

環境の準備 ディレクトリ コネクタ

- ・ディレクトリコネクタの要件(1ページ)
- ・サイジング情報 (6ページ)
- Windows Registry で SafeDllSearchMode を確認 $(6 \sim ジ)$
- Web プロキシの統合 (7 ページ)

ディレクトリ コネクタ の要件

Windows と Active Directory の要件

次のサポートディレクトリ コネクタされている Windows サーバにインストールできます。

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2003



(注) Cookie の問題を解決するには、ドメインコントローラを修正を含むリリース (Windows Server 2012 R2または2016) にアップグレードすることをお勧めします。

ディレクトリコネクタは、次の Active Directory サービスでサポートされています。

• Active Directory 2016

(ディレクトリコネクタ Windows Server 2019 で最新バージョンの Active Directory を使用している場合にサポートされます)

• Active Directory 2012

- Active Directory 2008 R2
- Active Directory 2008

次の追加要件に注意してください。

- ・ディレクトリコネクタTLS1.2 が必要。次のものをインストールする必要があります。
 - .NET Framework v3.5 (ディレクトリコネクタアプリケーションに必要)。何らかの問題が発生した場合は、「Enable .Net Framework 3.5」の指示に従って、[Add Roles And Features] ウィザードを使用します)。
 - ・.NET Framework v4.5 (TLS 1.2 に必要)
- Active Directory フォレストの機能レベル2 (Windows Server 2003) 以降が必要です。(詳細については、「Active Directory 機能レベルについて」を参照してください)。

ハードウェア要件

次の最小ディレクトリコネクタハードウェア要件を満たしているコンピュータにインストール する必要があります。

- $\bullet 8 \text{ GB} \oslash \text{RAM}$
- 50 GB のストレージ
- CPUの最小値なし

ネットワーク要件

ネットワークがファイアウォールの背後にある場合は、システムにインターネットへのHTTPS (ポート 443) アクセスがあることを確認します。

Webex組織要件

- ディレクトリコネクタ Control Hub からソフトウェアにWebexアクセスするには、トライアルまたは有料のサブスクリプションを含む組織が必要です。
- (オプション)初めてサインインする前に新しいWebexアプリユーザアカウントをアクティブにする場合は、次の操作を行うことを推奨します。
 - クラウドに同期するユーザのメールアドレスを含むドメインを追加、確認、任意で要求します。
 - ・お使いの Webex 組織と Identity Provider (idP) のシングルサインオン (SSO) 統合を実行 します。

 ・自動電子メール招待を抑制し、新しいユーザが自動電子メール招待を受信しないようにします。また、独自の電子メールキャンペーンを実行することもできます。(この機能を利用するには SSO 統合が必要です。

<u>
(注)</u>
(注)
詳編

詳細については、「Control Hubでのユーザーステータスとアクション」を参照してください。

インストール要件

- 複数ドメイン環境(単一フォレストまたは複数のフォレスト)の場合は、各Active Directory ドメインに対して1つのディレクトリコネクタをインストールする必要があります。別の既存のドメイン(A)で同期されたユーザデータを維持しながら新しいドメイン(B)を同期する場合は、ドメイン(B)の同期用のDirectory Connector をインストールするために、 別途サポートされている Windows サーバがあることを確認します。
- コネクタにサインインするには、Active Directory内の管理者アカウントは必要ありません。Control Hubの完全な管理者アカウントと同じユーザーであるローカルユーザーアカウントが必要です。

≥s							
ion View	Help						
es (Local)	Ö Samisas (Lasal)						
	Services (Local)	Name	Description	Status	Startun Tuno	Les On As	
	Cisco DirSync Service	Active Directory Certificate Servi	Creater m	Started	Automatic	Log On AS	
	Stop the service	Active Directory Certificate Services	AD DC Dom	Started	Automatic	Local System	
	Restart the service	Active Directory Web Services	AD D3 Dom	Started	Automatic	Local System	
		Application Experience	Processors	Started	Magual	Local System	
	Description: Cisco DirSync Connector Service	Application Experience	Provides a	Started	Automatic	Local System	
		Application Identity	Determiner	Junco	Manual	Local Service	
		Application Information	Facilitates	Started	Manual	Local System	
	1	Application Laver Cateway Service	Provides s	D tur teu	Manual	Local Service	
		Application Management	Processes i	Started	Manual	Local System	
		ASP NET State Service	Provides s	o con coo	Disabled	Network S	
		Background Intelligent Transfer	Transfers f	Started	Manual	Local System	
		Base Eiltering Engine	The Base F	Started	Automatic	Local Service	
	1	Certificate Propagation	Copies use	Started	Manual	Local System	
	1	Cisco DirSync Service	Cisco DirSv	Started	Automatic	Local System	Girco Dirfume Forgico Proportion (Local Computer)
	1	Cisco DirSync Service 4.0	Cisco DirSy	Started	Automatic	\administ	Cisco Dirsync Service Propercies (Local Computer)
	1	CNG Key Isolation	The CNG k	Started	Manual	Local System	General Log On Recovery Dependencies
	1	COM+ Event System	Supports S	Started	Automatic	Local Service	
	1	COM+ System Application	Manages t	Started	Manual	Local System	Log on as:
	1	Computer Browser	Maintains a	D tai tea	Disabled	Local System	I local System account
	1	Credential Manager	Provides s		Manual	Local System	Allow service to interact with desktop
	1	Cryptographic Services	Provides fo	Started	Automatic	Network S	
	1	OCOM Server Process Launcher	The DCOM	Started	Automatic	Local System	C This account: Browse
	1	Desktop Window Manager Sessio	Provides D	Started	Automatic	Local System	
		OFS Namespace	Enables vo	Started	Automatic	Local System	Password:
		O DFS Replication	Enables vo	Started	Automatic	Local System	
		O DHCP Client	Registers a	Started	Automatic	Local Service	Contim password:
	1	Diagnostic Policy Service	The Diagno	Started	Automatic (D	Local Service	Help me configure user account log on options
	1	Diagnostic Service Host	The Diagno		Manual	Local Service	
	1	Diagnostic System Host	The Diagno		Manual	Local System	
	1	Diagnostics Tracking Service	The Diagno	Started	Automatic	Local System	
	1	O Disk Defragmenter	Provides Di		Manual	Local System	
	1	O Distributed Link Tracking Client	Maintains li		Manual	Local System	
	1	Distributed Transaction Coordinator	Coordinate	Started	Automatic (D	Network S	
	1	O DNS Client	The DNS Cl	Started	Automatic	Network S	
	1	ONS Server	Enables DN	Started	Automatic	Local System	
	1	Encrypting File System (EFS)	Provides th		Manual	Local System	
	1	Extensible Authentication Protocol	The Extens		Manual	Local System	
	1	Ele Replication Service	Synchroniz	Started	Automatic	Local System	
	1	Eunction Discovery Provider Host	The FDPH		Manual	Local Service	OK Crossel
	1	Eunction Discovery Resource Pu	Publishes t		Manual	Local Service	OK Caricer A
	1	Google Chrome Elevation Service			Manual	Local System	
		Canda Lindata Comisa (gundata)	Keepe ways		Automatic (D	Local System	

このローカルユーザは、ドメインコントローラに接続して Active Directory ユーザオブジェ クトを読み取るために、その Windows マシンに対する権限を持っている必要があります。 マシンのログインアカウントは、ローカルマシンにソフトウェアをインストールする権限 を持つコンピュータ管理者である必要があります。(この情報は、仮想マシンのログイン にも適用されます)。



- コネクターにサインインしている間は、サインインアカウントは、Control Hubの完全な管理者アカウントと同じである必要があります。デフォルトでは、コネクタはローカルシステムアカウントを使用して Active Directory にアクセスします。ただし、Windows サービスを使用して、Active Directory にアクセスする別のアカウントを設定できます。(この情報は、仮想マシンのログインにも適用されます)。
- 次の手順を使用して、Windows Safe dynamic link library (DLL)の検索モードがWindows Registry で SafeDIISearchMode を確認 (6ページ) 有効になっていることを確認してくだ さい。
- 1つのフォレストで複数のドメインに AD LDS を使用する場合は、別ディレクトリ コネク タのマシンに Active Directory ドメインサービス/Active Directory ライトウェイトディレク トリサービス (ad DS/ad lds) をインストールすることをお勧めします。

複数ドメインの要件

のCisco directory connector 導入タスクのフロータスクを実行する前に、Active Directory の情報 を複数のドメインからクラウドに同期する場合は、次の要件と推奨事項に留意してください。

ドメインごとに個別ディレクトリコネクタのインスタンスが必要です。

- 同期ディレクトリコネクタする同じドメインにあるホスト上で、ソフトウェアが実行されている必要があります。
- でControl Hubドメインを確認または要求することをお勧めします。(「ドメインの追加、 確認および要求」を参照してください。)
- 50を超えるドメインを同期する場合は、組織を大規模な組織リストに移動させるためにチケットを開く必要があります。
- ・必要に応じて、ユーザアカウントとともにルームリソース情報を同期できます。(オンプレミスのルーム情報をWebex クラウドに同期を参照)。

自動ライセンス割り当てのための Active Directory グループの推奨事項

Active Directory グループは、ユーザアカウント、コンピュータアカウント、およびその他のグ ループを管理可能な単位に収集するために使用されます。個々のユーザではなくグループを使 用することで、ネットワークのメンテナンスと管理を簡素化することができます。

Active Directory には、次の2つのタイプのグループがあります。

- ・配布グループ:電子メール同報リストを作成するために使用されます。
- ・セキュリティグループ:共有リソースに権限を割り当てるために使用されます。

Create in: cisco	-interop.org/Webex
roup name:	
Webex Group Name	
roup name (pre-Windows 20	000):
Webex Group Name	
Group scope	Group type
O Domain local	 Security
 Global 	O Distribution
O Universal	

Active Directory でグループを作成する際には、次のガイドラインを考慮してください。

 各ロール、部門、またはサービス(販売、マーケティング、マネージャ、経理、Webex ラ イセンシングなど)のグローバルグループを作成します。

- ・組織全体で標準の命名規則を使用して、グループに関する重要な情報を簡単に識別できる ようにします。グループ名には、アクセスのレベル、リソースのタイプ、セキュリティレ ベル、グループスコープ、メール機能など、グループに関する詳細を含めることができま す。たとえば、グループ名「GSG_Webex_Licensing_EMEAR」は、Webex ライセンス EMEAR ユーザのグローバルセキュリティグループを指します。
- ・地域や経営上の階層など、わかりやすい方法でグループを整理します。グループの説明を 使用して、グループの目的を完全に説明します。
- 新しくプロビジョニングされたグループにユーザーを追加する前に、それらのグループの Control Hub で Auto License Group テンプレートを定義します。詳細については、「自動ラ イセンス割り当てテンプレートのセットアップ」を参照してください。

サイジング情報

ディレクトリコネクタは、オンプレミスの Active Directory と Webex クラウド間のブリッジと して機能します。そのため、コネクタにはクラウドと同期できる Active Directory オブジェクト の数の上限はありません。オンプレミスディレクトリオブジェクトの制限は、コネクタ自体で はなく、クラウドに同期されている Active Directory 環境の特定のバージョンおよび仕様に関連 付けられています。

同期の速度に影響する要因はいくつかあります。

- Active Directory オブジェクトの合計数。(5000 ユーザ同期ジョブには、5万の長さはかかりません)。
- ネットワークの速度と帯域幅。
- ・システムの負荷と仕様。

$\sim \rho$

ヒント 5万人以上のユーザを同期する場合は、フェイルオーバーと冗長性のため、2つ目のコネクタ を使用することを強く推奨します。

(注)

同期にはいくつかの要因が含まれているため、各導入は上記の要因によって異なるため、オブ ジェクトの同期にかかる時間の長さについて特定の時間値を指定することはできません。

Windows Registry で SafeDIISearchMode を確認

Safe dynamic link library (DLL)の検索モードは、Windows レジストリでデフォルトで設定され、 ユーザの現在のディレクトリを DLL の検索順序の後に配置します。このモードが何らかの理 由で無効になっている場合、攻撃者は悪意のある DLL (システムフォルダにある参照された DLL ファイルと同じ名前)をアプリケーションの現在の作業ディレクトリに配置する可能性が あります。

通常、Saf Edllsearchmode は有効になっていますが、レジストリ設定をダブルチェックするに は、次の手順を使用します。

始める前に

//\		•	<u>۱</u>	
	_ /	!	\mathbf{X}	

注意 Windows レジストリの変更は、細心の注意を払って実行する必要があります。これらの手順を 使用する前に、レジストリのバックアップを作成しておくことを推奨します。

手順

- ステップ1 Windows の検索または Run ウィンドウで、 regedit と入力し、enter キーを押します。
- ステップ2 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager に移動します。
- ステップ3 次のいずれかを選択します。
 - Saf Edllsearchmode が表示されない: それ以上のアクションは必要ありません。
 - Saf Edllsearchmode がリストされている: 値が1に設定されていることを確認します。

詳細については、「ダイナミックリンクライブラリの検索順序」を参照してください。

Web プロキシの統合

Web プロキシの統合

ご使用の環境で web プロキシ認証が有効になっているディレクトリ コネクタ場合でも、を使用できます。

組織で透過型Webプロキシが使用されている場合、認証はサポートされません。コネクタは、 正常に接続してユーザを同期します。

次のいずれかの方法を実行できます。

- Internet Explorer による明示的な Web プロキシ(コネクタは、Web プロキシの設定を継承 する)
- •.pacファイルによる明示的なWebプロキシ(コネクタは、企業固有のプロキシ設定を継承 する)
- コネクタと連携する透過型プロキシ(変更なし)

ブラウザを介した Web プロキシの使用

Internet Explorer を介してディレクトリコネクタ web プロキシを使用するように設定できます。

Cisco DirSync サービスが現在サインインしているユーザとは異なるアカウントから実行されて いる場合は、このアカウントでサインインして web プロキシを設定する必要もあります。

手順

- ステップ1 Internet Explorer から、[Internet Options] に移動し、[Connections] をクリックして、[LAN Settings] を選択します。
- ステップ2 Web プロキシでコネクタがインストールされている Windows インスタンスを指定します。コ ネクタは、次の Web プロキシの設定を継承します。
- ステップ3 プロキシ認証が使用されている環境では、次の URL を許可リストに追加します。
 - 同期のためのcloudconnector.webex.com。
 - idbroker.webex.com (認証用)
 - idbroker-static.webex.com は、フォント、js コンポーネントなどの静的リソースを提供します。

この作業は、サイト全体(すべてのホスト)で実行することも、コネクタがあるホストでのみ 実行することもできます。

- (注) Web プロキシを完全にバイパスするという目的で、これらの URL を許可リストに 追加する場合は、コネクタのホストが URL に直接アクセスすることを許可するように、ファイアウォール ACL テーブルが更新されていることを確認してください。
- ステップ4 環境で認証局から証明書失効リストを要求する必要がある場合は、次の URL を許可リストに 追加します。
 - *.quovadisglobal.com
 - *.digicert.com
 - *.godaddy.com
 - *.identrust.com
 - *.lencr.org

詳細については、Webex サービスにアクセスする必要があるドメインと URL に関するこの記 事を参照してください。https://help.webex.com/WBX000028782/ Network-Requirements-for-Webex-Services#id 135010

PAC ファイルを使用した Web プロキシの設定

.Pac ファイルを使用するようにクライアントブラウザを設定できます。このファイルは、web プロキシのアドレスとポート情報を提供します。ディレクトリコネクタエンタープライズ固有 のwebプロキシ設定を直接継承します。

手順

- ステップ1 コネクタが正常に接続して、Webex クラウドとユーザ情報を同期するには、コネクタがインス トールされているホストの.pac ファイル設定で、cloudconnector.webex.comのプロキシ認証が 無効になっていることを確認します。
- ステップ2 プロキシ認証が使用されている環境では、次のURLを許可リストに追加します。
 - •同期のためのcloudconnector.webex.com。
 - idbroker.webex.com (認証用)
 - idbroker-static.webex.com は、フォント、js コンポーネントなどの静的リソースを提供します。

この作業は、サイト全体(すべてのホスト)で実行することも、コネクタがあるホストでのみ 実行することもできます。

- (注) Web プロキシを完全にバイパスするという目的で、これらの URL を許可リストに 追加する場合は、コネクタのホストが URL に直接アクセスすることを許可するように、ファイアウォール ACL テーブルが更新されていることを確認してください。
- **ステップ3** 環境で認証局から証明書失効リストを要求する必要がある場合は、次の URL を許可リストに 追加します。
 - *.quovadisglobal.com
 - *.digicert.com
 - *.godaddy.com
 - *.identrust.com
 - *.lencr.org

詳細については、Webex サービスにアクセスする必要があるドメインと URL に関するこの記 事を参照してください。https://help.webex.com/WBX000028782/ Network-Requirements-for-Webex-Services#id_135010

NTLM プロキシ

ディレクトリ コネクタNT LAN Manager (NTLM)をサポートしています。NTLM は、ドメイン デバイス間でWindows認証をサポートして、セキュリティを確保するための手段の1つです。

NTLM 設計

ほとんどの場合、ユーザは、クライアント PC を介して別のワークステーションのリソースに アクセスすることを望んでいて、安全な方法で行うことが難しくなります。

一般的に、NTLMの技術的な設計は、「チャレンジ」と「レスポンス」のメカニズムに基づいています。

ユーザは、Windows アカウントとパスワードを使用してクライアント PC にサインインします。パスワードはローカルに保存されません。プレーンテキストのパスワードの代わりに、パスワードのハッシュ値はローカルに保存されます。ユーザがパスワードによってサインインすると、Windows OS は、格納されているハッシュ値と入力されたパスワードのハッシュ値を比較します。両方が同じであれば、認証は成功します。

ユーザが別のサーバのリソースにアクセスする必要がある場合、クライアントは、プレー ンテキストでアカウント名を使用してサーバに要求を送信します。

- サーバが要求を受信すると、サーバは16ビットのランダムキーを生成します。このキー は、チャレンジ(または Nonce)と呼ばれます。サーバがクライアントに戻る前に、チャレ ンジはサーバに保存されます。次に、サーバはプレーンテキストでクライアントにチャレ ンジを送信します。
- クライアントは、サーバから送信されたチャレンジを受信するとすぐに、ステップ1で説明したハッシュ値によってチャレンジを暗号化します。暗号化後に、値がサーバに返送されます。
- 4. サーバがクライアントから暗号化された値を受信すると、サーバはそれを検証のためにドメインコントローラに送信します。要求には、アカウント名、クライアントが送信した暗号化されたチャレンジ、および元のプレーンチャレンジが含まれます。
- 5. ドメインコントローラは、アカウント名に従ってパスワードのハッシュ値を取得できます。次に、ドメインコントローラは元のチャレンジで暗号化できます。その後、ドメインコントローラは、受信したハッシュ値と暗号化されたハッシュ値を比較できます。同じであれば、検証は成功します。

 (注) Windowsでは、セキュリティ認証がオペレーティングシステムに組み込まれているため、アプ リケーションによるセキュリティ認証のサポートが容易になります。そのため、さらに設定を 完了する必要はありません。

透過プロキシの設定

このシナリオでは、ブラウザは、透過的な web プロキシが http 要求 (ポート 80/ポート 443) を 代行受信していて、クライアント側の設定が不要であることを認識していません。

手順

ステップ1 透過プロキシを導入して、コネクタが接続してユーザを同期できるようにします。

ステップ2 コネクタの開始時に期待どおりのブラウザ認証ポップアップウィンドウが表示された場合は、 プロキシが正常であることを確認します。

プロキシ認証の設定

アクセスコントロールリストを作成して、許可リストにURL cloudconnector.webex.com を追加します。

エンタープライズファイアウォールサーバで、次のようにします。

手順

- ステップ1 DNS ルックアップを有効にします(まだ有効になっていない場合)。
- ステップ2 この接続の想定帯域幅を決定します(コネクタで約2mb/s以下)。これは必須ではありません。
- **ステップ3** コネクタホストに適用するアクセス制御リストを作成して、許可リストに追加するターゲット として cloudconnector.webex.com を指定します。

次に例を示します。

access-list 2000 acl-inside extended permit TCP [IP of the connector] cloudconnector.webex.com eq https

- **ステップ4** この ACL を適切なファイアウォール インターフェイスに適用します。これは、この1つのコ ネクタ ホストにのみ適用可能です。
- ステップ5 適切な暗黙の deny ステートメントを設定して、企業内の残りのホストが web プロキシを使用 する必要があることを確認します。

I

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては 、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている 場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容につい ては米国サイトのドキュメントを参照ください。