Webex Hybrid Directory サービス

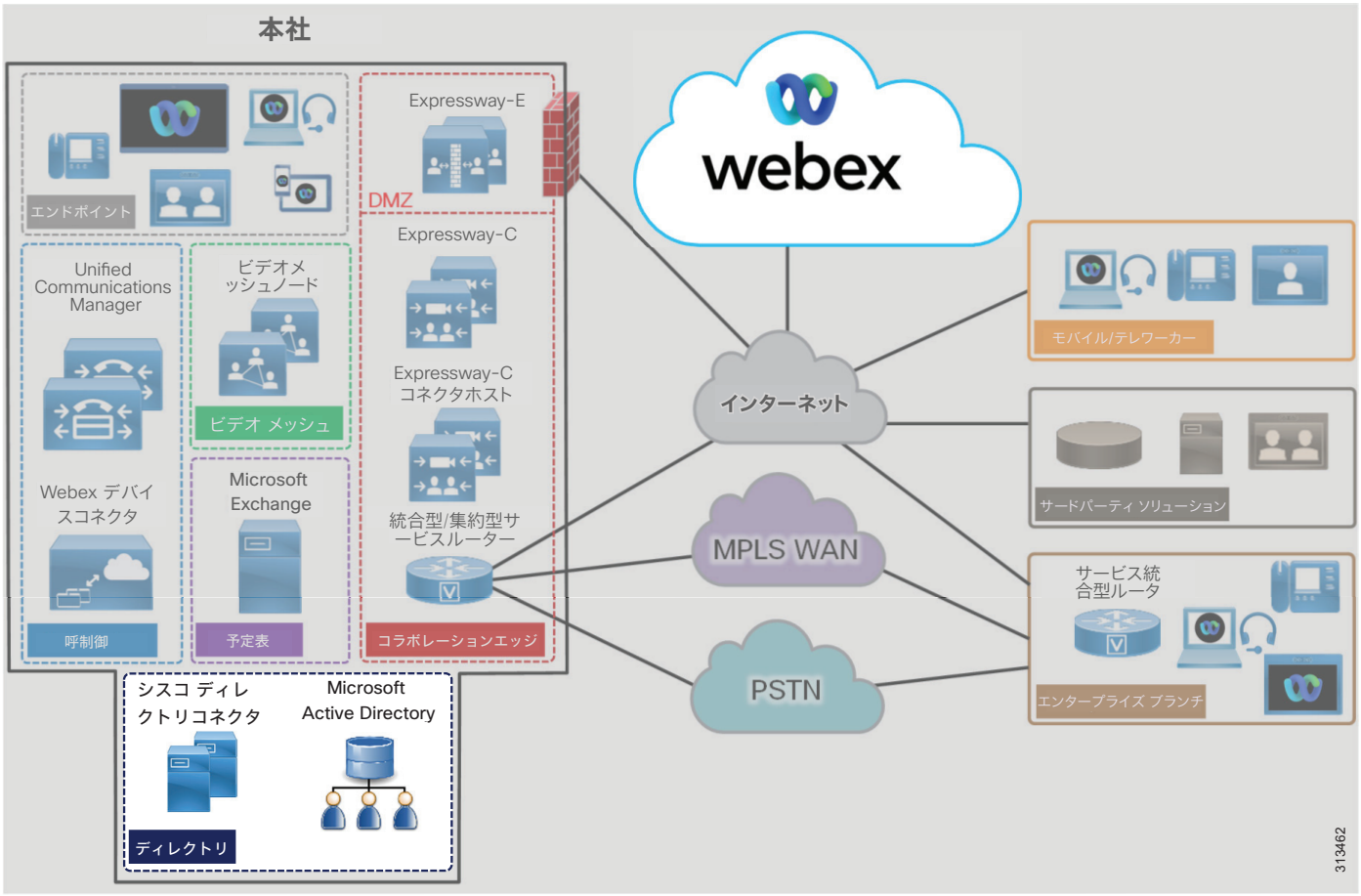
改訂日： 2021 年 10 月 22 日

Webex ハイブリッドサービスを使用すると、Webex カスタマーは、オンプレミス コラボレーション サービスを Webex に接続することができます。オンプレミスの LDAP ディレクトリとカスタマーの Webex 組織内の ID サービスとの間のディレクトリサービスを統合することで、ユーザーのオンボーディングを簡素化し、付加価値を高めることができます。

概要

C：図 2-1 に示す Webex Hybrid Directory サービスのアーキテクチャの概要を使用すると、Webex のカスタマーは、企業の Microsoft Active Directory と組織のアイデンティティストアを Webex に同期させることができます。これにより、Webex のユーザーのオンボーディングとサービスのプロビジョニングがシンプルで一貫性のあるものになります。

C：図 2-1　　Webex Hybrid Directory サービスのアーキテクチャ概要



前提条件

Webex ハイブリッド ディレクトリ サービスを実装して導入する前に、次の要件を実行してください。

- 組織内に Microsoft Active Directory を導入し、ユーザ情報を入力します。
- Cisco Unified Communications Manager（Unified CM）が Microsoft Active Directory と完全に統合されていることを確認します（ディレクトリの同期と認証）。
- オンプレミスのネットワークがファイアウォールで保護されている場合は、ポート 443 で HTTPSを使用したインターネットへのアウトバウンドアクセスが、直接またはHTTPプロキシ経由で利用できることを確認します。

コア コンポーネント

Webex Hybrid Directory サービスのコアコンポーネントは次のとおりです。

- Cisco Directory Connector
- Microsoft Active Directory

推奨される導入

Webex ハイブリッドディレクトリ サービスを Webex ハイブリッドサービス用 PA に展開するには、以下を推奨します。

- Unified CM エンド ユーザ データベースの [エンドユーザアカウントのメール ID（end-user account mail ID）] フィールドに、ユーザの電子メールアドレスが含まれていることを確認します。Webex アプリユーザーは、電子メールアドレスによって Cisco Unified CM エンドユーザーに関連付けられます。LDAP ディレクトリ 統合では、Unified CM エンドユーザーの [メールID（mail ID）] フィールドは通常、同期中に LDAP ディレクトリのメールフィールドからマッピングされます。
- Active Directory ドメイン サービスまたは Active Directory Lightweight Directory Service とは別の Windows サーバに Cisco Directory Connector をインストールします。
- ディレクトリ コネクタのインストールが完了したら、最初の同期を実行します。次に、Microsoft Active Directory 内でリソースおよびユーザ情報が変更（リソースまたはユーザの更新、削除、または追加）されたときに、ディレクトリ コネクタ（および Webex）を更新するように、完全同期および増分同期スケジュールを設定します。

主なメリット

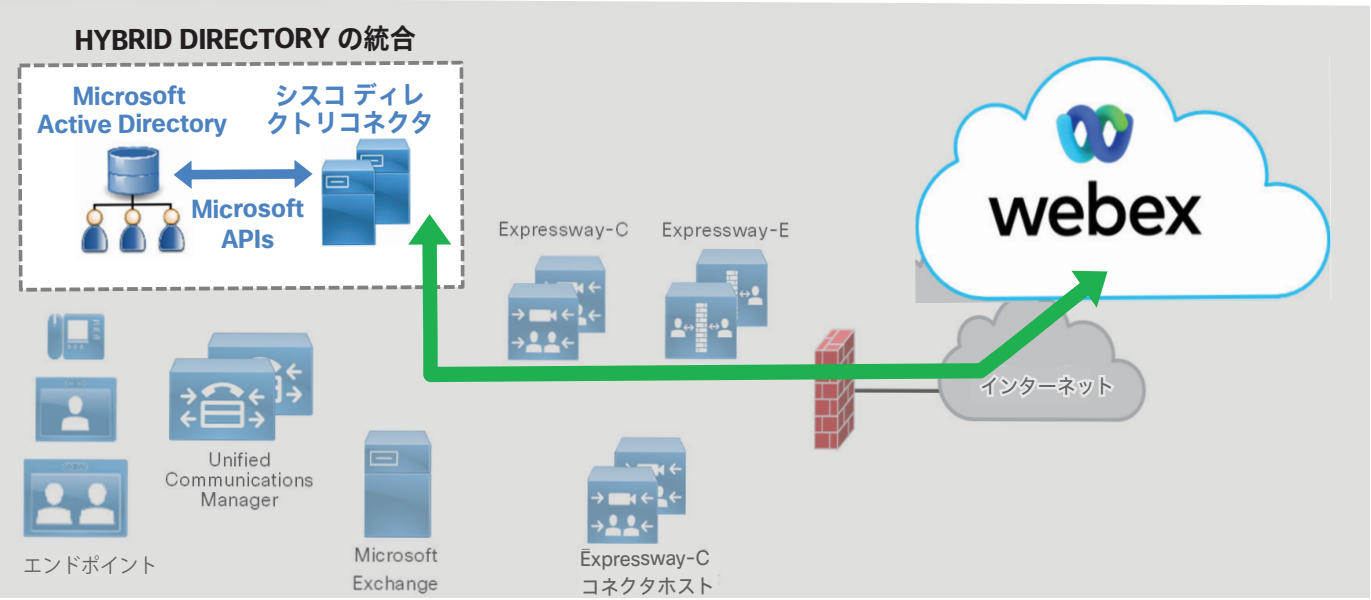
Webex ハイブリッド ディレクトリ サービスには、以下のようなメリットがあります。

- 企業の Microsoft Active Directory からクラウドへの ID、ユーザー、リソース、グループの同期、およびこの企業のディレクトリソースから Webex ユーザーアカウントの作成。
- 企業から Webex への HTTPS アウトバウンド接続は標準ポート 443 で行われます。これは通常、組織で許可されているため、ファイアウォール上のポートを開くための追加の設定は必要ありません。必要に応じて、組織の既存の HTTP プロキシを活用することもできます。
- Cisco Directory Connector を介して企業の Active Directory から Webex に、スケジュール設定された自動同期をユーザとリソースに実行します。
- 増分同期と完全同期により、リソースおよびユーザの ID 情報の管理が容易になります。
- Microsoft Active Directory と Cisco Directory Connector 間のカスタム属性マッピングにより、最大限の柔軟性を実現します。

アーキテクチャ

C：図 2-2は、Webex ハイブリッド ディレクトリ サービスとエンタープライズ ディレクトリの統合を示しています。この統合は、Microsoft Active Directory を使用してセントラルサイトに配置された Cisco Directory Connector に依存しています。Cisco Directory Connector は、冗長性と高可用性を実現するために、2 つの Microsoft Windows サーバに導入されています。

C：図 2-2　　Webex ハイブリッド ディレクトリ サービスとエンタープライズ ディレクトリの統合のためのアーキテクチャ



Cisco Directory Connector は、Microsoft Active Directory アプリケーション プログラミング インターフェイス（API）を使用して、Microsoft Active Directory からユーザ情報を取得します。この API は、Microsoft.Net Framework に基づいています。ディレクトリ コネクタは、HTTPS を使用して、ユーザ情報を組織の Webex ID ストアにプッシュします。

Cisco Directory Connector の役割

Cisco Directory Connector は、企業の Microsoft Active Directory と Webex の組織の ID ストアの間の同期エージェントの役割を果たします。ディレクトリコネクタは、最初に Active Directory からのユーザー情報とリソース情報を Webex に入力し、以降の同期でこの情報を保持して、企業の Active Directory で最新の移動、追加、変更および削除が発生した際に組織の Webex アイデンティティストアを更新します。

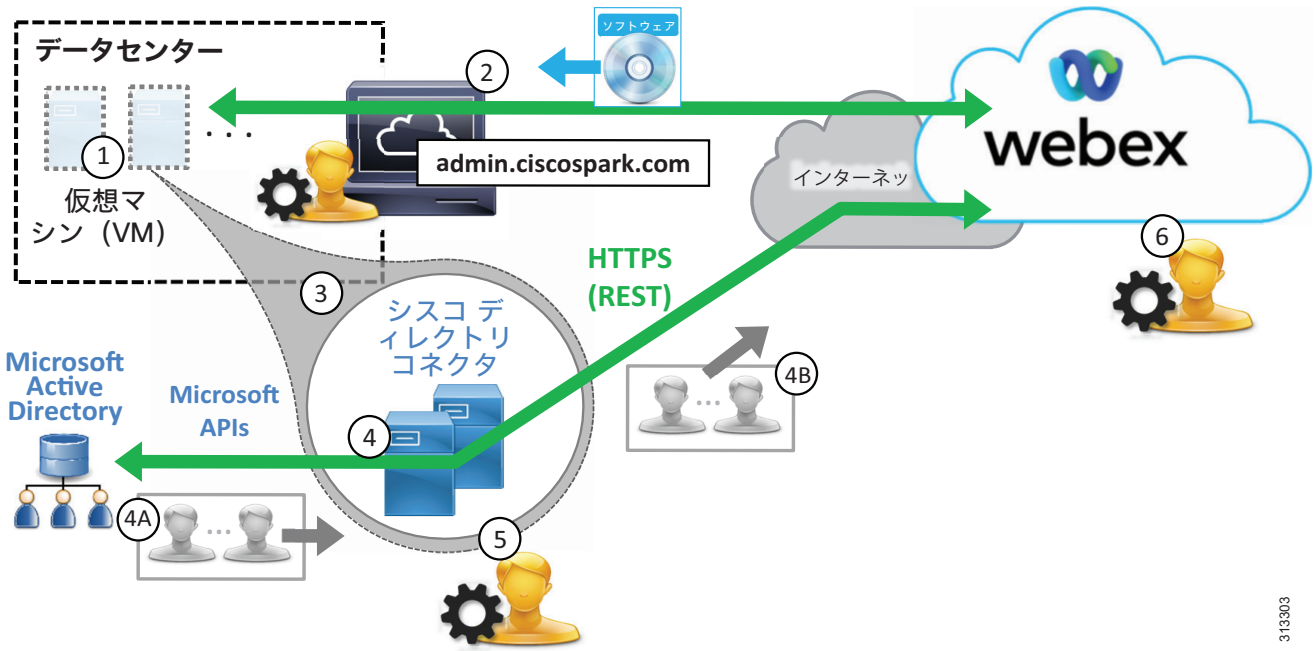
Microsoft Active Directory の役割

Microsoft Active Directory は、エンタープライズ リソースおよびユーザ リポジトリであり、その情報を検証する単一のソースです。ディレクトリ管理者は、移動、追加、変更、および削除を実行してディレクトリ内に含まれるエンタープライズ リソースおよびユーザ情報を管理します。Active Directoryでこの情報を更新すると、同期中に Cisco Directory Connector （次に Webex）に伝達されます。

展開の概要

C：図 2-3 は、Webex ハイブリッド ディレクトリ サービスを導入するために必要な手順を示しています。仮想 Microsoft Windows サーバを作成し、エンタープライズ データセンターに展開します（手順 1）。Windows サーバーの展開後、管理者は、https://admin.webex.com で Webex Control Hub にログインし、ディレクトリの同期を有効にして、Cisco Directory Connector ソフトウェア インストール パッケージをダウンロードします（手順 2）。次に、ディレクトリ コネクタを Windows サーバにインストールします（手順 3）。ディレクトリ コネクタがインストールされると、管理者はコネクタを設定し（手順 4）、Microsoft Active Directory とディレクトリコネクタの間（手順4A）、およびディレクトリコネクタとWebexの間（手順4B）で最初の同期を実行します。

C：図 2-3　　Webex ハイブリッド ディレクトリ サービスの導入の概要

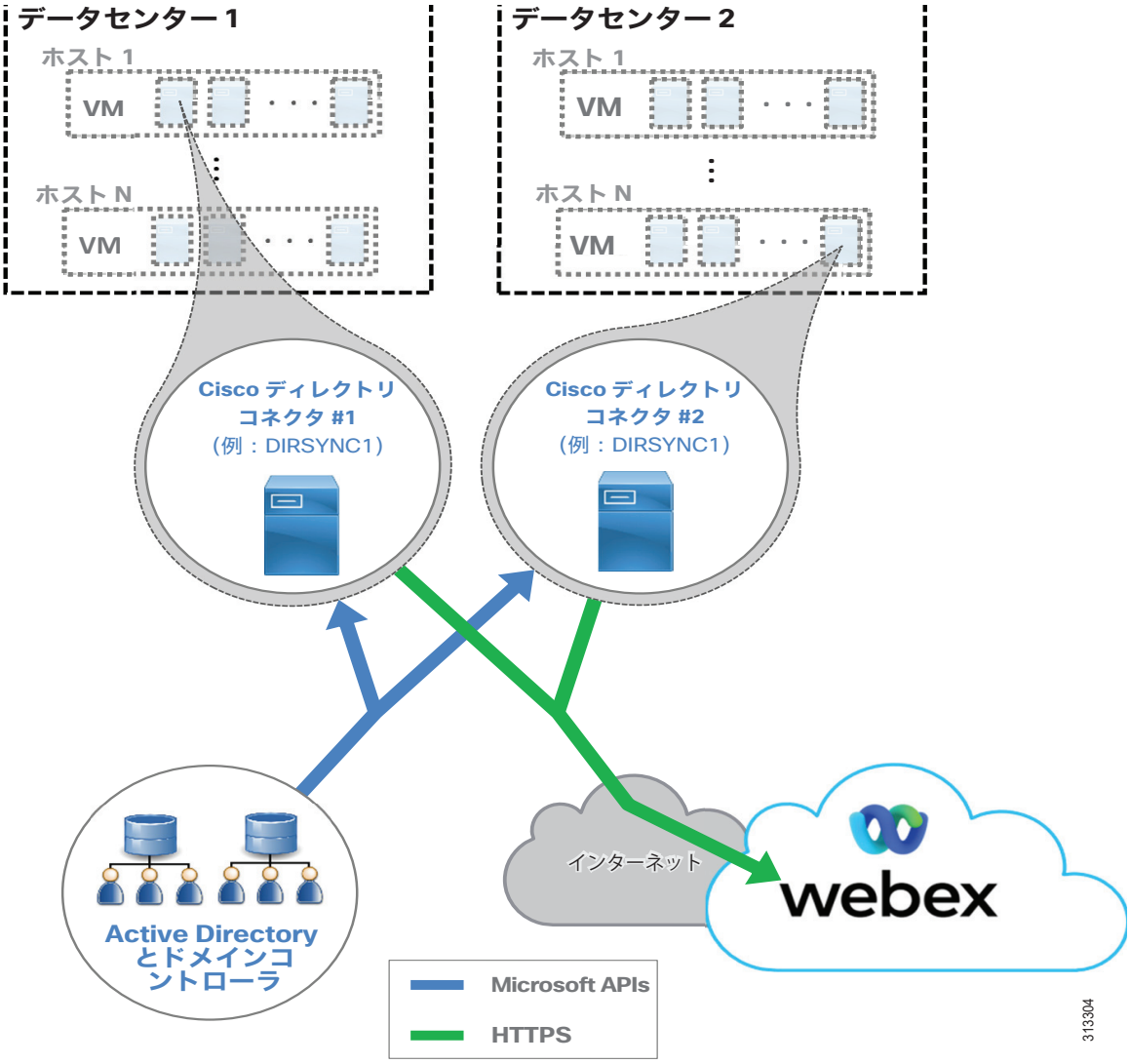


最初の同期が完了すると、管理者は定期的な増分同期と完全同期のスケジュールを設定します（手順5）。その後、管理者はユーザを管理し、必要に応じてクラウドサービスへのプロビジョニングを行います（手順 6）。

高可用性

C：図 2-4 に示すように、2 つの Cisco Directory Connector が導入されています。これらの Windows サーバ仮想マシンは、高可用性と冗長性を実現するために、別の建物またはデータセンターの別のホストに導入されます。ディレクトリ コネクタはペアで導入され、どちらもエンタープライズ ディレクトリとクラウドの間でディレクトリ情報を同期できます。ただし、通常の運用では、1 つのディレクトリ コネクタ（プライマリ）がディレクトリ同期を処理し、もう 1 つのディレクトリコネクタ（バックアップ）はWebexへの接続を維持しますが、同期は実行しません。プライマリ ディレクトリ コネクタに障害が発生した場合、バックアップ ディレクトリ コネクタは、設定されたフェールオーバー間隔に基づいて同期操作の処理を続行します。

C：図 2-4　　Webex ハイブリッド ディレクトリ サービスの高可用性



（注）　単一の Cisco Directory Connector のみが導入されている場合（非冗長導入)、ディレクトリ コネクタに障害が発生すると、Active Directory と Webex ID ストアの間でユーザ情報が同期されなくなります。管理者は、ディレクトリ コネクタが停止している間は、既存のユーザを管理し、それらのユーザをサービスにプロビジョニングできますが、ディレクトリ コネクタがサービスに戻されるまで、ユーザまたはリソースを Webex ID ストアに追加したり削除したりすることはできません。

Cisco Directory Connector の高可用性に関する考慮事項に加えて、Active Directory サービス、Webexへの接続性（HTTPS）、クラウドサービスの可用性など、統合の他の側面に冗長性を提供することも検討してください。

Microsoft コンポーネント（Active Directory、ドメインコントローラ、およびその他の Microsoft エンタープライズ ネットワーク サービス）は、冗長構成で導入する必要があります。高可用性の詳細については、Microsoft の製品マニュアルを参照してください。

また、企業から Webex サービスにアクセスするには、インターネットへの高可用性ネットワーク接続も必要です。できれば、異なるプロバイダからの冗長性のある物理的なインターネット接続を推奨します。

Webex サービスは、これらのサービスとコンポーネントが、柔軟性の高いコンピューティングプラットフォーム上の複数の物理データセンターに導入されているため、可用性が高くなっています。

拡張性

Webex ハイブリッド ディレクトリ サービスのサイジングと拡張性に関する主な考慮事項は、同期のサイズです。リソースとユーザ数については、エンタープライズ ディレクトリと検索ベースが大きいほど、同期が完了するまでに時間がかかります。このため、最初に同期操作を監視して、次の同期期間の開始前に増分同期と完全同期の両方が完了していることを確認することが重要です。専用の Windows サーバ ホストでディレクトリ コネクタを実行することを推奨します。Windows サーバーの負荷が増えると、パフォーマンスが低下し、システム全体の応答と同期時間が長くなる可能性があります。

Webex ハイブリッド ディレクトリ サービスのスケーリングの詳細については、「Cisco Webex Hybrid サービスのサイジング」の章を参照してください。

Webex Hybrid Directory サービス展開プロセス

Webex ハイブリッド ディレクトリ サービスでは、Cisco Directory Connector の導入と、オンプレミス ディレクトリと組織の Webex ID ストア間の同期が必要です。

ディレクトリ同期により、企業のユーザとリソースを Webex にインポートすることができます。ディレクトリの同期は、Webex Control Hub と Cisco Directory Connector を使用すると簡単に実行できます。Cisco Directory Connector を使用すると、自動的に企業のディレクトリ情報を Webex に同期できます。Cisco Directory Connector を使用しない場合、**.csv** ファイルを使用して手動でユーザーとリソースをインポートする必要があります。

(注) このセクションでは、Webex ハイブリッド ディレクトリ サービスの導入に関する概要を説明します。このガイダンスは、https://www.cisco.com/c/en/us/support/unified-communications/spark/products-installation-guides-list.html で入手可能な最新バージョンの『*Cisco Directory Connector 導入ガイド*』に記載されている詳細な手順と合わせて使用してください。

Webex ハイブリッド ディレクトリ サービスの導入は、Windows Server のインストールから始まり、その後 Cisco Directory Connector のダウンロード、インストール、および初期設定が行われます。Webex Hybrid Directory サービスを展開するには、以下のタスクを記載されている順序で実行してください。

1. Microsoft Windows サーバのホストを Cisco Directory Connector 用に導入します。
2. ディレクトリ同期を有効にし、Control Hub から Cisco Directory Connector ソフトウェアをダウンロードします。
3. Windows サーバ ホストに Cisco Directory Connector をインストールします。
4. ディレクトリ コネクタを設定し、最初の同期を完了します。
5. 定期的な増分同期と完全同期のスケジュールを設定します。
6. インポートされたユーザを管理し、Webex サービス用にプロビジョニングします。

1. Microsoft Windows サーバのホストを Cisco Directory Connector 用に導入します。

Cisco Directory Connector は、企業のネットワークに導入されている信頼された Microsoft Windows ドメイン サーバ上で動作します。サーバが Active Directory ドメインに参加し、Cisco Directory Connector サーバーをオンプレミスのドメインで認証するためには、管理者の読み取り専用アカウントが必要です。

新しい Microsoft Windows サーバを導入し、企業の Microsoft Active Directory ドメインに参加します。Webex Hybrid Directory サービスの可用性の高い展開を確実にするには、別のホストにある 2 番目のドメインの Microsoft Windows サーバーをインストールします。

Webex ハイブリッド ディレクトリ サービスでサポートされている特定の Microsoft Windows サーバおよび Microsoft Active Directory のバージョンの詳細については、以下で入手可能な『*Cisco Directory Connector 導入ガイド*』の最新バージョンを参照してください。

https://www.cisco.com/c/en/us/support/unified-communications/spark/products-installation-guides-list.html

（注） Microsoft Windowsサーバーは、企業の標準とポリシーに従って展開し設定する必要があり、ウイルスおよびマルウェアからの保護、デバイス管理、およびセキュリティに関する要件に準拠しなければなりません。

2. ディレクトリ同期を有効にし、Control Hub から Cisco Directory Connector ソフトウェアをダウンロードします。

手順 1 で展開した Windows サーバーホスト上の Web ブラウザから、https://admin.webex.com にある Control Hub にログインします。Webex 組織の管理者ログイン情報を使用します。

Control Hub で、**[ユーザー（Users）]** > **[ユーザーの管理（Manage users）]** の順に選択し、ディレクトリ同期を有効にします。次に、**[ディレクトリ同期の有効化（Enable Directory Synchronization）]** をクリックして **[次へ（Next）]** を選択して続行します。**[ダウンロードとインストール（Download and Install）]** リンクをクリックし、例えば DirectoryConnector.zip などの Cisco Directory Connector インストレーション **.zip** ファイルをローカルサーバーに保存します。

3. Windows サーバ ホストに Cisco Directory Connector をインストールします。

手順 2 でホストサーバーに保存した **.zip** ファイルを見つけます。ファイルを解凍してセットアップフォルダに移動し、セットアップフォルダで **.msi** ファイル（例：CiscoDirectoryConnector.msi）を実行して、Cisco Directory Connector のセットアップウィザードを起動します。

ライセンス契約書を承認するには、**[使用許諾契約書の条項に同意します（I accept the terms in the License Agreement）]** を選択し、**[次へ（Next）]** をクリックします。[Next] をクリックしてデフォルトのインストール場所を指定します。

サービス アカウントの **[ドメインアカウント（Domain Account）]** オプションを選択し、ドメイン アカウントのユーザ名とパスワードを入力します。**[ユーザ名（Username）]** フィールドに、Active Directory ドメインとユーザ名を <*domain*>\<*user_name*> の形式で入力します（例：ENT-PA\administrator）。**[次へ（Next）]** をクリックして、ドメイン アカウント情報を保存します。

[インストール（Install）] をクリックして、Cisco Directory Connector のインストールを開始します。

インストールが完了したら、2 番目の Windows サーバーホスト上でこの手順を繰り返して、冗長ディレクトリコネクタをインストールします。

4. ディレクトリ コネクタを設定し、最初の同期を完了します。

Cisco Directory Connector を起動し、その組織の管理者アカウントの電子メールアドレスおよびパスワードを使用して Webex 組織にサインインします。この電子メールアドレスおよびパスワードは、Control Hub 管理ポータルにログインする際に使用する電子メールアドレスおよびパスワードと同じものです。クリックし、Webex 組織とドメインを確認します。

次に、ディレクトリ コネクタの初期設定を実行します。ディレクトリ コネクタのダッシュボードで、**[構成（Configuration）]** タブをクリックします。

（注） [構成（Configuration）] タブまたはフィールド値が指定されていない場合は、デフォルト設定と値が使用されます。

[構成（Configuration）] 画面のタブに移動し、C：表 2-1 で示すとおり設定します。

C：表 2-1　　Cisco Directory Connector の設定

[構成] タブ	設定	説明と値
General	Connector Name	ディレクトリ コネクタの名前を入力します（例：DIRSYNC1）。これは、ダッシュボードと ControlHubの Web ポータルに表示される名前です。
	優先ドメインコントローラ	ドロップダウン メニューを使用して、1 つ以上のドメインコントローラを追加します。ネットワーク上のドメインコントローラを選択し、**[追加（Add）]** ボタンをクリックします。少なくとも 2 つのドメインコントローラを追加して、ネットワーク上でディレクトリ サービスの高可用性を確保します。
オブジェクトの選択 同期中、ユーザ情報（選択されたコンテナと構成済み LDAP フィルタに基づく）は、HTTPS 接続を介してディレクトリ コネクタから Webex にプッシュされます。これは企業の側から見ればアウトバウンド接続であるため、内部または外部のファイアウォールでインバウンド ポートを開く必要はありません。	Object Type	**[ユーザ（Users）]** ボックスがオンになっています。
	LDAP フィルタ	検索可能なコンテナの数を制限するために、必要な LDAP フィルタを標準 LDAP 形式で入力します。ディレクトリ コネクタは、社内の Microsoft Active Directory からユーザ情報を取得します。ユーザ情報は、ドメイン全体、または特定のコンテナや組織単位から取得することもできます。さらに精度を上げたい場合は、複数の LDAP フィルタを作成します。
	オンプレミスの基本 DN の同期	ウィンドウから 1 つ以上の DN を選択し（例：CN＝Users、DC = ent-pa、DC = com）、**[選択（Select）]** クリックして、ディレクトリ同期化アグリーメントに含める適切な同期化コンテナと同期化オブジェクト（例：ユーザ）を選択します。Webex ハイブリッド ディレクトリ サービスと Microsoft Active Directory の統合では、単一および複数のフォレストと、単一または複数のドメインを使用する導入がサポートされています。
ユーザ属性マッピング Cisco Directory Connector は、多数の Microsoft Active Directory の属性を Webex（顧客組織の ID ストア）と同期します。	Active Directory 属性名	[Active Directory属性（Active Directory attribute）] ドロップダウンリストからオプションを選択して、必要な Active Directory から Webex 属性名へのマッピングを設定します。少なくとも、Active Directory 属性名 **mail** が、必要な Webex 属性名 **uid** にマッピングされていることを確認してください。**mail** 属性は、ユーザを一意に識別するため、Webexでは重要な役割を果たします。ルーム システムを Webex デバイスとして登録する場合は、Active Directory 属性（例：ipPhone）を Webex 属性名 **sipAddresses;type-enterprise**にマッピングする必要もあります。マッピングする Active Directory 属性に一意の完全な SIP URI（例：sip:conf_room01@ent-pa.com または sip:12345@ent-pa.com など）を入力して、Webex ディレクトリに各デバイスのエンタープライズ ダイヤル可能な SIP URI が含まれていることを確認します。その他の一般的に同期される Active Directory 属性名には、displayName、givenName、および telephoneNumber などがあります。

[適用（Apply）] をクリックし、設定を保存して適用します。

上記のようにディレクトリ コネクタをインストールして設定したら、最初の完全同期を実行して、企業の Microsoft Active Directory からディレクトリ情報を取得し、組織の Webex ID ストアにプッシュします。

冗長 Cisco Directory Connector で、C：表 2-1 で記載されているものと同じ設定を構成しますが、コネクタ名の設定には、DIRSYNC2 など一意の名前を使用します。

5. 定期的な増分同期と完全同期のスケジュールを設定します。

最初の同期化の後は、企業の Active Directory で発生した移動、追加、および変更に応じて、組織の Webex ID ストアを更新しておくことが重要です。

エンタープライズディレクトリの変更を Webex で最新の状態に保つには、ディレクトリ コネクタの 1 つで定期的な増分同期と完全同期を設定します。[ディレクトリコネクタ設定（Directory Connector Configuration）)] タブに戻り、**[スケジュール（Schedule）]** を選択します。次に、C：表 2-2 のように同期設定を行います。

C：表 2-2　　Cisco Directory Connector のスケジュール設定

[構成] タブ	設定	説明と値
スケジュール（Schedule）	増分同期間隔	増分同期の間隔を分単位で設定します（たとえば、デフォルトは 10 分）。
	完全な同期のスケジュールの有効化	このオプションを選択します。
	スケジュール（Schedule）	定期的な完全同期を実行する時刻と曜日を選択します（たとえば、日曜日（S）の午前 7 時 30 分）。
	フェールオーバーの間隔	セカンダリ ディレクトリ コネクタがプライマリになり、増分同期と完全同期を引き継ぐまでの時間を分単位で設定します（たとえば、デフォルトは 60 分）。 この設定は、複数のディレクトリ コネクタがある高可用性導入に適用されます。

C：表 2-2 の設定は共有され、導入内の両方のディレクトリ コネクタに適用されます。

6. インポートされたユーザを管理し、Webex サービス用にプロビジョニングします。

エンタープライズ ディレクトリのユーザー情報が Webex に共有されたら、管理者は、Control Hub を使用してクラウドサービスにユーザーをプロビジョニングし、それらのサービス機能と設定を管理できます。

Webex 組織の管理者ログイン情報を使用して、Web ブラウザの https://admin.webex.com から Control Hub にログインします。

Control Hub で、**[ユーザー（Users）]** > **[ユーザーの管理（Manage User）]** の順に選択し、ユーザーサービスの管理とプロビジョニングを開始します。ディレクトリ同期を有効にすると、複数の方法でユーザーとユーザーが使用するサービスを変更することができます。ユーザは、個別に変更することも、一括で変更することもできます。

大量のユーザを一括で変更するには、**[CSVファイルによるユーザのエクスポートと変更（Export and modify users with a CSV file）]** または **[すべての同期ユーザを変更（Modify all synchronized users）]** のいずれかを選択します。CSV ファイル方式は、ユーザのグループを一括で変更する場合に適しています（一度に最大1100ユーザ）。一括で変更するためのCSVファイルの準備は手動の処理です。

すべてのユーザに対して機能またはサービスを有効にするには、**[すべての同期ユーザを変更（Modify all synchronized users）]** をクリックし、**[次へ（Next）]** をクリックします。確認メッセージが表示されたら、**[次へ（Next）]** をクリックして、ユーザに自動的に電子メールが送信されることを確認します。次の画面で、システムが最新の同期承諾のユーザーリストを同期するのを待ってから、**[次へ（Next）]** をクリックします。

次の画面で、メッセージ、会議、およびハイブリッドサービスを含むその他のサービスのユーザをプロビジョニングします。サービスを選択したら、**[次へ（Next）]** をクリックして、ユーザーアカウントの更新を開始します。更新が完了すると、ユーザは追加されたサービスとの機能の使用を開始できます。

（注） ライセンスされたサービスと機能を追加して有効にするには、有効なライセンスが必要です