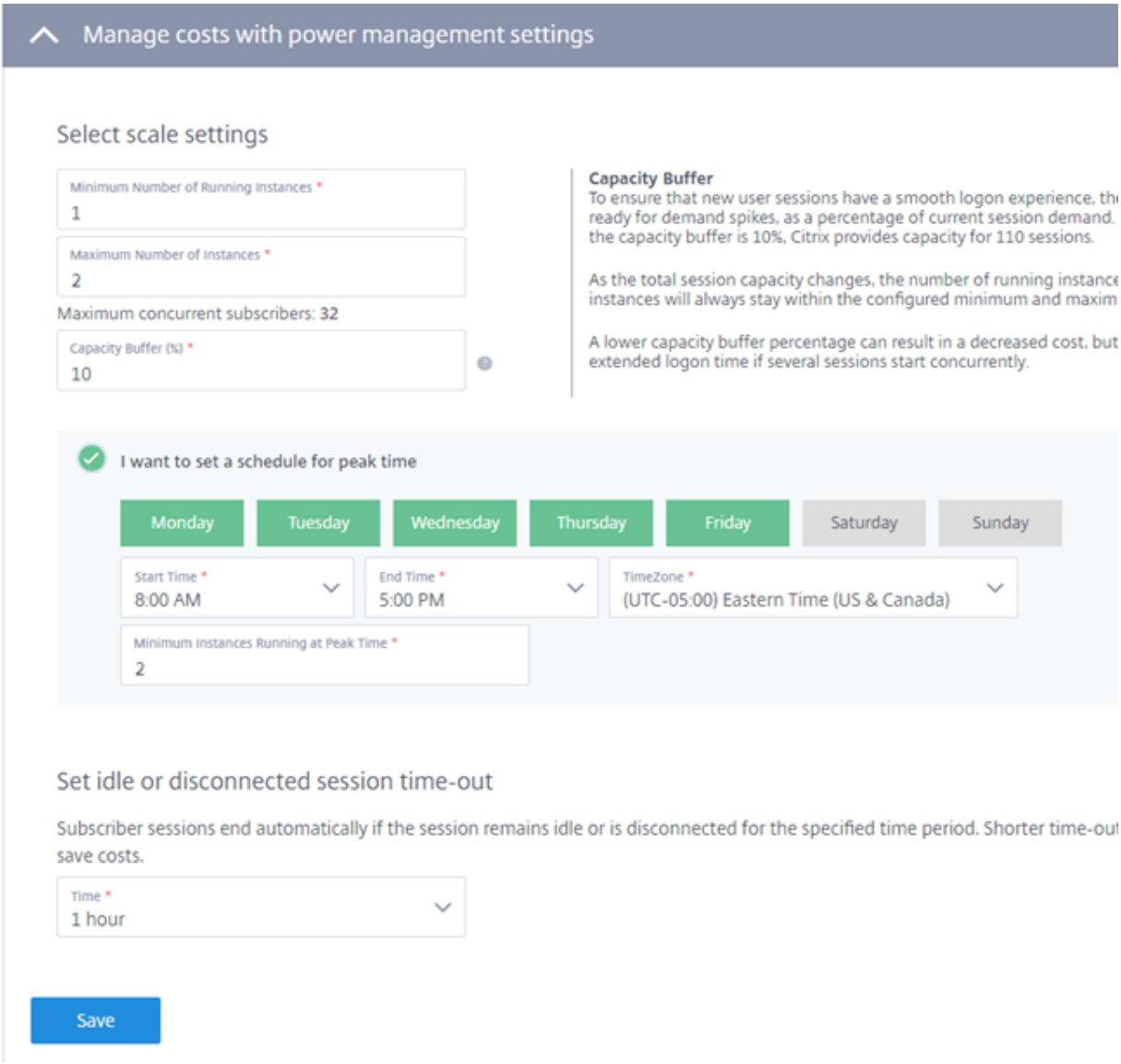
Azure Hybrid Use Benefits（HUB）が利用されます。詳しくは、「https://azure.microsoft.com/pricing/hybrid-use-benefit/」を参照してください。

HUB を使用すると、Azure ギャラリーから Windows Server ライセンスを追加する際に料金がかからなくなるため、Azure で VM を実行するコストが基本のコンピューティングレートまで抑えられます。HUB を使用するためのオンプレミスの Windows Servers イメージを Azure に用意する必要があります。Azure ギャラリーのイメージはサポートされません。オンプレミスの Windows Client ライセンスは、現在サポートされていません。Microsoft 社 Web サイトの「Windows Server 向け Azure Hybrid Benefit」を参照してください。

- 仮想マシンのサイズを選択：ワーカーロールを選択します（タスク、オフィス、ナレッジ、パワーなど）。ワーカーロールにより、使用するリソースが決まります。ワーカーロールを指定すると、インスタンスごとの負荷が適切に決定されます。いずれかのオプションを選択するか、独自のカスタムオプションを作成できます。

2. ［保存］をクリックします。

コストと電源管理設定を管理する



1. 次の情報を入力します：
   - スケール設定：
     - 最小実行インスタンス数：指定した数の VM が常に電源オンの状態になります。
     - 最大実行インスタンス数：本サービスで使用される VM 数の上限です。
     - 最大同時ユーザー数：同時ユーザーの数がこの制限以下に抑えられます。
     - 処理能力バッファ：現在のセッション需要の割合として、需要の急増に備えて追加するセッションを指定します。たとえば、アクティブなセッションが 100 個あり、処理能力バッファが 10%の場合、セッション 110 個分の処理能力が提供されます。

       セッションの総処理能力の変化に応じて、このカタログの実行インスタンスの数が増減します。実行インスタンスの数は、指定した最小値から最大値の間に常にとどまります。処理能力バッファの

数値を小さくすると、コストを抑えられます。ただし、複数のセッションが同時に開始された場合に、一部のセッションでログオン時間が長くなる可能性があります。

- ピーク時のスケジュール：実行する仮想マシンの数をピーク時とピーク時以外とで変更するには、このオプションを選択します。ピークの曜日、開始時刻、終了時刻、タイムゾーンを選択します。ピーク時の最小実行インスタンス数を指定します。
- アイドル状態または切断状態のセッションのタイムアウト：セッションを終了するまでの時間を指定します。ユーザーセッションがアイドル状態または切断状態になってから指定した時間が経過すると、セッションは自動で終了されます。タイムアウトの値を小さくすると、使用されていない VDA の電源をオフにしてコストを削減できます。

2. ［保存］をクリックします。

カタログを展開する

構成パネルの設定を完了したら、［展開の開始］をクリックしてカタログ作成を開始します。カタログの作成には 1〜2 時間（VM を多数指定した場合はそれ以上）かかります。

カタログが作成されると次の処理が行われます：

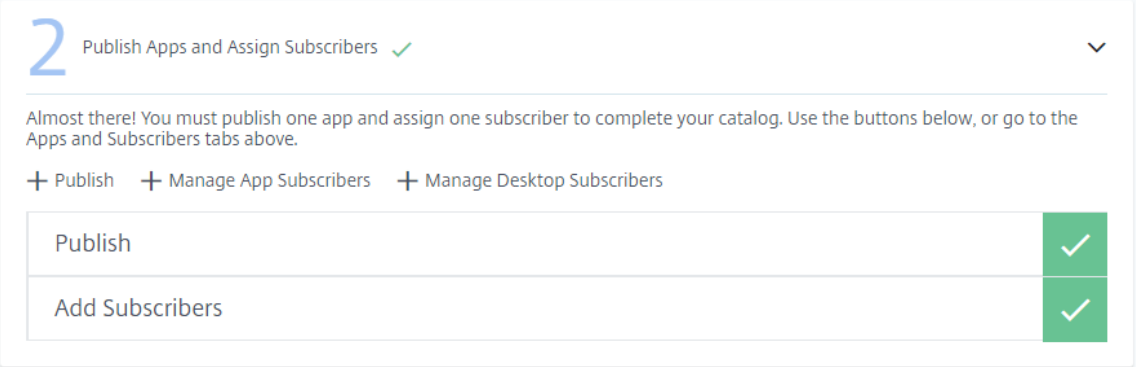
- Azure にワークロードマシンのリソースグループ（およびそのリソースグループのストレージアカウント）が自動で作成されます。
- VM には Xenappxx-xx-yyy という名前がつけられます。xx は環境要因、yy には番号が入ります。

アプリを公開してカタログの利用者を割り当てる

展開したカタログを完成させるには、アプリまたはデスクトップを 1 つ公開し、少なくとも 1 人の利用者を割り当てる必要があります。

公開できるアプリケーション（またはデスクトップ）は、カタログの作成に使用したイメージに含まれています。［スタート］メニューからアプリケーションを選択するか、マシン上のディレクトリパスを指定します。

1. まだCitrix Cloudにサインインしていない場合は、サインインします。左上のメニューで、［マイサービス］> ［**Virtual Apps and Desktops**］を選択します。
2. ［管理］タブで ［カタログ］をクリックします。
3. 作成されたカタログの省略記号メニュー（...）で、［カタログの管理］を選択します。
4. ［アプリを公開して利用者を割り当てる］を選択します。次のページが表示されます。

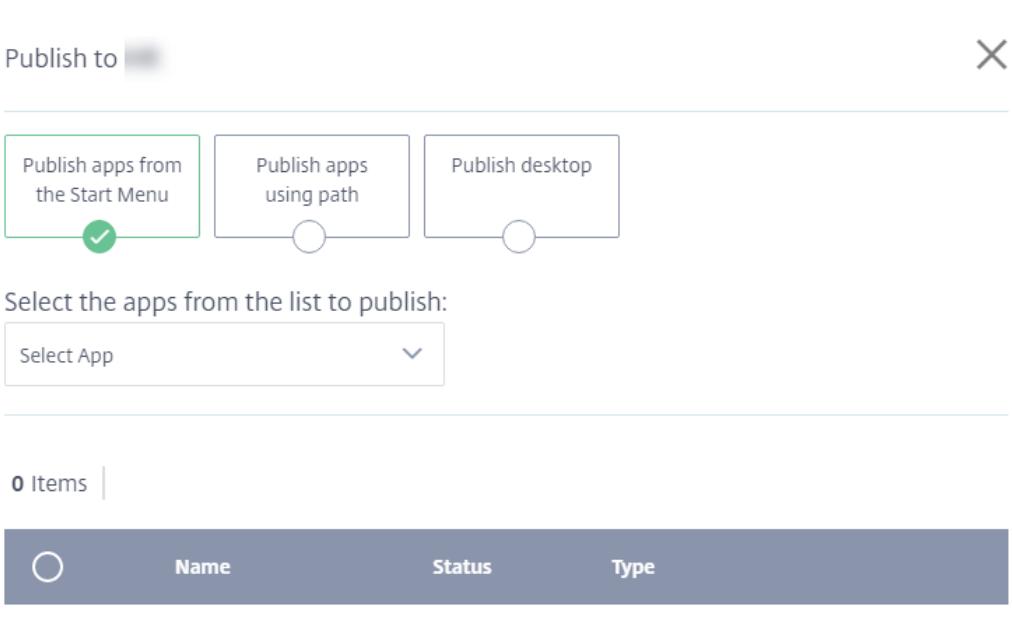


5. ［アプリを公開して利用者を割り当てる］ダイアログボックスで、［公開］をクリックします。［カタログ名に公開］ページに 3 つのオプションが表示されます。少なくとも 1 つを選択してください。任意で、このカタログでアプリとデスクトップの両方を公開するなどのように、オプションを複数選択することも可能です。

6. ［スタート］メニューにあるアプリを公開するには、次の操作を実行します：

   a) ［スタート］メニューから公開する］を選択します。

   b) 一覧からアプリケーションを選択します。



7. 場所などの情報を指定してアプリを公開するには、次の操作を実行します：

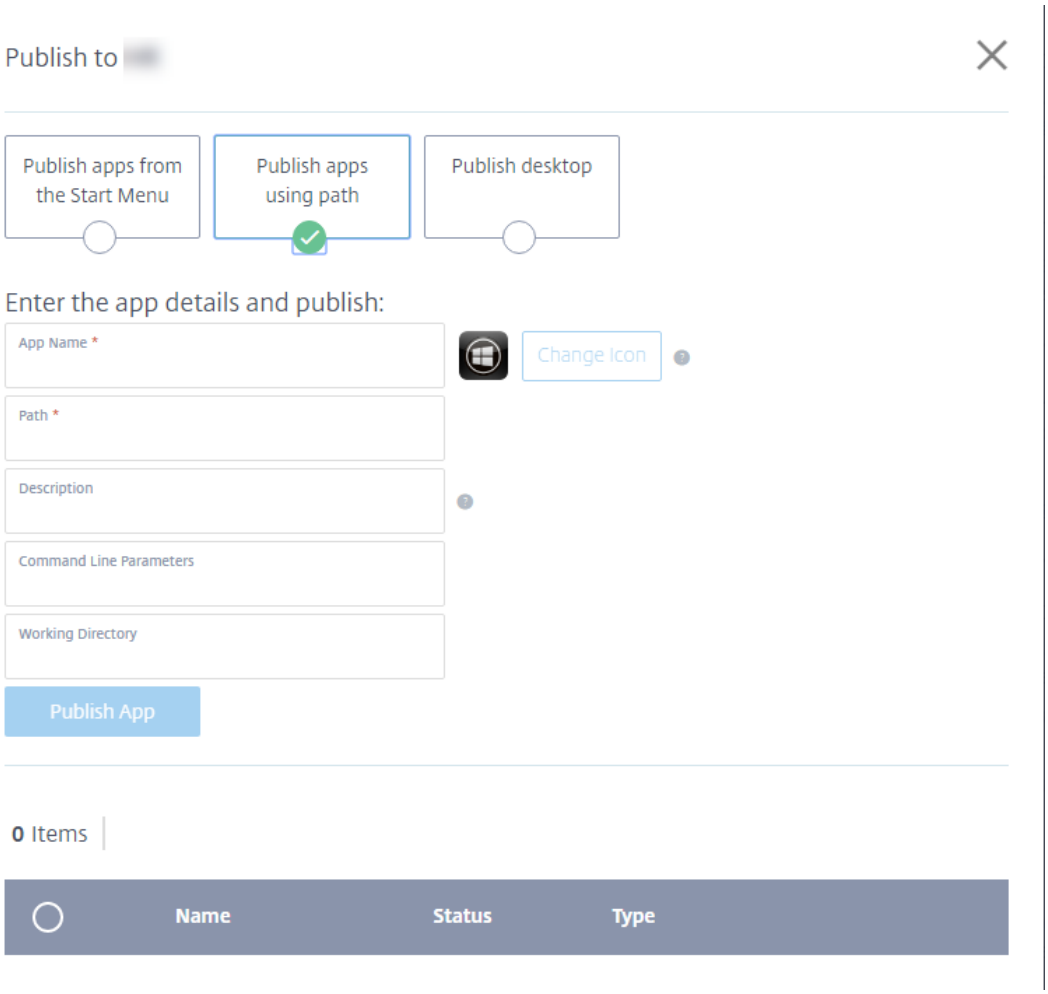
   a) ［パスを使用して公開する］を選択します。

   b) 各アプリケーションの名前とパス（例：c:\Windows\system1\app.exe）を入力します。

   c) 必要に応じて、ユーザーのワークスペース、コマンドラインパラメーター、および作業ディレクトリに表示する説明を入力します。

   d) 公開するアプリを表すアイコンを変更するには、［アイコンの変更］をクリックしてアイコンの場所を指定します。選択したアイコンを抽出できない場合は、メッセージが表示されます。この場合は、再度アイコンを選択するか、既存のアイコンのままにします。

e)［アプリを公開］をクリックします。



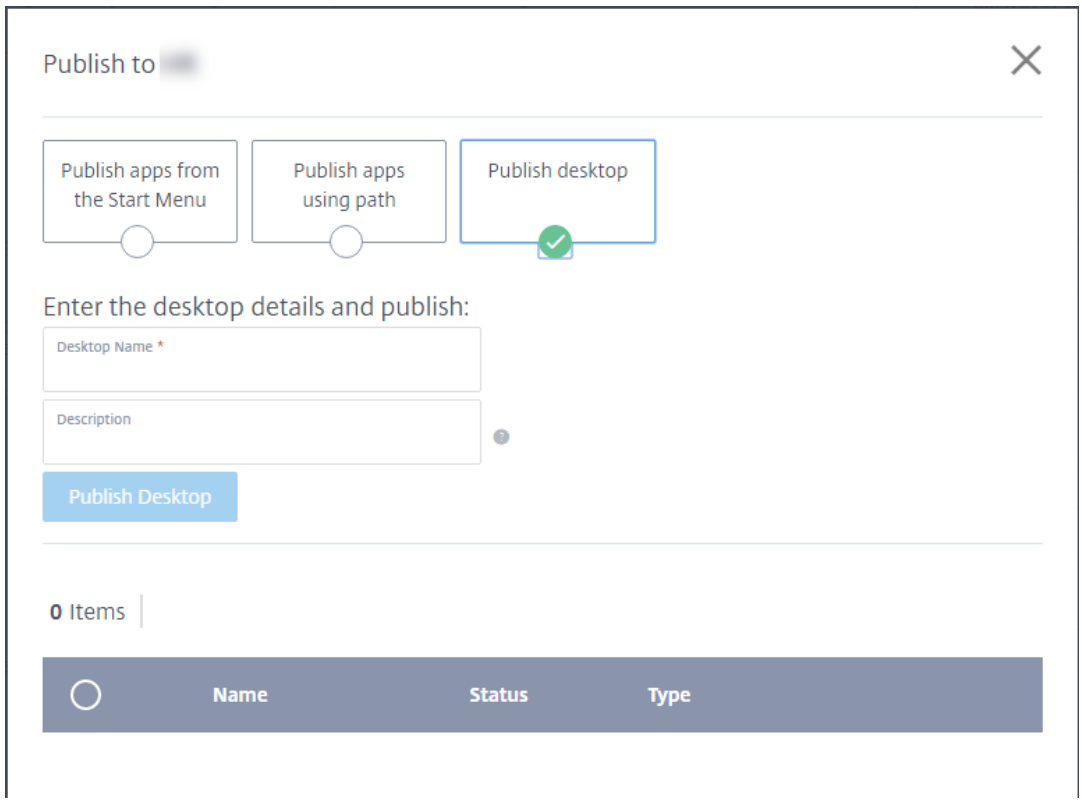
8. デスクトップを公開するには、次の操作を実行します：

a)［デスクトップを公開する］を選択します。

b) デスクトップの名前を入力します。

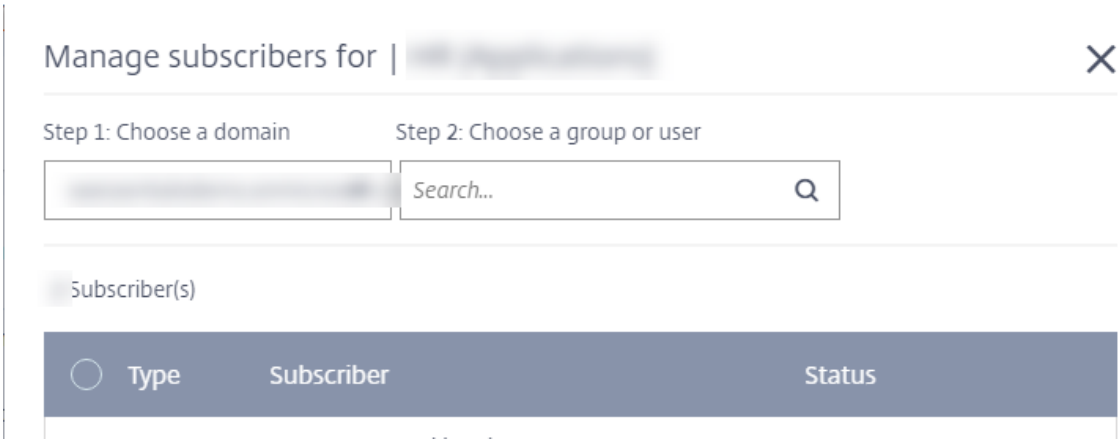
c) 必要に応じて、ユーザーのワークスペースに表示する説明を入力します。

d)［デスクトップを公開］をクリックします。



追加したアプリまたはデスクトップは、セレクタの下のリストに表示されます。追加したアプリまたはデスクトップを削除するには、削除するエントリの左にあるボタンを選択（またはエントリの横にあるゴミ箱アイコンをクリック）し、［削除］をクリックします。後でアプリまたはデスクトップを非公開にする場合は、非公開にするエントリの左にあるボタンを選択し、［非公開］をクリックします。

9. ［アプリを公開して利用者を割り当てる］ダイアログボックスで、［アプリの利用者の管理］または ［デスクトップの利用者の管理］をクリックします。



10. ドメインを選択して、ユーザーまたはユーザーグループを検索します。
11. ユーザー割り当てはアプリとデスクトップで別々に行います。アプリとデスクトップの両方にユーザーアクセスを割り当てるには、［アプリの利用者の管理］と ［デスクトップの利用者の管理］のそれぞれでユーザーを

割り当てます。

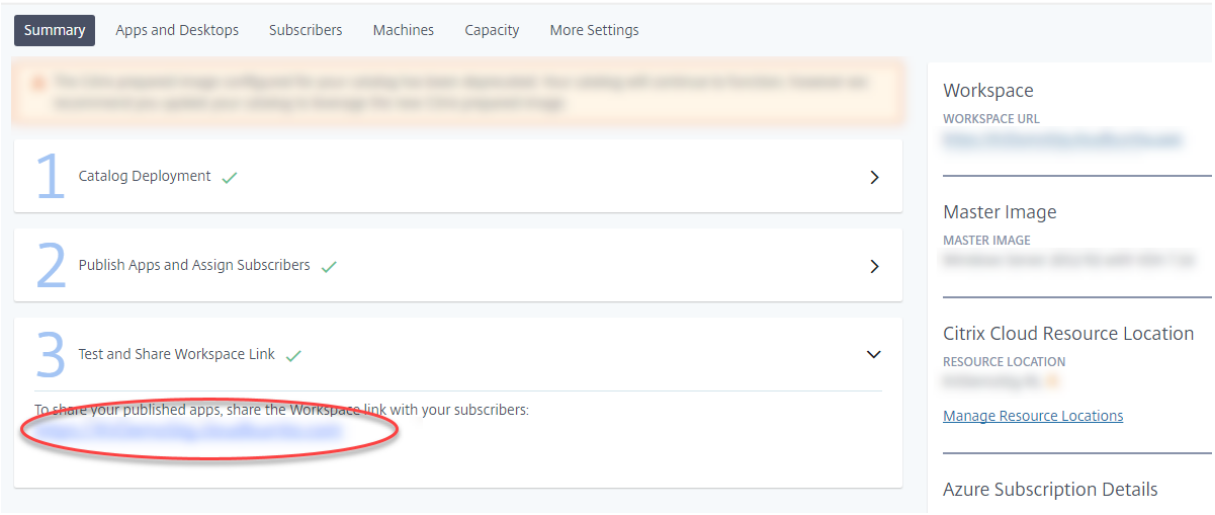
追加したユーザーまたはグループは、セレクタの下のリストに表示されます。選択したユーザーまたはグループを削除するには、そのエントリの横にあるゴミ箱アイコンをクリックして ［削除］をクリックします。後でユーザーを削除する場合は、削除するエントリの左側にあるボタンを選択し、［選択項目を削除］をクリックします。

ワークスペースリンクをテストして共有する

カタログの展開、アプリの公開、および利用者の割り当てが完了すると、利用者に公開したアプリとデスクトップへ利用者がアクセスできるリンクが表示されます。

1. まだCitrix Cloudにサインインしていない場合は、サインインします。左上のメニューで、［マイサービス］> ［**Virtual Apps and Desktops**］を選択します。
2. ［管理］タブで ［カタログ］をクリックします。
3. カタログの省略記号メニュー（...）で、［カタログの管理］を選択します。
4. ［ワークスペースリンクをテストして共有する］を選択します。

ワークスペースリンクが、次の図の円で囲んだ場所に表示されます。このリンクを利用者に提供します。ページの右側には、ワークスペースの URL と、カタログのマスターイメージ、リソースの場所、Azure サブスクリプション、およびドメインに関する情報が表示されます。



詳しくは、「ワークスペース環境」を参照してください。

マスターイメージとカタログを更新する

アプリケーションを更新または追加するには、カタログのマスターイメージの作成に使用した仮想マシンを更新します。

マスターイメージの更新

1. マスターイメージ VM の電源をオンにします。VM の電源をオンにしても、Azure Resource Manager にインストール済みのマスターイメージに影響はありません。
2. VM に更新またはアプリケーションをインストールします。
3. 仮想マシンをシャットダウンします。
4. Virtual Apps Essentials コンソールで、VM の VHD イメージへのパスが含まれる新しいイメージを追加します。

新しいイメージでカタログを更新

1. まだCitrix Cloudにサインインしていない場合は、サインインします。左上のメニューで、［マイサービス］> ［**Virtual Apps and Desktops**］を選択します。
2. ［管理］タブで ［カタログ］をクリックします。
3. カタログの省略記号メニュー（...）をクリックし、［カタログイメージの更新］をクリックします。
4. ［既存のイメージをリンクする］または ［新しいイメージをインポートする］を選択します。選択内容に応じて情報を入力します。
5. ［自動ログオフまでの時間］で、セッションが終了するまでの時間を指定します。
6. ［更新］をクリックします。

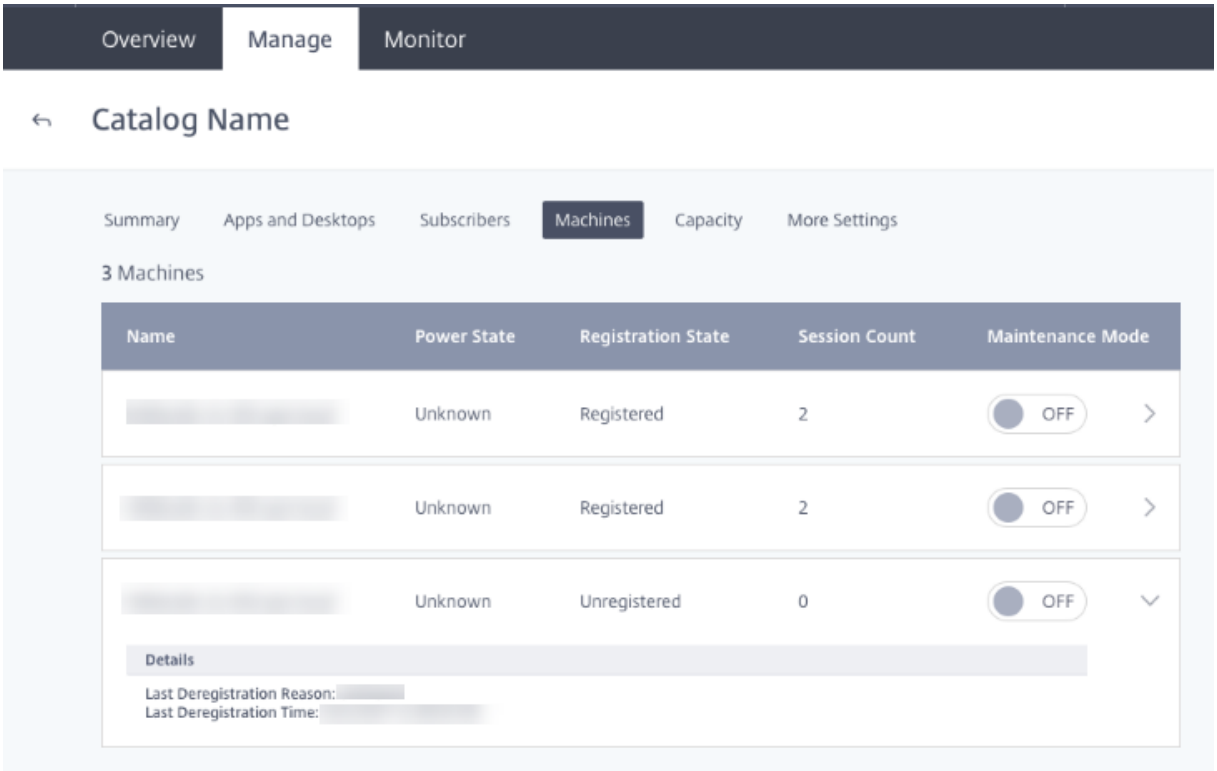
カタログの更新が開始された場合でも、ユーザーは初期処理が完了するまでは作業を継続できます。初期処理が完了すると、ユーザーに作業を保存してアプリケーションを終了するように求める警告メッセージが表示されます。VDA 上のすべてのアクティブなセッションが終了されると、その VDA の更新が完了します。ユーザーが指定時間内にログオフしない場合、セッションは自動的に終了されます。

カタログ内の **VDA** の数を更新

1. まだCitrix Cloudにサインインしていない場合は、サインインします。左上のメニューで、［マイサービス］> ［**Virtual Apps and Desktops**］を選択します。
2. ［管理］タブをクリックします。
3. ［カタログ］タブで、カタログを選択します。
4. ［処理能力］タブで、［スケール設定を選択する］の ［編集］を選択します。
5. ［最大実行インスタンス数］の値を変更して、カタログに必要な VDA 数に変更します。
6. ［保存］をクリックします。

マシンの状態を監視する

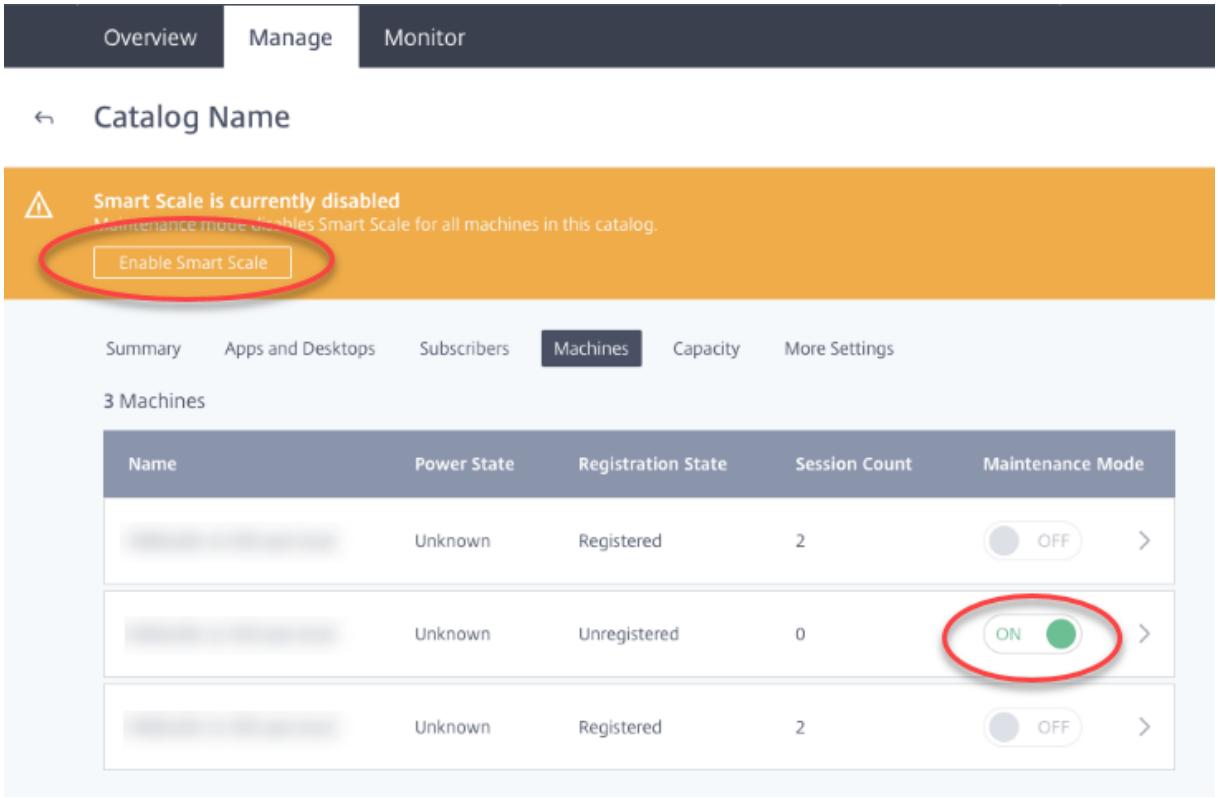
カタログを選択すると、カタログの概要ページの［マシン］タブに、そのカタログ内のすべてのマシンが一覧表示されます。画面には、各マシンの電源状態、登録状態、および現在のセッション数も表示されます。



マシンのメンテナンスモードのオン/オフを切り替えることができます。メンテナンスモードをオンにしている間は、マシンに接続できなくなります。ユーザーは既存のセッションに接続できますが、新しいセッションを開始することはできなくなります。パッチを適用する前には、マシンをメンテナンスモードにすることをお勧めします。

1 台以上のマシンでメンテナンスモードをオンにすると、そのカタログに含まれるマシンすべてで Smart Scale が一時的に無効になります。Smart Scale は、次のいずれかの操作を行うと再び有効になります:

- 画面上部の警告に表示される ［**Smart Scale** を有効にする］をクリックする。この操作を行うと、カタログに含まれるメンテナンスモードがオンになっているすべてのマシンで、メンテナンスモードが自動的にオフになります。
- 現在メンテナンスモードがオンになっている各マシンのメンテナンスモードを個別にオフにする。



サービスを監視する

1. まだCitrix Cloudにサインインしていない場合は、サインインします。左上のメニューで、［マイサービス］> ［**Virtual Apps and Desktops**］を選択します。
2. ［モニター］タブをクリックします。

セッション情報

Citrix Virtual Apps Essentials の全体的なパフォーマンスを監視するには:

1. 監視するカタログを選択します。セッションやログオン期間などの情報を確認できます。
2. セッションを選択して、次の操作を行います:
   - セッションを切断する
   - セッションからログオフする
   - メッセージを送信する
3. 各セッションをクリックして、プロセスや実行中のアプリケーションなど、セッションの詳細を確認します。

使用状況の情報

使用状況の情報では、指定したカタログではなくすべてのカタログの集計データが示しされます。

- ［使用状況の概要］には、アプリケーションの総起動回数と、過去 6 週間にアプリケーションを起動した一意のユーザーの数が表示されます。
- ［使用頻度が高いアプリケーション］には、今月および前月に最も多く使用されたアプリの一覧が表示されます。エントリの上にカーソルを置くと、アプリケーションが起動された回数が表示されます。
- ［使用頻度の高いユーザー］には、今月および前月における使用頻度の高い上位 10 名のユーザーと、各ユーザーのアプリケーションの起動回数が表示されます。

週のデータの期間は、月曜日（UTC 00:00）からクエリ時刻までです。月のデータの期間は、その月の初日（UTC 00:00）からクエリ時刻までです。

Profile Management

Profile Management を使用すると、ユーザーデバイスの場所に関係なく、ユーザーの仮想アプリケーションに個人設定が適用されるようになります。

Profile Management の構成は任意です。

Profile Management は、プロファイル最適化サービスで有効にできます。このサービスを利用することで、Windows でプロファイル設定を確実に管理できます。プロファイルを管理するとユーザーに単一のプロファイルのみが適用されるようになるため、一貫したユーザーエクスペリエンスを確保できます。ユーザープロファイルが自動的に集約および最適化されるため、管理と保存の手間が最小化されます。プロファイル最適化サービスにより、必要な管理、サポート、インフラストラクチャを最低限に抑えられます。また、ログオンおよびログオフ時のユーザーエクスペリエンスも向上します。

プロファイル最適化サービスを使用するには、すべての個人設定を保存するファイル共有が必要になります。ファイル共有は UNC パスとして指定する必要があります。このパスには、システム環境変数、Active Directory のユーザー属性、Profile Management の変数を含めることができます。UNC テキスト文字列の書式について詳しくは、「ユーザーストアへのパスを指定するには」を参照してください。

Profile Management の構成は Citrix Cloud で行います。

Profile Management を構成するには

1. まだCitrix Cloudにサインインしていない場合は、サインインします。左上のメニューで、［マイサービス］> ［**Virtual Apps and Desktops**］を選択します。
2. ［管理］タブで ［カタログ］をクリックします。
3. カタログの名前をクリックします。
4. ［詳細設定］をクリックします。
5. ［**Azure** サブスクリプションで **Profile Management** をセットアップする］で、ファイル共有へのパスを入力します。例：\fileserver\share#sAMAccountName#
6. ［保存］をクリックします。

Profile Management を有効にする場合は、ユーザーのプロファイルをさらに最適化するため、フォルダーリダイレクトを構成してユーザープロファイルのサイズの影響を最小限に抑えることも検討してください。フォルダーリダ

イレクトを適用することで、Profile Management ソリューションを強化できます。詳しくは、Microsoft Folder Redirection。

Microsoft RDS ライセンスサーバーを構成する

Citrix Virtual Apps Essentials は Windows Server リモートセッション機能にアクセスしますが、この機能には通常、リモートデスクトップサービスクライアントアクセスライセンス（RDS CAL：Remote Desktop Services Client Access License）が必要になります。VDA は、RDS CAL の要求のために RDS ライセンスサーバーに接続できる必要があります。ライセンスサーバーをインストールしてアクティブ化してください。詳しくは、「Activate the Remote Desktop Services License Server」を参照してください。概念実証環境では、Microsoft から提供される猶予期間を利用できます。

この手法により、Virtual Apps Essentials でライセンスサーバーの設定を適用できます。マスターイメージの RDS コンソールでは、ライセンスサーバーおよび接続ユーザー数モードを構成できます。また、Microsoft のグループポリシー設定を使用して、ライセンスサーバーを構成することもできます。詳しくは、「License your RDS deployment with client access licenses (CALs)」を参照してください。

グループポリシー設定を使用して **RDS** ライセンスサーバーを構成するには

1. 使用可能な VM のいずれかに、リモートデスクトップサービスのライセンスサーバーをインストールします。この VM は常に使用可能なものである必要があります。また、Citrix サービスのワークロードが常にこのライセンスサーバーに到達できる必要があります。
2. Microsoft のグループポリシーを使用して、ライセンスサーバーのアドレスと接続ユーザー数ライセンスモードを指定します。詳しくは、「Specify the Remote Desktop Licensing Mode for an RD Session Host Server」を参照してください。
3. Microsoft リモートアクセスの CAL ライセンスを購入した場合は、ライセンスをインストールする必要はありません。Microsoft リモートアクセスのライセンスは、Virtual Apps Essentials と合わせて Azure Marketplace で購入できます。

RDS ライセンスサーバーを構成するには

1. まだCitrix Cloudにサインインしていない場合は、サインインします。左上のメニューで、［マイサービス］> ［**Virtual Apps and Desktops**］を選択します。
2. ［管理］タブで ［カタログ］をクリックします。
3. カタログを選択してから ［詳細設定］を選択します。
4. ［ライセンスサーバーの FQDN を入力］に、ライセンスサーバーの完全修飾ドメイン名を入力します。
5. ［保存］をクリックします。

ユーザーの接続

ワークスペース環境

Citrix Cloud の Virtual Apps Essentials は、各顧客に合わせたワークスペース環境を実現します。最初のカタログを作成すると、Virtual Apps Essentials によりワークスペースの URL が自動的に構成されます。この URL から、ユーザーは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 URL は、［概要］タブの［カタログ詳細］パネルに表示されます。Virtual Apps Essentials では、オンプレミスでの StoreFront 展開はサポートされません。

カタログの作成後、ワークスペース構成機能を使用して、ワークスペースの URL と外観をカスタマイズできます。また、Azure Active Directory を使用したフェデレーション認証のプレビューバージョンを有効にすることもできます。

Azure Active Directory を使用したフェデレーション認証を有効にするには、次のタスクを行います。

- Azure AD を ID プロバイダーとして設定する。詳しくは、「Azure Active Directory を Citrix Cloud に接続する」を参照してください。
- Citrix Workspace の認証で Azure AD を使用できるようにする。

詳しくは、「Workspace の構成」を参照してください。

Citrix Gateway サービス

ユーザーが公開アプリケーションに安全にアクセスできるよう、Virtual Apps Essentials では Citrix Gateway サービスを使用しています。このサービスをお客様が構成する必要はありません。各ユーザーの 1 か月あたりのデータ送信量は 1GB までに制限されています。Azure Marketplace で、25GB 分の追加送信量を購入できます。追加送信量の料金は月単位で計算されます。

Virtual Apps Essentials のキャンセル

Virtual Apps Essentials を使用すると、次の要素について Azure から請求が行われる可能性があります:

- Virtual Apps Essentials サブスクリプション
- Virtual Apps Essentials によって作成された Azure リソース

Virtual Apps Essentials サービスに対する Microsoft Azure の料金は月ごとに請求されます。Virtual Apps Essentials を購入した場合は、購入月に請求されます。注文をキャンセルすると、翌月以降サービスが更新されなくなります。キャンセル月の末日までは、引き続き Citrix Cloud を使用して Virtual Apps Essentials にアクセスできます。

Azure の請求書には、次の Virtual Apps Essentials の明細が複数含まれる場合があります:

- Virtual Apps Essentials サービスのサブスクリプション
- Citrix Gateway サービスの追加送信量（購入した場合）
- Microsoft リモートアクセスの料金

- Virtual Apps Essentials の使用中に作成された Azure リソース

Azure での **Virtual Apps Essentials** のキャンセル

Virtual Apps Essentials のサブスクリプションをキャンセルするには、Azure ポータルで注文リソースを削除します。

1. Azure ポータルにサインインします。
2. ［すべてのリソース］をクリックします。
3. ［種類］列で、［Citrix Virtual Apps Essentials］をダブルクリックして開きます。
4. ごみ箱アイコンをクリックします。削除処理が開始されます。

Virtual Apps Essentials により作成された **Azure** リソースを削除する

Citrix Cloud で、アカウントに関連付けられているカタログとイメージを削除します。また、サブスクリプションリンクを削除するとともに、Citrix Cloud から Cloud Connector VM を確実に削除します。

まだCitrix Cloudにサインインしていない場合は、サインインします。左上のメニューで、［マイサービス］**>** ［**Virtual Apps and Desktops**］を選択します。

カタログを削除するには

1. ［管理］タブで ［カタログ］をクリックします。
2. 削除するカタログの横にある省略記号メニュー（...）で、［カタログの削除］を選択します。
3. 削除するカタログごとに前の手順を繰り返します。

マスターイメージを削除するには

1. ［管理］タブで ［マスターイメージ］をクリックします。
2. イメージを選択し、［削除］をクリックします。
3. 削除するイメージごとに前の手順を繰り返します。

Azure サブスクリプションへのリンクを削除するには

1. ［管理］タブで ［サブスクリプション］をクリックします。
2. 削除するサブスクリプションの横にあるゴミ箱アイコンをクリックします。Azure Portal が開きます。
3. グローバル管理者の Azure 資格情報で、Azure サブスクリプションにサインインします。
4. ［同意する］をクリックして、Virtual Apps Essentials で Azure アカウントにアクセスできるようにします。
5. ［削除］をクリックしてサブスクリプションのリンクを解除します。
6. 他のリンク済みの Azure サブスクリプションについても、上記の手順を繰り返します。

Citrix Cloud Connector VM を削除するには

1. 左上隅のメニューで、［リソースの場所］を選択します。
2. 削除する Cloud Connector VM を特定します。
3. Azure ポータルにサインインします。
4. Azure の ［リソース］ページで目的の VM を削除します。

パートナーリソース

Microsoft のクラウドソリューションプロバイダーチャネルで、本サービスの提供が開始されました。詳しくは、「Citrix Essentials が Microsoft CSP に対応」を参照してください。

支援が必要な場合

Virtual Apps Essentials で問題が発生した場合は、「ヘルプとサポートの利用」の手順に従ってチケットを作成してください。

詳細情報

- Virtual Apps Essentials 環境での Citrix ポリシーの使用について詳しくは、CTX220345を参照してください。
- カタログ作成エラーをトラブルシューティングするには、CTX224151を参照してください。

Citrix Virtual Apps and Desktops Standard for Azure へのアップグレード

詳しくは、Citrix Virtual Apps Essentials から Citrix Virtual Apps and Desktops Standard for Azure へのアップグレードに関する記事を参照してください。

Citrix Virtual Desktops Essentials

September 17, 2021

Citrix Virtual Desktops Essentials では、Microsoft Azure で Windows 10 仮想デスクトップを管理および配信できます。

Virtual Desktops Essentials は、Azure Marketplace 専用に設計されています。シトリックスと Microsoft は、Virtual Desktops Essentials と Azure IaaS（Infrastructure as a Service）のエクスペリエンスを統一するパートナー関係を結んでいます。このパートナー関係により、単一のインターフェイスで、Azure からの完全な Windows 10 のデジタルワークスペースの配信を実現しています。

Virtual Desktops Essentials により、次のことが可能です:

- Azure 上に Windows 10 仮想デスクトップを展開して保護する
- Citrix HDX の各種機能を使用して最高レベルのユーザーエクスペリエンスを提供する
- Citrix Workspace アプリを使用して任意のデバイスにセキュアなアクセスを提供する
- Microsoft Azure および Citrix Cloud から展開を管理する

Citrix Virtual Desktops Essentials では、Windows 10 を簡単に展開できます。単一の管理プレーンでデスクトップを迅速に展開し、大量のデスクトップをまとめて管理し、ユーザーに充実したアクセス環境を提供できます。

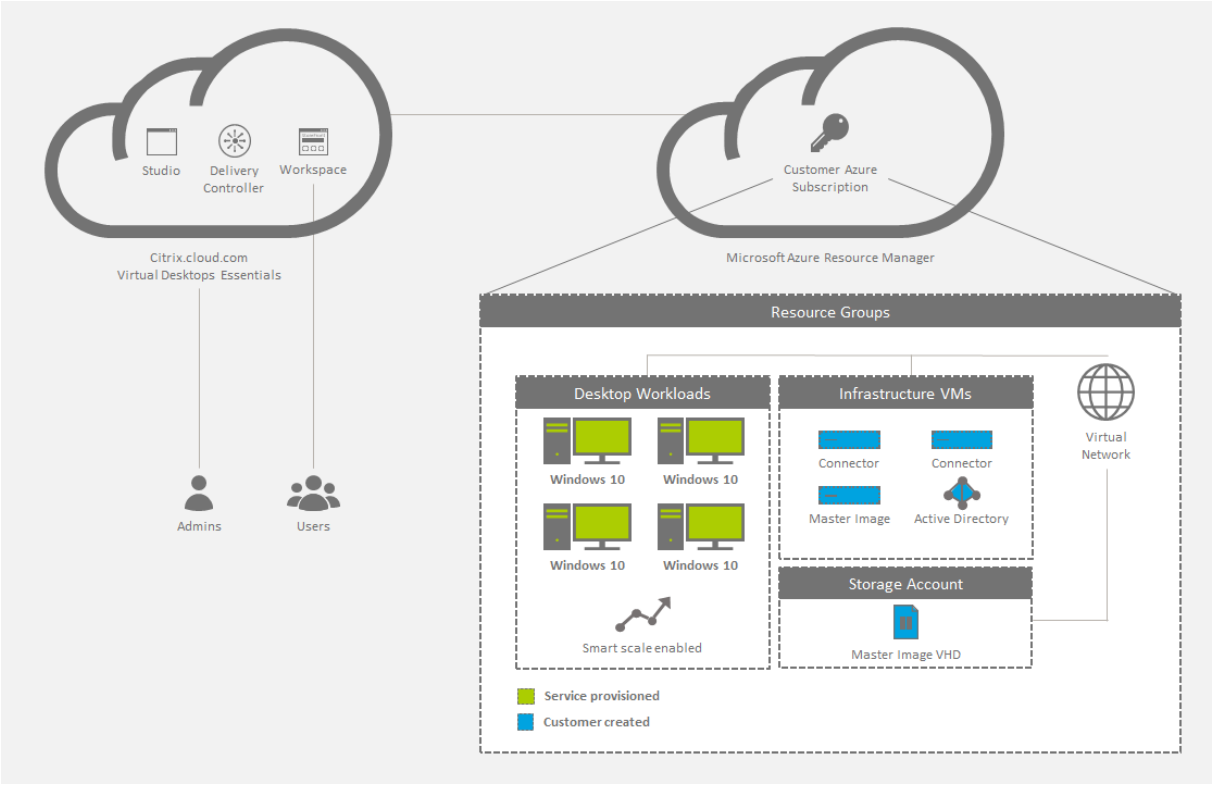
Windows 10 デスクトップの管理は Citrix Studio で、セッションの監視は Citrix Director で行います。ユーザーは Citrix Workspace アプリにログオンして、Windows 10 仮想デスクトップに接続します。

Citrix Virtual Desktops Essentials を構成した後に、Citrix Workspace への URL をユーザーに提供します。ユーザーは、自分のデバイス上の Citrix Workspace アプリを使用して、提供された URL でデスクトップに接続します。ユーザーが Citrix Workspace アプリにログオンすると、Windows 10 デスクトップのアイコンがワークスペースウィンドウに表示されます。

> 重要:
>
> Virtual Desktops Essentials で Citrix Workspace URL が表示されます。この URL の形式は通常、「`https://<yourcompanyname>.cloud.com`」です。Virtual Desktops Essentials のセットアップが完了したら、利用者がデスクトップにアクセスできるように、ワークスペースの URL リンクをテストして利用者と共有します。Virtual Desktops Essentials では、オンプレミス StoreFront はサポートされません。

ワークスペースについて詳しくは、「Workspace の構成」を参照してください。

次の図に、Virtual Desktops Essentials の展開アーキテクチャの概要を示します。



新機能

2018 年 12 月：クラウドホスト **StoreFront** が削除されました

クラウドホスト StoreFront は、Virtual Desktops Essentials で使用できなくなりました。2017 年 12 月以前に Virtual Desktops Essentials（XenDesktop Essentials の新名称）を購入したお客様は、この記事で説明しているように、Citrix Workspace を使用して、利用者にデスクトップアクセスを提供できます。

2018 年 8 月：新しい製品名

一定期間シトリックスのお客様かパートナーだった経験がある方は、製品や製品ドキュメントに新しい名前が使用されていることにお気付きになるかもしれません。このシトリックス製品を初めてお使いになる場合、製品またはコンポーネントで異なる名前が表示されることがあります。

新しい製品名とコンポーネント名は、シトリックスの製品ラインとクラウド戦略の拡大によるものです。ここでは、次の名前を使用します。

- **Citrix Virtual Desktops Essentials**：業界トップクラスの XenDesktop テクノロジが拡張され、Citrix Virtual Desktops となりました。Citrix Virtual Desktops において VDI は、先進的なコンテキストに統合され、セキュリティ保護されたアプリとして、あらゆる作業アプリケーションにセキュアにアクセスするために優先して使用される方法です。XenDesktop Essentials は、Citrix Virtual Desktops Essentials に変更されました。
- **Citrix Workspace** アプリ： Citrix Workspace アプリには、既存の Citrix Receiver テクノロジやその他の Citrix Workspace クライアントテクノロジが組み込まれています。エンドユーザーに最高の作業を実行するために必要なすべての作業アプリ、ファイル、およびデバイスと対話できる統合されたコンテキスト上のエクスペリエンスをエンドユーザーに提供するための追加機能を提供するように拡張されました。
- **Citrix Gateway**：NetScaler Gateway は、Citrix Gateway になりました。Citrix Gateway を使用すると、ベストな仕事を行うために必要なアプリケーションやデータに、安全かつコンテキストに応じたアクセスが可能になります。

製品内のコンテンツには、以前の名前が含まれている場合があります。たとえば、コンソールのテキスト、メッセージ、ディレクトリ名またはファイル名に以前の名前が含まれている場合があります。既存のお客様のスクリプトの破損を防ぐために、コマンドや MSI などの一部のアイテムでは、以前の名前を引き続き保持できます。

関連する製品ドキュメントや、この製品のドキュメントからリンクされているその他のリソース（ビデオやブログの投稿など）には、以前の名前が含まれている場合があります。この移行の間はご迷惑をおかけしますが、何卒ご容赦願います。新しい名前について詳しくは、https://www.citrix.com/about/citrix-product-guide/を参照してください。

Virtual Desktops Essentials の購入方法

Virtual Desktops Essentials を購入またはキャンセルする方法について詳しくは、『How to buy or cancel the Virtual Desktops Essentials Service』を参照してください。

システム要件、前提条件、および互換性

Virtual Desktops Essentials を利用するには、いくつかの補完用の製品とコンポーネントのほか、インストール、構成、操作を行うための特定のアカウント権限が必要になります。

Microsoft Azure

Virtual Desktops Essentials は、Microsoft Azure のみをサポートするように設計されています。使用する Azure 環境は、Virtual Desktops Essentials をサポートするための最低要件を満たす必要があります:

- エンタープライズ契約による Azure サブスクリプションまたは Microsoft CSP Azure サブスクリプション。
- Windows Server Active Directory または Azure Active Directory Domain Services
- Azure Active Directory のテナント

  > 重要:
  >
  > Windows 10 デスクトップを展開するには、Azure サブスクリプションに Azure Active Directory のテナントが含まれている必要があります。Azure Active Directory のテナントまたは別のアクティブディレクトリを使用することで、承認済みのユーザーを識別できます。

- Active Directory ドメインコントローラー
- 目的のリージョンに配置された Azure Resource Manager（ARM）の仮想ネットワークとサブネット。仮想ネットワークには、ドメインコントローラーをポイントするカスタムドメインネームサーバー（DNS: Domain Name Server）エントリを構成します。また仮想ネットワークには、デスクトップを保持できる大きさのサブネットが 1 つ必要です。

  DNS エントリとデスクトップサブネットには同じ仮想ネットワークを使用してください。
- サブスクリプションに含まれる共同作成者以上の権限を持つ Azure Active Directory ユーザー
- 必要なカスタマイズやアプリケーションなどを含め Microsoft Windows 10 がインストールされている仮想マシン 1 台

Citrix Cloud Connector

Citrix Cloud Connector により、Citrix Cloud とリソースの場所との間の通信が認証および暗号化されます。Virtual Desktops Essentials では、リソースは Microsoft Azure に配置されます。Citrix Cloud を使用するには、リソースの場所を中断なくに利用できるよう、2 つの Windows サーバー仮想マシンに Citrix Cloud Connector をインストールする必要があります。

Cloud Connector について詳しくは、「Citrix Cloud Connector」を参照してください。

Citrix Cloud

- Citrix Cloud アカウント

- Citrix Cloud 内の Citrix Virtual Apps and Desktops サービスへのアクセスは、Virtual Desktops Essentials の購入の一部として有効になっています。
- （オプション）ICA プロキシモードに構成した Citrix ADC VPX 1 つ。社内ネットワーク外からのアクセス用です。
  - ICA プロキシにより、ユーザーに提供するアプリケーションおよびデスクトップへ安全にアクセスできるようになります。
  - Citrix ADC VPX の設定について詳しくは、「Microsoft Azure での Citrix NetScaler VPX の展開」を参照してください。

既知の問題

- Citrix ヘルプデスク管理者のカスタムアクセスロールが正しく機能しない。回避策として、クラウド管理者ロールを使用するか、フルアクセスを有効にします。[BRK-3589]
- Azure AD Domain Services を使用する場合：ワークスペースのログオン UPN（User Principal Name：ユーザープリンシパル名）には、Azure AD Domain Services の有効化時に指定したドメイン名を含める必要があります。作成したカスタムドメインをプライマリとして指定している場合でも、ログオンにカスタムドメインの UPN を使用することはできません。

ステップ 1：Azure サブスクリプションを Virtual Desktops Essentials に接続する

1. Azure ポータルにサインインします。
2. Azure でドメイン参加済みの Windows Server 仮想マシンを開き、Web ブラウザーを開きます。
3. 仮想マシンの Web ブラウザーで、Citrix Cloudにサインインします。Virtual Apps and Desktops サービスが開きます。
4. 左上のメニューで、［リソースの場所］を選択します。
5. ［リソースの場所］ページで ［ダウンロード］をクリックします。`cwcconnector.exe`ファイルをダウンロードします。
6. ダウンロードしたプログラムをダブルクリックして、インストーラーを起動します。
7. 画面の指示に従って Citrix Cloud の資格情報を入力します。画面の指示に従って、Citrix Cloud Connector をインストールして構成します。
8. Cloud Connector をもう 1 つインストールするには、1 つ以上の他のサーバー VM で手順 4～7 を繰り返します。

Cloud Connector のインストール時、インストールを実行するユーザーを認証し、インストーラーの権限を検証し、Cloud Connector が提供するサービスをダウンロードして構成するために、Citrix Cloud にアクセスします。インストールには、インストールを開始したユーザーの権限が使用されます。

インストール後、Citrix Cloud 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。詳しくは、「ID およびアクセス管理」を参照してください。

ステップ **2**：ホスト接続を作成する

始める前に、Azure Active Directory の資格情報とサブスクリプション ID を用意してください。ホスト接続を作成する Azure AD ユーザーは、Azure AD のネイティブクラウドユーザーであるか、エンタープライズドメインと同期している必要があります。ユーザーアカウントに、招待または委任された Microsoft アカウントは使用できません。

1. Citrix Cloudにサインインします。
2. 左上のメニューで、［マイサービス］**>**［**Virtual Apps and Desktops**］を選択します。
3. ［管理］をクリックします。Studio 管理コンソールが開きます。
4. Studio の［ナビゲーション］ペインで ［構成］**>**［ホスト］の順に選択します。
5. ［操作］ペインの ［接続およびリソースの追加］をクリックします。
6. ［接続およびリソースの追加］ページで次の操作を行います：
    a) ［接続の種類］で ［**Microsoft Azure**］を選択します。
    b) Azure 環境で ［**Azure Global**］を選択し、［次へ］をクリックします。
7. ［接続の詳細］で次の操作を行います：
    a) ［サブスクリプション **ID**］に Azure サブスクリプション ID を入力します。
    b) ［接続名］に接続名を入力し、次の操作のどちらかを行います：
        i. ［新規作成］をクリックして「オプション 1：接続を作成する」の手順に従います。
        ii. ［既存のものを使用］をクリックしてさらに設定を構成します。「オプション 2：既存のホスト接続を使用する」の手順に進みます。

オプション **1**：接続を作成する

1. サブスクリプションの共同作成者以上のアカウントで Azure にサインインします。
2. Azure によりホスト接続が自動で作成されます。Studio で、［接続済み］というテキスト付きの緑色のチェックマークが、［接続およびリソースの追加］ページに表示されます。
3. ［次へ］をクリックします。
4. ［リージョン］ページで、仮想ネットワークが存在するリージョンを選択して ［次へ］をクリックします。
5. ［ネットワーク］ページで以下の設定を行います：
    a) リソースの名前を入力します。
    b) リソースグループの仮想ネットワークを選択します。
    c) リソースグループに適用するサブネットを選択し、［次へ］をクリックします。
6. ［概要］ページで ［完了］をクリックします。Microsoft Azure Resource Manager へのホスト接続が完成します。

オプション **2**：既存のホスト接続を使用する

［既存のものを使用］をクリックすると、［既存のサービスプリンシパルの詳細］ページが表示されます：

1. ［サブスクリプション **ID**］に Microsoft Azure サブスクリプション ID を入力します。
2. ［サブスクリプション名］に Azure サブスクリプションの名前を入力します。

3. [**OK**] をクリックします。
4. [接続] ページで以下を実行します:
    a) [新しい接続を作成する] をクリックし、Microsoft Azure サブスクリプション ID と接続名（オプション）を入力して、[新規作成] をクリックします。Microsoft 認証ダイアログボックスが表示されます。

    以前に作成した接続を使用する場合は、[既存の接続を使用する] を選択します。次に、接続を選択します。

    b) Microsoft Azure Active Directory ユーザーのユーザー名とパスワードを入力します。Citrix Cloud により、指定したサブスクリプションのマシンを作成および管理する権限を持つサービスプリンシパルが作成されます。
5. [リージョン] ページで、Microsoft Azure リソースグループが存在する Azure リージョンを選択します。
6. [ネットワーク] ページで以下の設定を行います:
    a) リソースの名前を入力します。接続名を入力した場合は、その接続名をリソース名に使用してください。
    b) Microsoft Azure リソースグループの仮想ネットワークを選択します。
    c) この接続に使用するサブネットを選択します。サブネットが 1 つしか存在しない場合は、そのサブネットがデフォルトで選択されます。

ステップ **3**: **Windows 10** デスクトップのプールを作成する

デスクトップをホストする準備として、Windows 10 仮想マシンに Citrix Virtual Delivery Agent（VDA）ソフトウェアをインストールします。VDA には次の機能があります:

- マシンが Virtual Desktops Essentials に登録できるようになります。
- マシンとユーザーデバイスとの間の接続を確立して管理します。
- ユーザーまたはセッションで Citrix ライセンスが使用可能であることを確認します。
- 構成済みのポリシーをセッションに適用します。
- セッション情報を Virtual Desktops Essentials に通知します。

基本イメージに **VDA** をインストールするには

1. Windows 10 イメージを起動します。
2. https://www.citrix.com/downloads/citrix-cloud/product-software/xenapp-and-xendesktop-service.htmlに移動して、デスクトップ OS 用の VDA をダウンロードします。
3. VDA のインストールを開始します。
4. [環境] ページで、[マスター **MCS** イメージを作成する] を選択します。
5. [追加コンポーネント] ページで、[**Citrix App-V** 公開コンポーネントを有効にする] 以外のすべてのコンポーネントを選択します。
6. [**Delivery Controller**] ページで、Cloud Connector 仮想マシンの場所を入力します。[次へ] をクリックして、警告メッセージを確認します。

7. ［機能］ページで、すべての設定をデフォルトのままにして ［次へ］をクリックします。
8. ［次へ］をクリックし、残りのページはデフォルト設定のままにします。
9. ［概要］ページで ［インストール］をクリックします。
10. 仮想マシンを再起動し、再びサインインします。
11. 設定が有効になったことを確認します。
12. 仮想マシンをシャットダウンします。VDA を登録するには、仮想マシンをシャットダウンする必要があります。

ストレージアカウントを作成する

Microsoft Azure では、基本イメージの仮想ハードディスクをホストするためのストレージアカウントが必要になります。既存のストレージアカウントでドライブをホストするか、ストレージアカウントを作成することができます。

> 重要:
>
> マシンカタログを作成する前に、Azure の目的のストレージアカウントに Windows 10 マスターイメージをアップロードしてください。

イメージ用のストレージアカウントを作成するには

1. Microsoft Azure のナビゲーションペインで、［ストレージアカウント］をクリックします。
2. ［ストレージアカウント］ページで ［追加］をクリックします。
3. ［名前］に名前を入力します。
4. ［デプロイモデル］で ［リソースマネージャー］を選択します。
5. ［パフォーマンス］で ［標準］を選択します。
6. ［レプリケーション］、［**Storage Service Encryption**］、［サブスクリプション］についてはデフォルト設定のままにします。
7. ［リソースグループ］で、次のいずれかの操作を行います:
   a) リソースグループを作成する場合は ［新規作成］をクリックします。グループの名前を入力します。
   b) 既存のリソースグループを使用する場合は、［既存のものを使用］をクリックします。グループを選択します。
8. このストレージアカウントをダッシュボードに表示するには、［ダッシュボードにピン留めする］をクリックします。
9. ［作成］をクリックします。

ストレージアカウントを作成したので、次は BLOB コンテナを作成し、「VHD」など仮想ハードディスクを表す名前を付けます。

イメージ **VHD** 用の **BLOB** コンテナを作成するには

1. Microsoft Azure のナビゲーションペインで、［ストレージアカウント］をクリックし、先ほど作成したストレージアカウントを選択します。

2. [**BLOB** サービス] の中央のナビゲーションペインで、[コンテナ] をクリックします。
3. [詳細] ペインで [コンテナ] をクリックします。
4. [新しいコンテナ] ペインで、コンテナに名前を付けます。
5. [アクセスの種類] で [**BLOB**] を選択し、[作成] をクリックします。新しい BLOB コンテナがペインに表示されます。
6. BLOB の URL をコピーしてテキストファイルに保存します。この URL は、後で変換した VHD をアップロードするために使用します。

Citrix Virtual Desktops Essentials のマシンカタログを作成する

マシンカタログとは、単一のエンティティとして管理する仮想デスクトップをグループ化したものです。これらの仮想デスクトップが、ユーザーに提供するリソースになります。カタログ内のすべてのマシンには、同じオペレーティングシステムおよび VDA がインストールされている必要があります。

通常、管理者はマスターイメージを作成して、それを基にカタログ内に同一構成の仮想マシンを作成します。

1. Citrix Cloud にサインインします。左上のメニューで、[マイサービス] **>** [**Virtual Apps and Desktops**] を選択します。
2. [管理] タブを選択します。
3. Studio のナビゲーションペインで [マシンカタログ] をクリックします。
4. [操作] ペインの [マシンカタログの作成] をクリックします。
5. [オペレーションシステム] ページで、デスクトップ OS だけがオプションとして表示されていることを確認します。表示されているオプションを選択し、[次へ] をクリックします。
6. [デスクトップエクスペリエンス] ページで、次の操作を行います:
   a) [ユーザーがログオンするたびに同じデスクトップに接続する（静的)] をオンにします。
   b) [はい、専用の仮想マシンを作成してローカルディスクに変更を保存する] を選択します。
7. [マスターイメージ] ページで、次の操作を行います:
   a) 先ほど作成した BLOB ストレージ内の VHD に移動し、選択します。ナビゲーションツリーは、Azure の階層に沿った構造になっています:
      - リソースグループ
      - ストレージアカウント
      - コンテナ
      - 仮想ハードディスク（VHD）
      - イメージ名
   b) [このカタログの最小機能レベルを選択します] のオプションは、デフォルトのままにします。
8. [ストレージとライセンスの種類] ページで、目的のストレージの種類とライセンスの設定を選択します。
9. [仮想マシン] ページで、仮想マシンの数と Azure 仮想マシンのサイズを選択します。
10. [ネットワークインターフェイスカード] ページで、Citrix マシンの Azure サブネット名に関連付けるネットワークアダプタを選択します。[カードの追加] をクリックして、さらにネットワークアダプタを追加することもできます。
11. [コンピューターアカウント] ページで、次の操作を行います:

a) ［新しい **Active Directory** アカウントを作成する］をクリックします。
b) コンピューターアカウントのドメインを選択します。
c) 新しいマシンの組織単位（OU）を選択します。
d) 新しいマシンのアカウントの命名方式を入力します。番号を自動的に増加させるには、2 つの数字記号（##）を入力します。数字か文字かを選択します。ポンド（#）記号は命名規則に沿って変換されます。たとえば、mymachcatalog## は mymachcatalog01 または mymachcatalogAB になります。

12. ［ドメイン資格情報］ページで ［資格情報の入力］をクリックし、［**Windows** セキュリティ］ダイアログボックスでユーザー名とパスワードを入力します。このアカウントが、コンピューターアカウントの作成に使用されます。
13. ［概要］ページで、カタログの名前と管理者用の説明を入力します。
14. ［完了］をクリックします。

仮想マシンが作成され、新しいストレージアカウントが Microsoft Azure のダッシュボードに表示されます。マシンカタログサービスによる仮想マシンの展開中、Azure には VHD を備えた準備用の仮想マシンが一時的に作成されます。

Microsoft Azure でイメージ名を特定するには

1. Azure ポータルにサインインします。
2. ダッシュボードのナビゲーションペインで、［すべてのリソース］をクリックします。サブスクリプションの一覧が表示されます。
3. 該当するサブスクリプションを選択します。
4. ［すべての設定］をクリックします。
5. ［リソースグループ］をクリックします。
6. 該当するリソースグループを選択します。
7. Citrix VDA のインストールが含まれる Windows 10 仮想マシンを選択します。
8. ［すべての設定］をクリックします。
9. ［ディスク］をクリックします。
10. OS ディスクを選択します。［OS ディスク］ウィンドウの最初のテキストボックスに、イメージの URL が次の例のような形式で表示されます。この URL から、ストレージアカウント名とイメージ名が得られます。例: `https://<storage account name>.blob.core.window.net/vhds/<image name>`。
11. ［マシン］ページの一覧のテンプレートは、Azure サブスクリプションから直接取得されます。

ステップ **4**: **Windows 10** デスクトップをユーザーに割り当てる

デリバリーグループは、1 つ以上のマシンカタログから選択したマシンをグループ化したものです。デリバリーグループでは、これらのマシンを使用できるユーザーを指定します。

1. Studio のナビゲーションペインで ［デリバリーグループ］を選択し、［操作］ペインの ［デリバリーグループの作成］を選択します。

2. デリバリーグループで使用可能にするマシンの数を指定します。マシンカタログで使用可能になるマシンの数よりも大きな数値は指定できません。
3. ［配信の種類］ページで ［デスクトップ］を選択します。
4. ［ユーザー］ページで、ユーザー管理を Citrix Cloud に任せるオプションを選択します。このオプションを選択すると、Citrix Cloud でデリバリーグループへのアクセスを管理できるようになります。（Studio からユーザーを追加することもできます。）
5. ［概要］ページで、デリバリーグループの名前と、必要に応じて説明を入力します。

上記の手順を完了したら、デリバリーグループを編集してユーザーのアクセスを構成します。ユーザーの追加や削除、ユーザー設定の変更を行うことができます。

Studio でデリバリーグループのユーザーを追加または削除する

1. Studio のナビゲーションペインで ［デリバリーグループ］を選択します。
2. グループを選択して、［操作］ペインの ［デリバリーグループの編集］をクリックします。
3. ユーザーを追加する場合は、［ユーザー］ページで ［追加］をクリックし、追加するユーザーを指定します。ユーザーを削除する場合は、1 人または複数のユーザーを選択し、［削除］をクリックします。また、チェックボックスをオンまたはオフにして、匿名ユーザーによるアクセスを有効化または無効化することもできます。
4. ［**OK**］をクリックします。

Studio でデリバリーグループのユーザー設定を変更する

このページの名前には、［ユーザー設定］または ［基本設定］のどちらかが表示されます。

1. Studio のナビゲーションペインで ［デリバリーグループ］を選択します。
2. グループを選択して、［操作］ペインの ［デリバリーグループの編集］をクリックします。
3. ［ユーザー設定］（または ［基本設定］）ページで、次の操作を行います：
    a) ［説明］に、ワークスペースでユーザーに表示されるテキストを入力します。
    b) Azure のタイムゾーンに合わせてタイムゾーンを設定します。
    c) ［デリバリーグループの有効化］をオンにします。
    d) ユーザーごとのデスクトップの最大数を設定します。
4. ［**OK**］をクリックして設定を保存します。

Citrix Cloud でユーザーアクセスを追加する

1. Citrix Cloud にサインインし、［ライブラリを表示］をクリックします。
2. ［デスクトップ］タイルで、右隅にある省略記号（...）をクリックします。
3. デリバリーグループへのアクセスを許可するユーザーグループを検索して、一覧に追加します。
4. 完了したら、［**X**］をクリックしてウィンドウを閉じます。

利用者リストへ追加したグループに、Windows 10 仮想デスクトップが割り当てられます。

ステップ **5**：**Azure** で **Citrix ADC VPX** を構成する（オプション）

Citrix ADC VPX 仮想アプライアンスは、Microsoft Azure Marketplace でイメージとして使用することができます。Microsoft Azure Resource Manager（ARM）で Citrix ADC VPX を展開すると、Azure のクラウドコンピューティング機能を活用できるようになります。また、ビジネスのニーズに合わせて Citrix Gateway の負荷分散機能とトラフィック管理機能を使用することもできます。

Citrix ADC VPX インスタンスは、次の 2 通りの方法で Azure Resource Manager に展開できます：

- スタンドアロンのインスタンス
- アクティブ/アクティブモードまたはアクティブ/スタンバイモードの高可用性ペア

リモートから接続するユーザーがいる場合は、Azure で Citrix ADC VPX を構成し、Citrix Workspace アプリと Windows 10 デスクトップ間にセキュアな接続を作成します。

展開が完了したら、リモートデスクトッププロトコル（RDP：Remote Desktop Protocol）を使用していずれかの Cloud Connector マシンに接続します。接続したら、Citrix Gateway 管理コンソールから引き続き Citrix ADC VPX の構成を行います。

構成について詳しくは、「Deploying Citrix ADC VPX instance on Microsoft Azure」を参照してください。

Azure で Citrix ADC VPX を設定したら、Citrix Cloud で Citrix Gateway を有効にします。

アクセスを保護するように **Citrix Gateway** の設定を構成するには

1. Citrix Gateway の管理者資格情報を使用して、管理者コンソールにログオンします。IP アドレスを追加で構成する必要はありません。［スキップ］をクリックします。
2. ［ホスト名］、［**DNS IP** アドレス］、［タイムゾーン］に、仮想ネットワークの IP アドレスと DNS 設定を入力します。この設定は、Active Directory ドメインコントローラ上で確認できます。
3. ［完了］をクリックします。この段階では Citrix ADC VPX を再起動する必要はありません。
4. ［構成］タブの ［ライセンス］をクリックし、Citrix Gateway の構成に必要なライセンスをアップロードします。
5. ライセンスをアップロードしたら、アプライアンスを再起動します。
6. 仮想マシンが再起動したら、Citrix Gateway の資格情報を使用して再度ログオンします。

Citrix Gateway で **Citrix Virtual Desktops Essentials** の設定を構成する

上記の設定を構成したら、Citrix Gateway で Quick Configuration ウィザードを実行します。詳しくは、「Configuring Settings with the Quick Configuration Wizard」を参照してください。

高可用性および負荷分散に合わせて **Citrix Gateway** を構成する

Microsoft Azure 展開環境では、Azure ロードバランサーを使用することで、2 台の Citrix 仮想マシンから成る高可用性構成を実現できます。ロードバランサーにより、クライアントトラフィックが両方の Citrix Gateway インスタンスで構成されている仮想サーバー全体に分散されます。

クライアントトラフィックがインターネットから発生している場合には、インターネットと Citrix Gateway インスタンスの間に外部ロードバランサーを展開し、クライアントトラフィックを分散させます。この構成について詳しくは、「Configure a high-availability setup with a single IP address and a single NIC」を参照してください。

受信ポート 80 を Citrix Gateway のネットワークセキュリティグループに追加して、Citrix Gateway のパブリック IP アドレスを使用して Citrix Gateway を構成することもできます。この構成が完了したら、管理コンソールへのアクセスの保護のため受信ポート 80 のルールは削除することをお勧めします。

ステップ **6**: ユーザーを接続する

本サービスは、Citrix Workspace によりユーザーデバイスへ配信されます。Citrix Cloud コンソールの左上隅のメニューで ［ワークスペースの構成］を選択します。

最初のカタログを作成すると、Virtual Desktops Essentials によりワークスペースの URL が自動的に構成されます。この URL は、カタログの詳細の下に表示されます。ワークスペースの URL と外観はカスタマイズ可能です。また、Azure Active Directory を使用したフェデレーション認証のプレビューバージョンを有効にすることもできます。詳しくは、「Workspace の構成」を参照してください。

1. Citrix Cloud コンソールの左上隅のメニューで ［ワークスペースの構成］を選択します。［サービス統合］タブを選択します。このサービスが一覧に表示されます。
2. ドメイン資格情報を使用してワークスペース URL にログオンし、デスクトップを起動することで、接続のテストを行います。
3. URL をコピーできるようにユーザーに提供します。ユーザーは、Web ブラウザーまたは Citrix Workspace アプリのアドレスバーにこの URL を入力するか貼り付けることで、デスクトップにアクセスできます。

Citrix ADC VPX を使用したリモートアクセス

1. Citrix Cloud コンソールで、［管理］、［サービス提供］の順にクリックします。
2. ［**Citrix Gateway**］を有効にします。
3. ［リソースの場所］で ［自分の **Citrix Gateway** を使用する］を選択します。
4. テキストフィールドに Citrix Gateway アドレスを入力します。プロトコルは含めないでください。ポート番号は含めることができます。
5. セッション画面の保持を使用する場合は、この機能を有効にします。
6. 保存します。
7. ドメイン資格情報を使用してワークスペース URL にログオンし、デスクトップを起動することで、接続のテストを行います。
8. URL をコピーできるようにユーザーに提供します。ユーザーは、Web ブラウザーまたは Citrix Workspace アプリのアドレスバーに URL を入力するか貼り付けることで、デスクトップにアクセスできます。

パートナーリソース

本サービスは、Microsoft のクラウドソリューションプロバイダーチャネルでも入手できます。詳しくは、「Citrix Essentials が Microsoft CSP に対応」を参照してください。

Citrix Virtual Apps and Desktops Standard for Azure へのアップグレード

詳しくは、Citrix Virtual Desktops Essentials から Citrix Virtual Apps and Desktops Standard for Azure へのアップグレードに関する記事を参照してください。

高度な設定

June 20, 2019

Citrix Cloud ドキュメントサイトの「高度な設定」セクションには、Citrix チームのさまざまな技術情報記事が掲載されています。このセクションの記事は、アプリケーションやデータの配信に役立つ主要コンポーネントを安全かつ耐障害性のある方法で展開するための詳細ガイダンスです。

さらに Citrix の技術専門家によるテクニカル記事、参照アーキテクチャ、およびベストプラクティスが必要な場合は、「Citrix Tech Zone」にアクセスしてください。

Citrix Cloud プラットフォームおよびサービスのコミュニティサポートフォーラムについては、「Citrix Discussions」を参照してください。

Citrix Virtual Apps and Desktops サービス用のオンプレミス StoreFront 認証参照アーキテクチャ

January 22, 2020

Citrix Workspace プラットフォームを使用せず、顧客データセンター内で Citrix StoreFront をホストする理由はさまざまです。一部の環境は複雑であるため、StoreFront がサービスのプライマリユーザーフロントエンドである場合は、Citrix Cloud コンポーネントが StoreFront および Active Directory とどのように通信するかを理解しておく必要があります。

Citrix Workspace は Citrix Virtual Apps and Desktops のほとんどのユースケースの要件を満たすことができますが、StoreFront を顧客のデータセンターやリソースの場所にホストする必要があるユースケースと要件がいくつかあります。

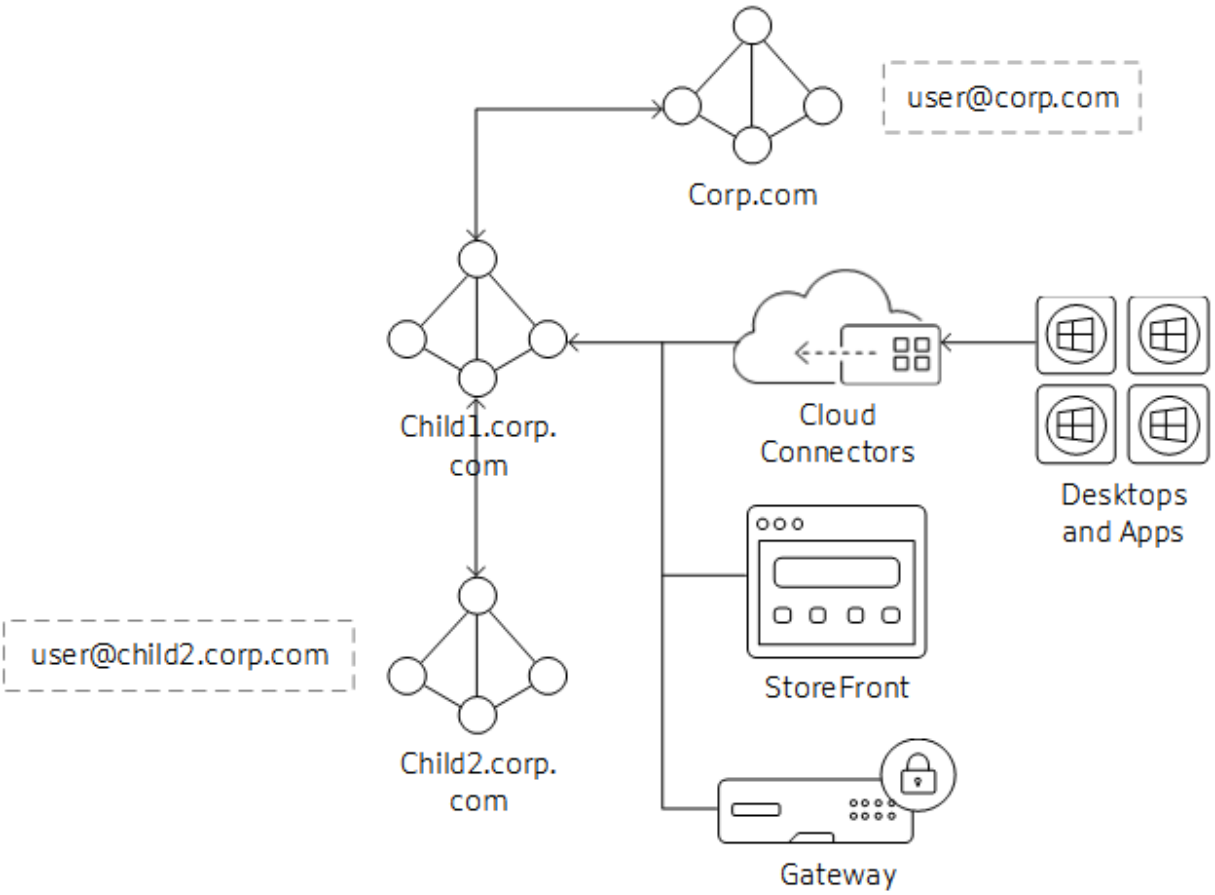
オンプレミス **StoreFront** を保守する理由

- Cloud Connector でのローカルホストキャッシュ機能のサポート
- スマートカードや SAML などの認証方法は、Citrix Workspace ではサポートされていません。
- 非デフォルトのストア構成（web.config の変更）
- 内部ユーザーおよび外部ユーザー用の複数のストア構成のホスティング

この記事では、高レベルのアーキテクチャについて、および、Active Directory の仕様でサポートされているさまざまな認証シナリオとコンポーネントがどのように通信するかについて、説明します。Cloud Connector はドメインの 1 つに参加し、Virtual Apps and Desktops サービスが、Active Directory ユーザーと、ドメインまたは信頼済みドメインのグループを割り当てられるようにします。Cloud Connector は、StoreFront および Citrix Gateway コンポーネント用の Delivery Controller および STA サーバーとしても機能します。

この記事では、StoreFront と Gateway のコンポーネントが、各データセンターで一緒にホストされていることを前提としています。

リソースドメインとしての親子関係のドメイン



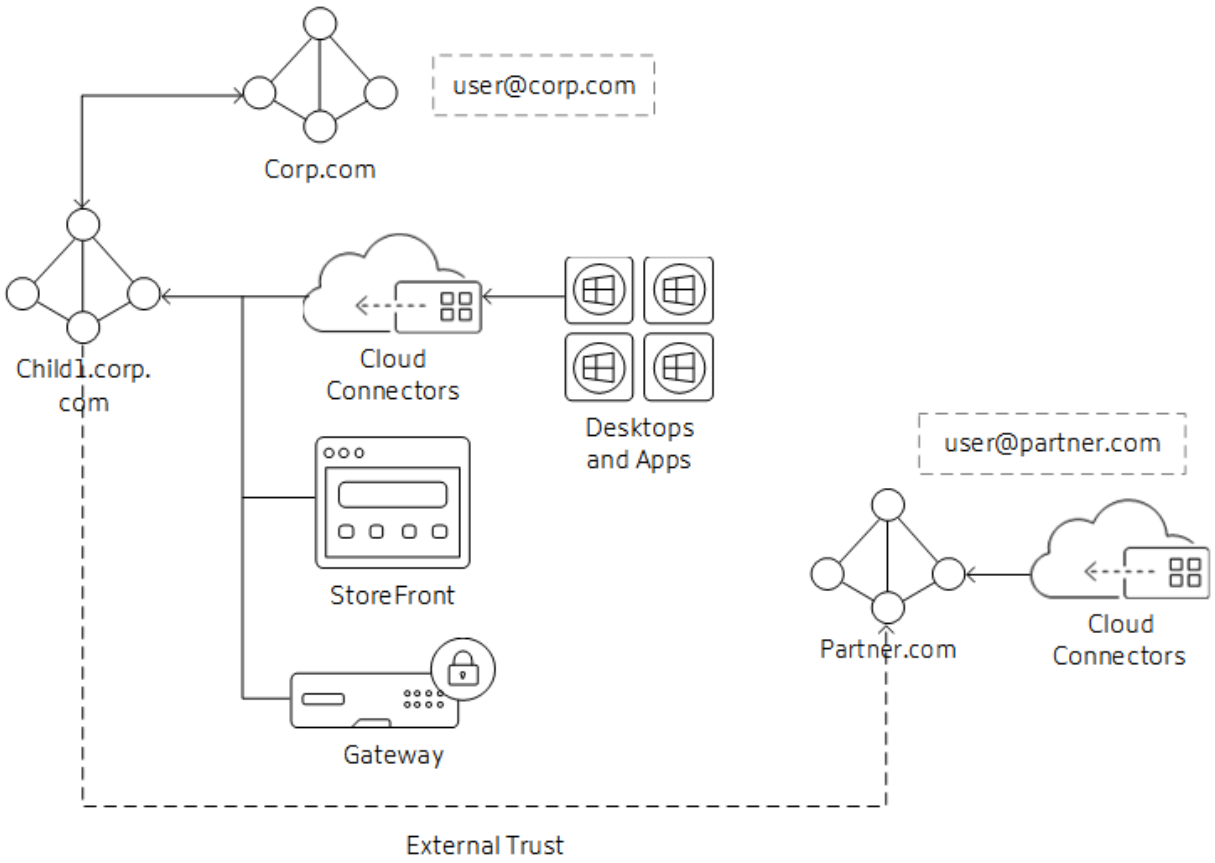
このシナリオでは、子ドメインは Virtual Desktop Agent（VDA）と StoreFront インスタンスのリソースドメインとして機能しています。親ドメインは、子ドメインのリソースにアクセスする予定のユーザーを保持します。

1. Cloud Connector は、子ドメインにのみ参加します。子ドメインと親ドメインの間の双方向の推移的な信頼関係により、Cloud Connector は親ドメインのグローバルカタログと通信できます。
2. StoreFront は子ドメインに参加しています。ストア認証は、Citrix Gateway からユーザー名/パスワードおよびパススルー用に設定されます。ユーザー名/パスワード認証は、任意のドメインを信頼するように設定されています。
3. Citrix Gateway 認証プロファイルは、UPN をプライマリログオン方法として使用するように、親ドメイン用に設定されています。子ドメインから認証する必要があるユーザーがいる場合は、子ドメインの LDAP 認証プロファイルとポリシーも Gateway vServer にバインドする必要があります。
4. Citrix Gateway Session OS と Web のプロファイルを編集し、公開アプリケーション/Single Sign-On Domain 設定を空白に設定します（設定を上書きする必要がある場合があります）。

接続ワークフロー

1. User@corp.com が、Citrix Gateway にログオンします。Gateway は認証プロファイルを介してユーザーを検索し、ポリシーアクションを照合します。
2. 資格情報が StoreFront に渡されます。StoreFront は資格情報を受け入れて Cloud Connector に渡します（Delivery Controller として機能します）。
3. Cloud Connector は、Citrix Cloud に必要なユーザーオブジェクトの詳細を調べます。
4. Cloud Connector は ID 情報を Citrix Cloud に渡し、ID トークンはユーザーを認証して、ユーザーに割り当てられているリソースを列挙します。
5. Cloud Connector は、ユーザーの列挙のために、割り当てられたリソースを StoreFront に返します。
6. ユーザーがアプリケーションまたはデスクトップを起動すると、Citrix Gateway は設定済みの Cloud Connector を使用して、STA チケット要求を生成します。
7. Citrix Cloud ブローカーは、リソースドメインの Cloud Connector とそのリソースの場所に登録されている VDA との間のセッションを管理します。
8. セッションは、クライアント、Citrix Gateway、解決済みの VDA の間で確立されます。

外部の信頼済みドメインからリソースドメインへ



このシナリオでは、ビジネスパートナーはコーポレートユーザーに公開されているリソースにアクセスする必要があります。企業ドメインは corp.com で、パートナードメインは partner.com です。

1. 企業ドメインは、パートナードメインに対して送信できる外部の信頼を持っています。パートナードメインのユーザーは、企業ドメインに参加しているリソースに対して認証できます。
2. Citrix Cloud の顧客には、corp.com の Cloud Connector 用と partner.com の Cloud Connector 用の 2 つのリソースの場所が必要です。partner.com の Cloud Connector は、ドメインへの認証および ID 呼び出しにのみ必要です。VDA やセッションの仲介には使用されません。
3. StoreFront は、corp.com のドメインに参加しています。corp.com ドメインの Cloud Connector は、ストア構成の Delivery Controller として使用されます。ストア認証は、Citrix Gateway からユーザー名/パスワードおよびパススルー用に設定されます。ユーザー名/パスワード認証は、任意のドメインを信頼するように設定されています。
4. Citrix Gateway 認証プロファイルは、UPN をプライマリログオン方法として使用するように、corp.com ドメイン用に設定されています。UPN を使用し、それを corp.com ドメインと同じ Gateway vServer にバインドするよう、partner.com ドメインの 2 番目のプロファイルとポリシーを設定します。
5. Citrix Gateway Session OS と Web のプロファイルを編集し、公開アプリケーション/Single Sign-On Domain 設定を空白に設定します（設定を上書きする必要がある場合があります）。

> 注:
>
> 外部の信頼済みドメインの場所によっては、外部ドメインのユーザーはリソースまたは親ドメインのユーザーよりも起動時間が長くなる可能性があります。

接続ワークフロー

1. User@partner.com が、Citrix Gateway にログオンします。Gateway は、UPN 参照を照合する認証プロファイルを介してユーザーを検索し、ポリシーアクションを照合します。
2. 資格情報が StoreFront に渡されます。StoreFront は資格情報を受け入れて Cloud Connector に渡します(Delivery Controller として機能します)。
3. Cloud Connector は、Citrix Cloud に必要なユーザーオブジェクトの詳細の参照を実行します。
4. Cloud Connector は ID 情報を Citrix Cloud に渡し、ID トークンはユーザーを認証して、ユーザーに割り当てられているリソースを列挙します。
5. Cloud Connector は、ユーザーの列挙のために、割り当てられたリソースを StoreFront に返します。
6. ユーザーがアプリケーションまたはデスクトップを起動すると、Citrix Gateway は設定済みの Cloud Connector を使用して、STA チケット要求を生成します(この場合は child1.corp.com から)。
7. Citrix Cloud ブローカーは、リソースドメインの Cloud Connector とそのリソースの場所に登録されている VDA との間のセッションを管理します。
8. このセッションはクライアント、Citrix Gateway、および解決された VDA の間で確立されます。

リソースドメインへのフォレストの信頼/ショートカットの信頼

フォレストの信頼およびショートカットの信頼のドメインは、リソースドメインに対する外部ドメインの信頼関係として扱われる場合にのみサポートされます。フォレストの信頼については、「外部の信頼済みドメインからリソースドメインへ」セクションで説明されているのと同じ手順に従うことができます。このセクションの内容は、ユーザーとリソース間のネイティブのフォレストの信頼のサポート状況によって、将来変更される可能性があります。

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States