Cisco Webex Hybrid Data Security 導入ガイド

初版：2017 年 8 月 18 日

最終更新：2020 年 6 月 16 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

新規および変更情報

日付	変更内容
2020 年 6 月 16 日	「ノードの削除 （45 ページ）」が更新され、Control Hub UI の変更が反映されました。
2020 年 6 月 4 日	「HDS ホストの構成 ISO の作成 （21 ページ）」が更新され、ユーザが設定する可能性がある詳細設定の変更が反映されました。
2020 年 5 月29 日	「HDS ホストの構成 ISO の作成 （21 ページ）」が更新され、SQL Server データベースで TLS も使用可能であることが記載されました。また、UI の変更が反映され、その他いくつかの点が明確化されました。
2020 年 5 月 5 日	「仮想ホストの要件 （12 ページ）」が更新され、ESXi 6.5 の新しい要件が記載されました。
2020年4月21日	「外部接続の要件 （14 ページ）」が更新され、新しい南北アメリカ CI ホストについて記載されました。
2020 年 4 月 1 日	「外部接続の要件 （14 ページ）」が更新され、地域 CI ホストに関する情報が記載されました。
2020 年 2 月 20 日	「HDS ホストの構成 ISO の作成 （21 ページ）」が更新され、HDS セットアップ ツールの新しいオプションの [詳細設定（Advanced Settings）] 画面に関する情報が記載されました。
2020 年 2 月 4 日	「プロキシ サーバの要件 （15 ページ）」が更新されました。
2019 年 12 月 16 日	ブロックされた外部 DNS 解決モードが動作するための要件を「プロキシ サーバの要件 （15 ページ）」に明示しました。

新規および変更情報

日付	変更内容
2019 年 11 月 19 日	次のセクションで、ブロックされた外部 DNS 解決モードに関する情報を追加しました。 • プロキシ サポート （8 ページ） • プロキシ統合のための HDS ノードの構成 （29 ページ） • ブロックされた外部 DNS 解決モードをオフにする （44 ページ）
2019 年 11 月 8 日	ノードのネットワーク設定は、後ではなく OVA を導入するときに設定できるようになりました。 それに伴い、次の項を更新しました。 • Hybrid Data Security 導入タスク フロー （19 ページ） • HDS ホスト OVA のインストール （26 ページ） • Hybrid Data Security VM のセットアップ （27 ページ） （注） OVA 導入時にネットワーク設定を設定するためのオプションは、ESXi 6.5 を使用してテストされています。このオプションは、以前のバージョンでは使用できない場合があります。
2019 年 9 月 6 日	データベース サーバの要件 （13 ページ）に SQL Server 標準が追加されました。
2019 年 8 月 29 日	WebSocket トラフィックを無視して適切に動作するように Squid プロキシを構成する方法に関するガイドラインを記載した付録 Hybrid Data Security の Squid プロキシの構成 （59 ページ） を追加しました。
2019 年 8 月 20 日	Webex クラウドとの Hybrid Data Security ノード通信に対するプロキシサポートについて説明する項を追加および更新しました。 • プロキシ サポート （8 ページ） • プロキシ サーバの要件 （15 ページ） • プロキシ統合のための HDS ノードの構成 （29 ページ） 既存の導入環境のプロキシサポートの内容だけを確認するには、ヘルプ記事「ハイブリッド データ セキュリティと Webex ビデオ メッシュのプロキシ サポート」 を参照してください。
2019 年 6 月 13 日	「トライアルから実稼働への移行タスク フロー （35 ページ）」を更新して、組織がディレクトリ同期を使用している場合は、トライアルを開始する前に `HdsTrialGroup` グループ オブジェクトを同期する必要があるという注記を追加しました。

新規および変更情報

日付	変更内容
2019 年 3 月 6 日	• 要件と前提条件を「環境の準備 （11 ページ）」の章に移動しました。 • 「Hybrid Data Security クラスタのセットアップ （19 ページ）」の章に Hybrid Data Security 導入タスク フロー （19 ページ）の概要を追加しました。 （次の章の手順に従って）トライアルを開始するまでは、ノードでサービスがアクティブ化されていないことを通知するアラームが生成されるという注記を追加しました。 • 「トライアルの実施と実稼働への移行 （35 ページ）」の章にトライアルから実稼働への移行タスク フロー （35 ページ）を追加しました。
2019 年 2 月 28 日	• OVA が作成するディスクのサイズを反映して、Hybrid Data Security ノードにする仮想ホストを準備する際に確保するローカルハードディスクの容量を 50 GB から 20 GB に修正しました。
2019 年 2 月 26 日	• Hybrid Data Security ノードが、PostgreSQL データベース サーバとの暗号化された接続と、TLS 対応 Syslog サーバへの暗号化されたロギング接続をサポートするようになりました。「HDS ホストの構成 ISO の作成 （21 ページ）」を更新して手順を追加しました。 • 「Hybrid Data Security ノード VM のインターネット接続要件」の表から、宛先 URL を削除しました。現在この表は、「Webex Teams サービスのネットワーク要件」の表「Webex Teams ハイブリッド サービスの追加 URL」にリストされている URL を参照するようになっています。
2019 年 1 月 24 日	• Hybrid Data Security が、データベースとして Microsoft SQL Server をサポートするようになりました。SQL Server Always On（Always On フェールオーバー クラスタと Always On 可用性グループ）は、Hybrid Data Security で使用される JDBC ドライバでサポートされています。SQL Server を使用した導入に関する内容を追加しました。 （注） Microsoft SQL Server サポートの対象は、Hybrid Data Security の新しい導入環境のみです。現在、既存の導入環境では PostgreSQL から Microsoft SQL Server へのデータの移行はサポートされていません。

新規および変更情報

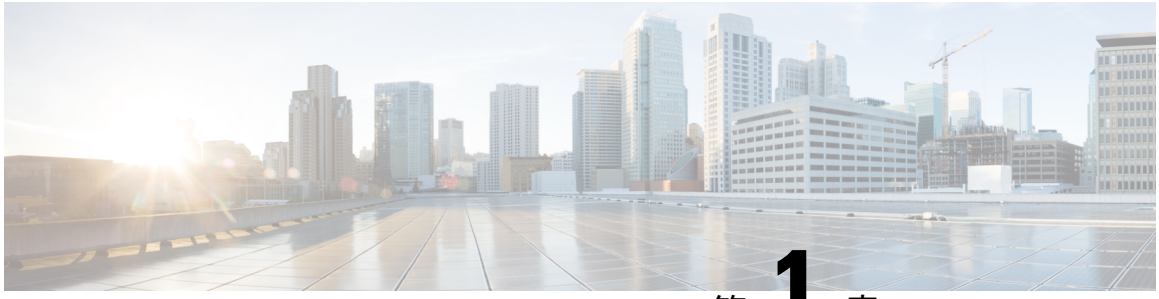
日付	変更内容
2018 年 11 月 5 日	• 「HDS ホストの構成 ISO の作成 （21 ページ）」および「ノード構成の変更 （42 ページ）」に、`docker rmi ciscosparkhds/hds-setup:stable` を使用して既存の Docker HDS インスタンスをクリーンアップするための準備手順を追加しました。 • 「HDS ホストの構成 ISO の作成 （21 ページ）」のキー アクセス レベルのステップを、インターフェイスに合わせて更新しました。
2018 年 10 月 19 日	• 「Hybrid Data Security の前提条件への対応 （16 ページ）」のファイアウォール接続情報を、ノードの要件と ISO 構成マシンの要件に分けました。
2018 年 7 月 31 日	• 「Hybrid Data Security の前提条件への対応 （16 ページ）」に、ポート 22（SSH アクセス）と、NAT およびファイアウォール接続に関する情報を追加しました。
2018 年 5 月 21 日	Cisco Spark のリブランディングを反映して、次のように用語を変更しました。 • Cisco Spark Hybrid Data Security は Cisco Webex Hybrid Data Security に変更されています。 • Cisco Spark アプリは Cisco Webex Teams アプリに変更されています。 • Cisco Collaboration Cloud は Cisco Webex クラウドに変更されています。
2018 年 4 月 11 日	• 「ディザスタ リカバリのためのスタンバイ データ センター （6 ページ）」を追加しました。 • 「Hybrid Data Security の前提条件への対応 （16 ページ）」を更新して、バックアップ環境は別のデータ センター内に配置する必要があることを明記しました。 • 「ディザスタ リカバリ後のクラスタの再構築 （46 ページ）」が更新されました。
2018 年 2 月 22 日	• 「HDS ホストの構成 ISO の作成 （21 ページ）」および「ノード構成の変更 （42 ページ）」に、サービス アカウント パスワードの 9 ヶ月の有効期間に関する情報と、HDS セットアップ ツールを使用してサービス アカウント パスワードをリセットする手順を追加しました。

新規および変更情報

日付	変更内容
2018 年 2 月 15 日	• 表「X.509 証明書の要件 （11 ページ）」に、証明書をワイルドカード証明書にすることはできないこと、KMS は x.509v3 SAN フィールドで定義されているドメインではなく、CN ドメインを使用することを明記しました。
2018 年 1 月 18 日	• 付録「HDS ノードとクラウド間のトラフィック （57 ページ）」を追加しました。 • 「Hybrid Data Security に関する既知の問題 （53 ページ）」から解決済みの問題を削除しました。 • 「Hybrid Data Security の前提条件への対応 （16 ページ）」の HDS ノードの TCP 接続要件のリストで、index.docker.io を *.docker.io に変更し、*.cloudfront.net を追加しました。 • 「HDS ホストの構成 ISO の作成 （21 ページ）」を更新して、データベース ホストと Syslogd サーバを DNS で解決できない場合、IP アドレスを使用して構成するよう説明しました。
2017 年 11 月 2 日	• HdsTrialGroup のディレクトリ同期について明確にしました。 • VM ノードにマウントするための ISO 構成ファイルのアップロード手順を修正しました。
2017 年 8 月 18 日	初版

新規および変更情報

目 次



第 1 章

Hybrid Data Security の概要

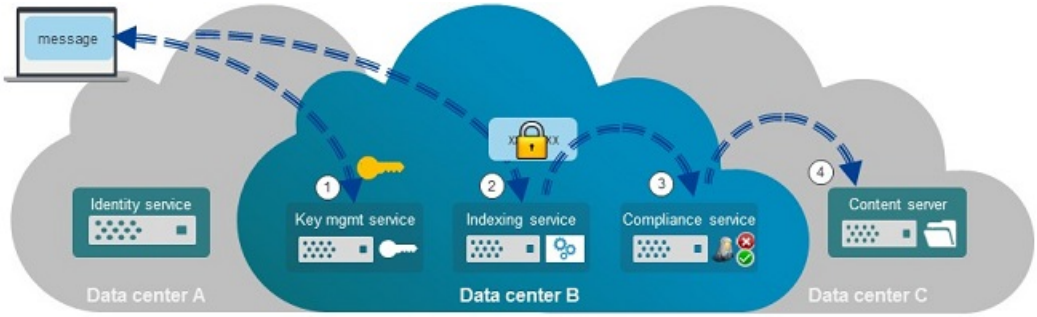
Cisco Webex Teams を設計する際に当初から主な焦点とされていたのは、データ セキュリティです。このセキュリティの基盤は、Webex Teams クライアントがキー管理サービス（KMS）とやり取りすることで実現されるエンドツーエンドのコンテンツ暗号化です。KMS は、クライアントがメッセージやファイルを動的に暗号化および復号化するために使用する暗号キーを作成および管理します。

Webex Teams ではデフォルトで、シスコのセキュリティ レルム内のクラウド KMS に保管された動的キーによってエンドツーエンドの暗号化が行われます。Hybrid Data Security は KMS とその他のセキュリティ関連の機能をユーザの企業データ センターに移すため、そのユーザのみが暗号化されたコンテンツのキーを保持します。

セキュリティ レルムのアーキテクチャ

Cisco Webex のクラウド アーキテクチャでは、次に示すように、サービスがタイプ別に異なるレルム、つまり信頼ドメインに分離されます。

図 *1 :* 分離されたレルム（***Hybrid Data Security*** なし）



Hybrid Data Security について理解を深めるため、最初にクラウドのレルム内でシスコのすべての機能が提供される純粋なクラウドの場合を見てみましょう。アイデンティティ サービスは、ユーザを電子メール アドレスなどの個人情報と直接関連付けることができる唯一の場所であり、データ センター B のセキュリティ レルムから論理的にも物理的にも分離されています。さらにこの 2 つのレルムも、暗号化されたコンテンツが最終的に保管されるデータ センター C のレルムから分離されています。

この図では、クライアントはユーザのラップトップ上で Cisco Webex Teams アプリ を実行しており、アイデンティティ サービスによって認証されています。ユーザがスペースに送信するメッセージを作成すると、次の手順が実行されます。

1. クライアントがキー管理サービス（KMS）とのセキュアな接続を確立し、メッセージを暗号化するためのキーを要求します。このセキュア接続では ECDH が使用され、KMS は AES-256 マスター キーを使用してキーを暗号化します。
2. メッセージがクライアントから送信される前に暗号化されます。クライアントがインデックス サービスにメッセージを送信します。インデックス サービスは、その後のコンテンツ検索を支援するために暗号化された検索インデックスを作成します。
3. 暗号化されたメッセージがコンプライアンス チェックのためにコンプライアンス サービスに送信されます。
4. 暗号化されたメッセージが保管用のレルムに格納されます。

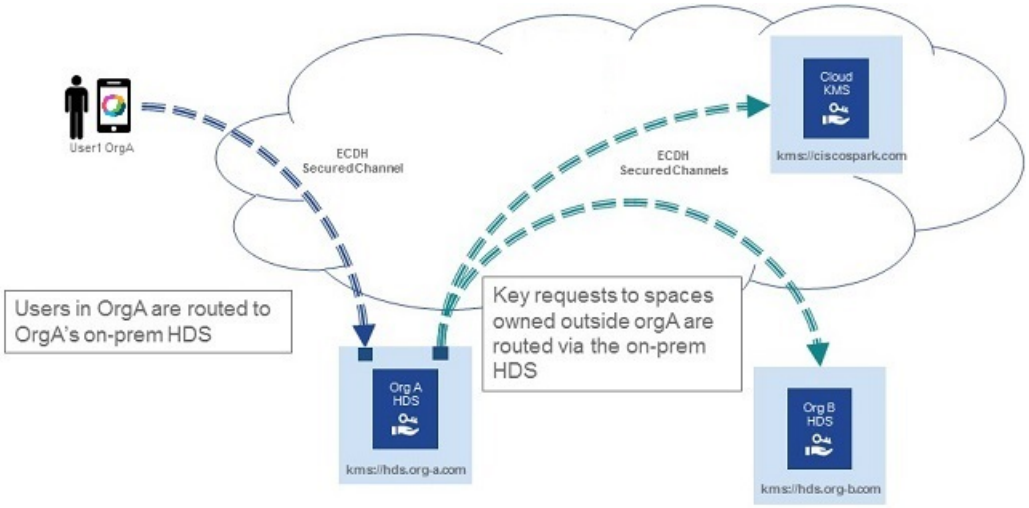
Hybrid Data Security を導入する場合は、セキュリティ レルムの機能（KMS、インデックス作成、およびコンプライアンス）をオンプレミスのデータ センターに移動します。Cisco Webex を構成するその他のクラウドサービス（アイデンティティとコンテンツの保管を含む）は、シスコのレルムに残ります。

他の組織とのコラボレーション

組織内のユーザは定期的に Cisco Webex Teams を使用して、他の組織の外部参加者と連携することができます。（ユーザの 1 人が作成したために）組織が所有しているスペースのキーをいずれかのユーザから要求された場合、KMS は ECDH で保護されたチャネルを介してクライアントにキーを送信します。ただし、そのスペースのキーを別の組織が所有している場合、KMS

は別の ECDH チャネルを介して Cisco Webex クラウドに要求をルーティングし、該当する KMS からキーを取得した後、そのキーを元のチャネルを介してユーザに返します。

図 *2:*



OrgA で実行されている KMS サービスは、x.509 PKI 証明書を使用して他の組織の KMS への接続を検証します。Hybrid Data Security 導入環境で使用する x.509 証明書を生成する方法の詳細については、「環境の準備 （11 ページ）」を参照してください。

Hybrid Data Security の導入時に期待されること

Hybrid Data Security の導入では、ユーザの深い関与と、暗号キーの所有に伴うリスクの認識が必要です。

Hybrid Data Security を導入するには、次のものを用意する必要があります。

- Cisco Webex Teams プランのサポート対象となっている国内に開設された安全なデータ センター。
- 「環境の準備 （11 ページ）」に記載されている機器、ソフトウェア、およびネットワーク アクセス。

Hybrid Data Security 用に作成した構成 ISO、またはお客様提供のデータベースのいずれかが完全に失われると、キーが失われます。キーが失われた場合、ユーザは Cisco Webex Teams 内のスペース コンテンツやその他の暗号化されたデータを復号化できなくなります。このような場合は、新しい導入を構築できますが、表示されるのは新しいコンテンツだけです。データへのアクセスが失われるのを避けるには、次のような対策が必要です。

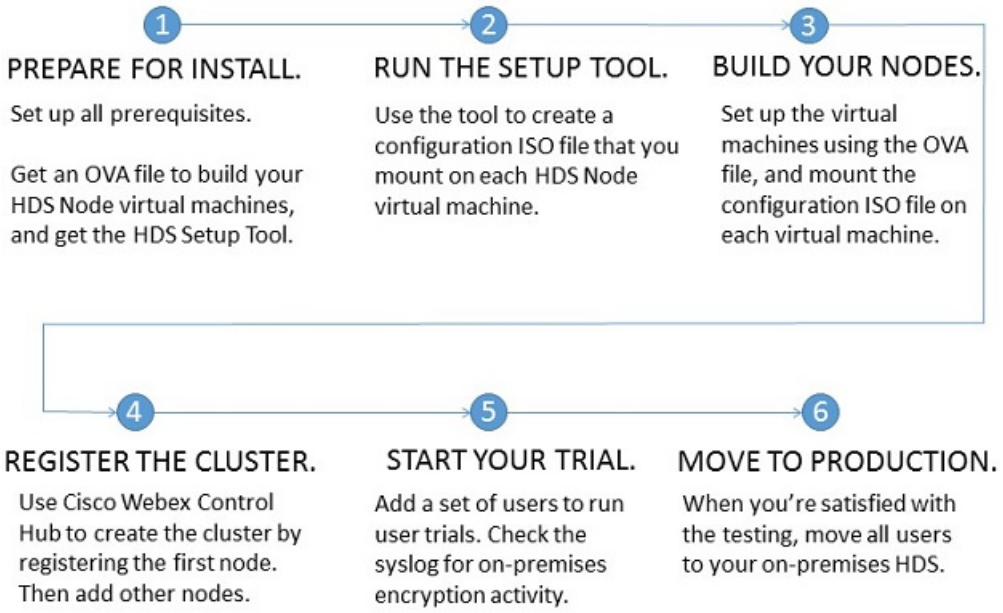
- データベースおよび構成 ISO のバックアップとリカバリを管理します。
- データベース ディスクの障害やデータ センターの災害などの大災害が発生した場合に、迅速なディザスタ リカバリを実行できるように準備します。

セットアップ プロセスの概要

このドキュメントでは、Hybrid Data Security 導入環境のセットアップと管理について説明します。

- **Hybrid Data Security** のセットアップ：これには、必要なインフラストラクチャの準備と Hybrid Data Security ソフトウェアのインストール、ユーザのサブセットを使用したトライアルモードでの導入環境のテスト、テスト完了後の実稼働への移行が含まれます。これにより、組織全体がセキュリティ機能として Hybrid Data Security クラスタを使用するようになります。

  セットアップ、トライアル、実稼働の各フェーズについては、以降の 3 つの章で詳しく説明します。



- **Hybrid Data Security 導入環境の保守**：Cisco Webex クラウドは自動的かつ継続的にアップグレードされます。IT部門は、この導入のティア 1 サポートを提供し、必要に応じてシスコ サポートと契約できます。Cisco Webex Control Hub では、画面上の通知を使用したり、電子メールベースのアラートを設定したりできます。

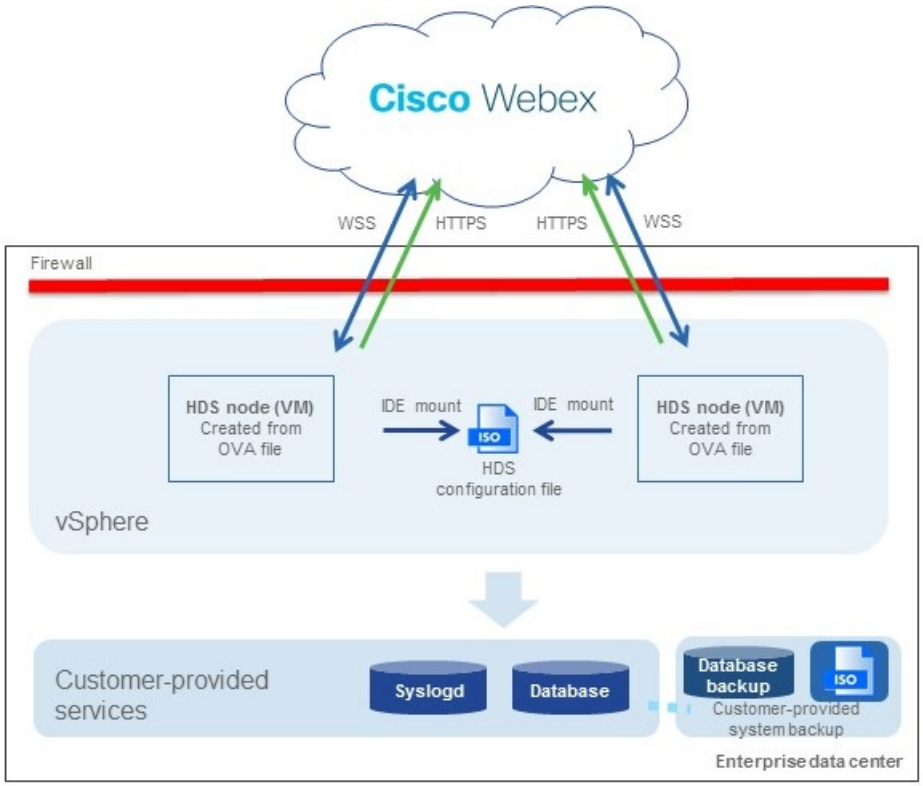
- **一般的なアラート、トラブルシューティング手順、および既知の問題の理解**：Hybrid Data Security の導入時または使用時に問題が発生した場合は、このガイドの最後の章と付録の「既知の問題」が問題の特定と修正に役立ちます。

Hybrid Data Security の導入モデル

企業データ センター内では、Hybrid Data Security を別個の仮想ホスト上のノードの単一クラスタとして導入します。ノードは安全な WebSocket と安全な HTTP を介して Cisco Webex クラウドと通信します。

インストール プロセスでは、ユーザが用意した VM に仮想アプライアンスをセットアップするための OVA ファイルが提供されます。ユーザは HDS セットアップ ツールを使用して、各ノードにマウントするカスタム クラスタ構成 ISO ファイルを作成します。Hybrid Data Security クラスタでは、お客様提供の Syslogd サーバと PostgreSQL または Microsoft SQL Server データベースを使用します。（Syslogd とデータベース接続の詳細は HDS セットアップ ツールで構成します）。

図 *3 : Hybrid Data Security* の導入モデル



クラスタには 2 つ以上のノードを含める必要があります。ノードの推奨数は 3、最大数は 5 です。複数のノードを導入すると、ノード上のソフトウェア アップグレードやその他のメンテナンス アクティビティ中にサービスが中断されなくなります。（Cisco Webex クラウドがアップグレードするノードは 1 度に 1 つのみです）。

クラスタ内のすべてのノードは同じキー データストアにアクセスし、同じ syslog サーバにアクティビティを記録します。ノード自体はステートレスであり、クラウドの指示に従ってラウンド ロビン方式でキー要求を処理します。

ノードは、ユーザが Cisco Webex Control Hub に登録したときにアクティブになります。個別のノードの稼働を停止するには、そのノードを登録解除します。必要な場合は後で再登録できます。

サポートされるクラスタは組織ごとに 1 つのみです。

Hybrid Data Security のトライアル モード

Hybrid Data Security 導入をセットアップしたら、最初にパイロット ユーザを作成して導入を試用します。トライアル期間中、これらのユーザは暗号キーやその他のセキュリティ レルム サービスに関してオンプレミスの Hybrid Data Security ドメインを使用します。他のユーザは、クラウドのセキュリティ レルムを使用し続けます。

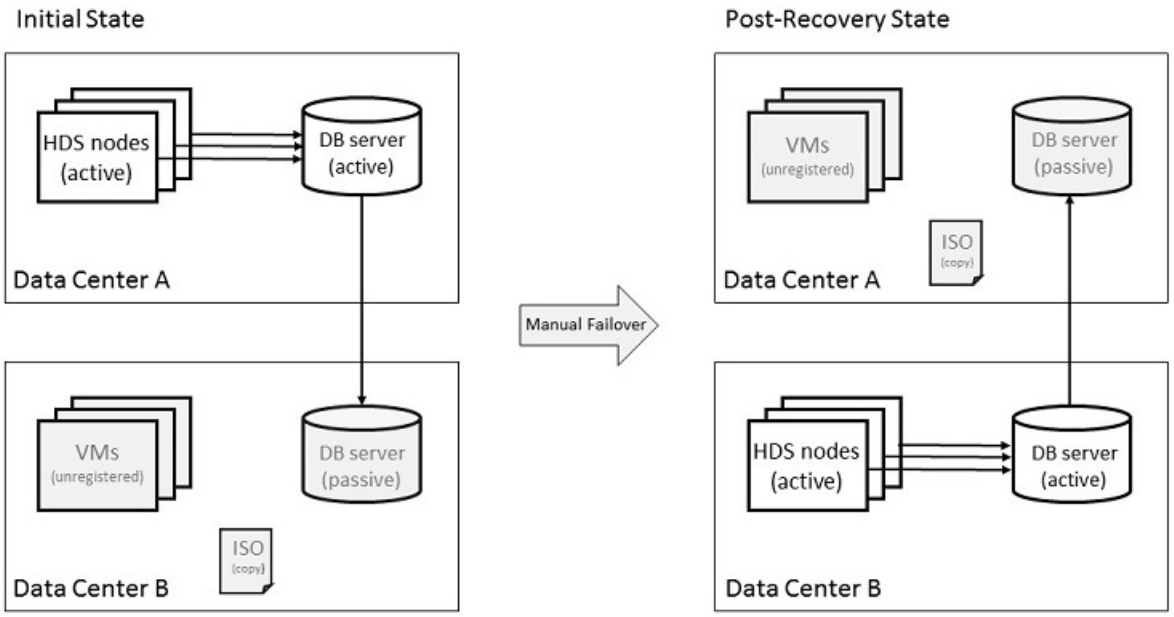
トライアル中に導入を続行しないことを決定し、サービスを非アクティブ化する場合は、パイロット ユーザと、トライアル期間中に作成された新しいスペースを介してパイロット ユーザとやり取りを行ったすべてのユーザは、メッセージやコンテンツにアクセスできなくなります。これらのユーザには、Cisco Webex Teams アプリに「このメッセージを復号化できません（This message cannot be decrypted）」というメッセージが表示されます。

導入がトライアル ユーザに対して適切に機能していることを確認し、Hybrid Data Security をすべてのユーザに拡張する準備が整ったら、実稼働に移行できます。パイロット ユーザは、トライアル中に使用したキーに引き続きアクセスできます。ただし、実稼働と元のトライアルの間でモードを切り替えることはできません。ディザスタ リカバリの実施などの目的でサービスを非アクティブ化する必要がある場合は、再アクティブ化したときに新しいトライアルを開始し、新しいトライアル用のパイロット ユーザを設定してから実稼働モードに戻る必要があります。この時点でユーザがデータに引き続きアクセスできるかどうかは、クラスタ内のキー データストアと Hybrid Data Security ノード用の ISO 構成ファイルのバックアップが適切に保持されているかどうかによります。

ディザスタ リカバリのためのスタンバイ データ センター

導入時に、セキュアなスタンバイ データ センターをセットアップします。スタンバイ データ センターに、PostgreSQL または Microsoft SQL Server データベースのバックアップ コピーと、ハイブリッド データ セキュリティ ノード用に生成された構成 ISO ファイルを保管します。データ センターで障害が発生した場合、導入環境を手動でスタンバイ データ センターにフェールオーバーできます。

図 *4:* スタンバイ データ センターへの手動フェールオーバー



データ センター A で障害が発生した場合は、次の手順に従います。

1. Cisco Webex Control Hub から、データ センター A の HDS ノードを削除します。
2. データ センター B のデータベース サーバをアクティブ（プライマリまたはマスター）データベースにします。
3. データ センター B とデータ センター A のデータベース ログイン情報が異なる場合は、セットアップ ツールを実行して ISO 構成ファイルを更新します。
4. ISO 構成ファイルをデータ センター B の VM にマウントし、それらの VM を Control Hub に登録します。
5. できるだけ早く、ISO 構成ファイルとアクティブ データベースのバックアップ コピーがあることを確認します。

フェールオーバー手順の詳細については、「ディザスタ リカバリ後のクラスタの再構築 （46 ページ）」を参照してください。

（注） アクティブな Hybrid Data Security ノードは、常にアクティブなデータベース サーバと同じデータ センター内に存在する必要があります。

プロキシ サポート

Hybrid Data Security では、明示的かつ透過的な検査プロキシと非検査プロキシがサポートされています。これらのプロキシを導入環境に関連付けることで、企業からクラウドへのトラフィックを保護およびモニタリングできます。ノード上のプラットフォーム管理インターフェイスを使用して、証明書を管理できます。また、ノード上にプロキシをセットアップした後の全体的な接続ステータスも確認できます。

Hybrid Data Security ノードは、次のプロキシ オプションをサポートしています。

- **プロキシなし**：プロキシを統合するために HDS ノードセットアップの信頼ストアとプロキシ構成を使用しない場合、これがデフォルトになります。証明書の更新は必要ありません。
- **透過的な非検査プロキシ**：ノードは特定のプロキシ サーバ アドレスを使用するように構成されないため、非検査プロキシと連動するための変更は必要ありません。証明書の更新は必要ありません。
- **透過的なトンネリングまたは検査プロキシ**：ノードは特定のプロキシ サーバ アドレスを使用するように構成されません。ノード上の HTTP または HTTPS の構成を変更する必要はありません。ただし、ノードがプロキシを信頼するよう、ノードにはルート証明書が必要です。通常、IT は検査プロキシを使用して、アクセス可能な Web サイトおよび許可されないコンテンツのタイプに関するポリシーを適用します。このタイプのプロキシは、すべてのトラフィックを（HTTPS も）復号化します。
- **明示的なプロキシ**：明示的なプロキシを使用する場合、HDS ノードに使用するプロキシ サーバと認証方式を指示します。明示的なプロキシを構成するには、各ノードに次の情報を入力する必要があります。

  1. [プロキシ IP/FQDN（Proxy IP/FQDN）]：プロキシ マシンに到達可能なアドレス。
  2. [プロキシポート（Proxy Port）]：プロキシがプロキシ経由のトラフィックをリッスンするために使用するポート番号。
  3. **プロキシプロトコル**：プロキシサーバのサポート対象に応じて、次のプロトコルの中から選択します。
     - HTTP：クライアントが送信するすべての要求を表示および制御します。
     - HTTPS：サーバへのチャネルを提供します。クライアントがサーバの証明書を受信して検証します。
  4. [認証タイプ（Authentication Type）]：次の認証タイプの中から選択します。
     - [なし（None）]：これ以上の認証は必要ありません。

       プロキシ プロトコルとして HTTP または HTTPS のいずれかを選択した場合に使用できます。

- [基本（Basic）]：要求を行うときにユーザ名とパスワードを入力する HTTP ユーザエージェントに対して使用されます。Base64 エンコーディングを使用します。

  プロキシ プロトコルとして HTTP または HTTPS のいずれかを選択した場合に使用できます。

  各ノードでユーザ名とパスワードを入力する必要があります。

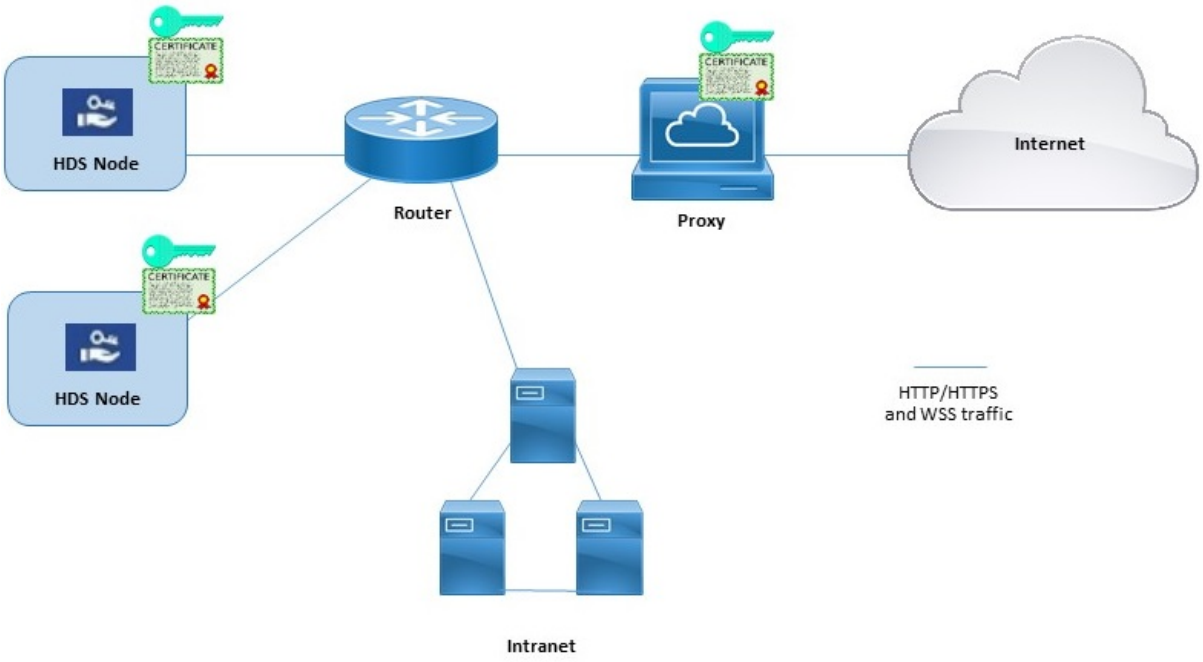
- [ダイジェスト（Digest）]：機密情報を送信する前にアカウントを確認するために使用されます。ネットワーク経由で送信する前に、ユーザ名とパスワードにハッシュ関数を適用します。

  プロキシ プロトコルとして HTTPS を選択した場合にのみ使用できます。

  各ノードでユーザ名とパスワードを入力する必要があります。

Hybrid Data Security ノードとプロキシの例

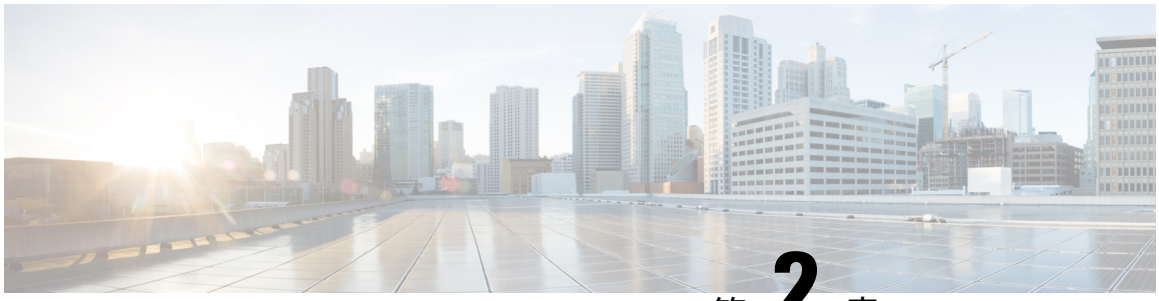
次の図は、Hybrid Data Security、ネットワーク、プロキシ間の接続例を示しています。透過的な検査プロキシと明示的な HTTPS 検査プロキシのオプションでは、プロキシと Hybrid Data Security ノードに同じルート証明書がインストールされている必要があります。



ブロックされた外部 DNS 解決モード（明示的なプロキシ設定）

ノードを登録するか、ノードのプロキシ設定を確認すると、プロセスは、Cisco Webex クラウドへの DNS ルックアップと接続をテストします。内部クライアントに対する外部 DNS 解決を許可しない明示的なプロキシ設定を導入している環境で、ノードが DNS サーバに照会できな

い場合、そのノードは自動的にブロックされた外部 DNS 解決モードに入ります。このモードでは、ノード登録およびその他のプロキシ接続テストを続行できます。



第 2 章

環境の準備

Hybrid Data Security の要件

Cisco Webex ライセンスの要件

Hybrid Data Security を導入するには、次の要件を満たしている必要があります。

- Pro Pack for Cisco Webex Control Hub を使用していること（https://www.cisco.com/go/pro-pack を参照してください）。

X.509 証明書の要件

証明書チェーンは、次の要件を満たしている必要があります。

表 *1 : Hybrid Data Security* 導入に使用する *x.509* 証明書の要件

要件	詳細
• 信頼できる認証局（CA）によって署名されていること	デフォルトでは、Mozilla リスト（https://wiki.mozilla.org/CA:IncludedCAs）内の CA（WoSign と StartCom を除く）を信頼します。

要件	詳細
• Hybrid Data Security 導入環境を識別する共通名（CN）ドメイン名を持っていること • ワイルドカード証明書ではないこと	この CN は、到達可能またはライブ ホストである必要はありません。組織を反映する名前（`hds.company.com` など）を使用することをお勧めします。 CN に *（ワイルドカード）を含めることはできません。 CN は、Hybrid Data Securityノードを Cisco Webex Teams クライアントに対して確認するために使用されます。クラスタ内の Hybrid Data Security ノードすべてが同じ証明書を使用します。KMS は、x.509v3 SAN フィールドで定義されるドメインではなく、この CN ドメインを使用して自身を識別します。 この証明書を持つノードを登録すると、CN ドメイン名の変更はサポートされなくなります。トライアルと実稼働の両方の導入環境に適用できるドメインを選択してください。
• SHA1 シグニチャでないこと	KMS ソフトウェアは、他の組織の KMS への接続を検証する場合に SHA1 シグニチャをサポートしません。
• パスワードで保護された PKCS #12 ファイルとしてフォーマットされていること • アップロードする証明書、秘密キー、および中間証明書に `kms-private-key` というフレンドリ名を付けます。	証明書の形式は、OpenSSL などのコンバーターを使用して変更できます。 HDS セットアップ ツールを実行するときは、パスワードを入力する必要があります。

KMS ソフトウェアは、キー使用法または拡張キー使用法の制約を適用しません。一部の認証局は、各証明書（サーバ認証など）に対して拡張キー使用法の制約を適用することを要求します。サーバ認証やその他の設定を使用しても問題ありません。

仮想ホストの要件

クラスタ内で Hybrid Data Security ノードとしてセットアップする仮想ホストには、次の要件があります。

- 同じセキュアなデータ センターに配置された最小 2 個（推奨 3 個、最大 5 個）の独立したホスト
- VMware ESXi 6.5 以降がインストールされ、実行されていること

重要　それ以前のバージョンの ESXi を使用している場合は、アップグレードする必要があります。

- サーバごとに少なくとも 4 つの vCPU、8 GB のメイン メモリ、20 GB のローカル ハード ディスク容量があること

データベース サーバの要件

データベース サーバには2つのオプションがあります。それぞれの要件は、次のとおりです。

表 *2:* データベースのタイプごとのデータベース サーバの要件

PostgreSQL	Microsoft SQL Server
• PostgreSQL 9.6 以降がインストールされて実行中であること	• Service Pack 2 および Cumulative Update 2 以降が適用された SQL Server 2016 Enterprise または Standard がインストールされて実行中であること • セットアップ時に[混合モード認証（Mixed Mode Authentication）] を選択すること。Windows 認証モードはサポートされていません。
最小 8 個の vCPU、16 GB のメイン メモリ、十分なハード ディスク容量とこの容量を超えていないことを確認するためのモニタリング（記憶域を増やすことなく長期間データベースを実行したい場合は、2 TB を推奨）	最小 8 個の vCPU、16 GB のメイン メモリ、十分なハード ディスク容量とこの容量を超えていないことを確認するためのモニタリング（記憶域を増やすことなく長期間データベースを実行したい場合は、2 TB を推奨）

現在、HDS ソフトウェアはデータベース サーバとの通信用に次のドライバ バージョンをインストールします。

PostgreSQL	Microsoft SQL Server
Postgres JDBC ドライバ 42.2.5	SQL Server JDBC ドライバ 4.6 このドライバ バージョンでは、SQL Server Always On（Always On フェールオーバー クラスタ インスタンスと Always ON 可用性グループ）がサポートされています。

外部接続の要件

HDS アプリケーション用に次の接続を許可するように、ファイアウォールを設定します。

Application	プロトコル	ポート	アプリケーションからの方向	宛先

Hybrid Data Security ノード	TCP	443	アウトバウンド HTTPS および WSS	• Cisco Webex サーバ：
				  • *.wbx2.com
				  • *.ciscospark.com
				• リージョンの共通アイデンティティ ホスト
				• Webex Teams サービスのネットワーク要件の表「Webex Teams ハイブリッド サービスの追加 URL」にリストされているその他の URL

HDS セットアップ ツール	TCP	443	アウトバウンド HTTPS	• *.wbx2.com • リージョンの共通アイデンティティ ホスト • hub.docker.com

（注） 上記の表にリストされているドメイン宛先へのアウトバウンド接続が NAT またはファイアウォールで許可されている限り、Hybrid Data Security ノードはネットワーク アクセス変換（NAT）と連動するか、ファイアウォールの背後に配置されます。Hybrid Data Security ノードへのインバウンド接続の場合、インターネットから可視になるポートはありません。データ センター内でクライアントが管理目的で Hybrid Data Security ノードにアクセスするには、TCP ポート 443 および 22 を使用する必要があります。

共通アイデンティティ（CI）ホストの URL は、リージョン固有のものです。現在の CI ホストは次のとおりです。

リージョン	共通アイデンティティ ホストの URL
アメリカ地域	• https://idbroker.webex.com • https://identity.webex.com • https://idbroker-b-us.webex.com • https://identity-b-us.webex.com
欧州連合	• https://idbroker-eu.webex.com • https://identity-eu.webex.com

プロキシ サーバの要件

- Hybrid Data Security ノードに統合できるプロキシ ソリューションとして公式にサポートされているのは、次のプロキシです。
  - 透過的なプロキシ：Cisco Web セキュリティ アプライアンス（WSA）
  - 明示的なプロキシ：Squid

（注） HTTPS トラフィックを検査する Squid プロキシは、WebSocket（wss）の接続確立に干渉する可能性があります。この問題を回避するには、「Hybrid Data Security の Squid プロキシの構成 （59 ページ）」を参照してください。

- 明示的なプロキシでは、次の認証タイプの組み合わせがサポートされています。
  - HTTP または HTTPS を使用した認証なし
  - HTTP または HTTPS を使用した基本認証
  - HTTPS のみを使用したダイジェスト認証
- 透過的な検査プロキシまたは明示的な HTTPS プロキシの場合、プロキシのルート証明書のコピーが必要です。このガイドの導入手順で、Hybrid Data Security ノードの信頼ストアにコピーをアップロードする方法を説明しています。
- HDS ノードをホストするネットワークは、ポート 443 でアウトバウンド TCP トラフィックを強制的にプロキシ経由でルーティングするように構成されている必要があります。
- Web トラフィックを検査するプロキシは、WebSocket 接続に干渉する可能性があります。この問題が発生した場合、`wbx2.com` および `ciscospark.com` へのトラフィックをバイパスする（検査しない）と、問題が解決します。

Hybrid Data Security の前提条件への対応

次のチェックリストを使用して、Hybrid Data Security クラスタをインストールして構成できるよう準備してください。

手順

ステップ 1 Cisco Webex 組織が Pro Pack for Cisco Webex Control Hub に対して有効になっていることを確認し、完全な組織管理者権限を持つアカウントのクレデンシャルを取得します。このプロセスの詳細については、シスコ パートナーまたはアカウント マネージャにお問い合わせください。

ステップ 2 HDS 導入環境に使用するドメイン名を選択し（たとえば、`hds.company.com`）、x.509 証明書、秘密キー、およびすべての中間証明書を含む証明書チェーンを取得します。証明書チェーンは、「X.509 証明書の要件 （11 ページ）」に記載されている要件を満たしている必要があります。

ステップ 3 クラスタ内の Hybrid Data Security ノードとしてセットアップする同等の仮想ホストを準備します。「仮想ホストの要件 （12 ページ）」に記載されている要件を満たす個別のホストが、同じセキュア データ センターに少なくとも 2 つ（推奨は 3 つ、最大 5 つ）が配置されている必要があります。

ステップ 4 「データベース サーバの要件 （13 ページ）」に従って、クラスタのキーデータストアとして機能するデータベース サーバを準備します。このデータベース サーバは、仮想ホストと同じセキュアなデータ センター内に配置されている必要があります。

a) キー ストレージのデータベースを作成します。（このデータベースは新規作成する必要があります。デフォルトのデータベースは使用しないでください。HDS アプリケーションは、インストール時にデータベース スキーマを作成します。）

b) ノードがデータベース サーバとの通信に使用する次の詳細情報を収集します。

- ホスト名または IP アドレス（ホスト）とポート
- キー ストレージとして使用するデータベースの名前（dbname）
- キー ストレージ データベースに対するすべての権限を持つユーザのユーザ名とパスワード

ステップ 5 迅速にディザスタ リカバリを行えるように、別のデータ センターにバックアップ環境をセットアップします。バックアップ環境には、VM の実稼働環境とバックアップ データベース サーバをミラーリングします。たとえば、実稼働環境に HDS ノードを実行する 3 つの VM がある場合、バックアップ環境にも 3 つの VM が必要です。

ステップ 6 クラスタ内のノードからログを収集する Syslog ホストをセットアップします。Syslog ホストのネットワーク アドレスと Syslog ポート（デフォルトは UDP 514）を収集します。

ステップ 7 Hybrid Data Security ノード、データベース サーバ、および syslog ホストのセキュア バックアップ ポリシーを作成します。回復不能なデータ損失を防ぐために、少なくとも Hybrid Data Security ノードで生成されたデータベースと構成 ISO ファイルをバックアップする必要があります。

注意 Hybrid Data Security ノードにはコンテンツの暗号化と復号に使用されるキーが保管されるため、運用中の導入環境が保守されていないと、そのコンテンツが**回復不能**になります。

Cisco Webex Teams クライアントは自身のキーをキャッシュするため、停止してもすぐには認識されず、その状態は徐々に明らかになります。一時的な停止は防ぐことができませんが、回復可能です。ただし、データベースまたは構成 ISO ファイルのいずれかを完全に損失すると（使用可能なバックアップがない状態）、顧客データが回復不能になります。Hybrid Data Security ノードのオペレータは、データベースと構成 ISO ファイルを頻繁にバックアップし、壊滅的な障害が発生した場合に Hybrid Data Security データ センターを再構築できるよう準備する必要があります。

ステップ 8 ファイアウォールが、「外部接続の要件 （14 ページ）」で説明されている Hybrid Data Security ノードに対する接続を許可するように構成されていることを確認します。

ステップ 9 サポート対象の OS（Microsoft Windows 10 Professional または Enterprise 64 ビット、あるいは Mac OSX Yosemite 10.10.3 以降）で稼働し、http://127.0.0.1:8080 でアクセスできる Web ブラウザがインストールされている任意のローカル マシンに Docker（https://www.docker.com）をインストールします。

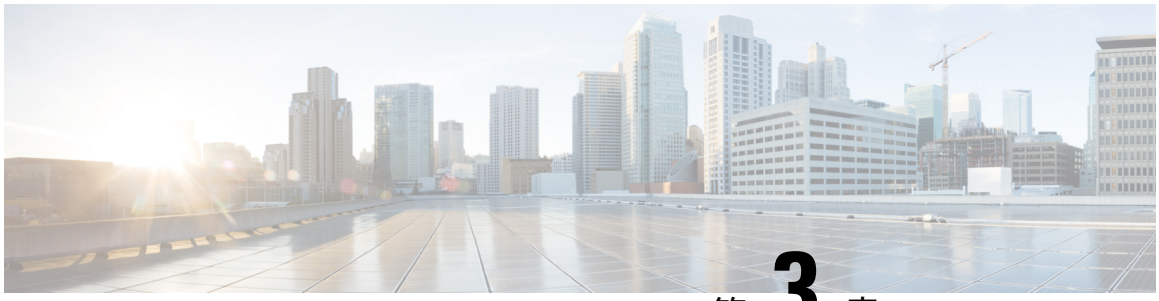
Docker インスタンスを使用して HDS セットアップ ツールをダウンロードして実行します。これにより、すべての Hybrid Data Security ノードのローカル構成情報が形成されます。

HDS セットアップ ツールをインストールして実行するには、ローカル マシンが「外部接続の要件 （14 ページ）」に記載されている接続要件を満たしている必要があります。

ステップ 10 プロキシを Hybrid Data Security に統合する場合は、「プロキシ サーバの要件 （15 ページ）」を満たしていることを確認します。

ステップ 11 組織でディレクトリ同期を使用している場合は、Active Directory に `HdsTrialGroup` という名前のグループを作成し、そのグループにパイロット ユーザを追加します。トライアル グループには、最大 250 のユーザを含めることができます。`HdsTrialGroup` オブジェクトをクラウドに同期してからでないと、組織でトライアルを開始できません。グループ オブジェクトを同期するには、ディレクトリ コネクタの **[構成（Configuration）] > [オブジェクト選択（Object Selection）]** メニューからグループ オブジェクトを選択します。（詳細な手順については、『Cisco Directory Connector 導入ガイド』を参照してください）。

注意 所定のスペースのキーは、そのスペースの作成者によって設定されます。パイロット ユーザを選択する際は、Hybrid Data Security 導入環境を永久に非アクティブ化することにした場合、パイロットユーザが作成したスペース内のコンテンツにすべてのユーザがアクセスできなくなることに留意してください。アクセスできなくなったことは、ユーザのアプリがキャッシュされたコンテンツのコピーを更新した時点ですぐに明らかになります。



第 3 章

Hybrid Data Security クラスタのセットアップ

Hybrid Data Security 導入タスク フロー

始める前に

環境の準備 （11 ページ）

手順

	コマンドまたはアクション	目的
ステップ 1	インストール ファイルのダウンロード （20 ページ）	後で使用できるように、ローカル マシンに OVA ファイルをダウンロードします。
ステップ 2	HDS ホストの構成 ISO の作成 （21 ページ）	HDS セットアップ ツールを使用して、Hybrid Data Security ノード用の ISO 構成ファイルを作成します。

	コマンドまたはアクション	目的
ステップ 3	HDS ホスト OVA のインストール （26 ページ）	OVA ファイルから仮想マシンを作成し、ネットワーク設定などの初期設定を実行します。 （注） OVA 導入時にネットワーク設定を設定するためのオプションは、ESXi 6.5 を使用してテストされています。このオプションは、以前のバージョンでは使用できない場合があります。
ステップ 4	Hybrid Data Security VM のセットアップ （27 ページ）	VM コンソールにログインし、サインイン資格情報を設定します。OVA の導入時にノードを設定していない場合は、ノードのネットワーク設定を行います。
ステップ 5	HDS 構成 ISO のアップロードとマウント （28 ページ）	HDS セットアップツールで作成した ISO 構成ファイルを使用して VM を構成します。
ステップ 6	プロキシ統合のための HDS ノードの構成 （29 ページ）	ネットワーク環境にプロキシを構成する必要がある場合は、ノードに使用するプロキシのタイプを指定し、必要に応じてプロキシ証明書を信頼ストアに追加します。
ステップ 7	クラスタ内の最初のノードの登録 （32 ページ）	Cisco Webex クラウドに VM を Hybrid Data Security ノードとして登録します。
ステップ 8	追加ノードの作成と登録 （33 ページ）	クラスタのセットアップを完了します。
ステップ 9	トライアルの実施と実稼働への移行 （35 ページ） （次の章）	トライアルを開始するまでは、ノードでサービスがアクティブ化されていないことを通知するアラームが生成されます。

インストール ファイルのダウンロード

このタスクでは、OVA ファイルを（Hybrid Data Security ノードとしてセットアップしたサーバではなく）コンピュータにダウンロードします。このファイルは、後のインストールプロセスで使用します。

手順

ステップ 1 https://admin.webex.com にサインインして、[サービス（Services）] をクリックします。

ステップ 2 [ハイブリッドサービス（Hybrid Services）] セクションで、Hybrid Data Security カードを見つけて [セットアップ（Set up）] をクリックします。

このカードが無効になっているか、表示されない場合は、アカウントチームまたはパートナー組織にお問い合わせください。アカウント番号を伝え、Hybrid Data Security に対して組織を有効にするよう依頼してください。アカウント番号を確認するには、右上に示されている組織名の横にある歯車をクリックします。

ステップ 3 [いいえ（No）] を選択してノードをまだセットアップしていないことを示し、[次へ（Next）] をクリックします。
OVA ファイルのダウンロードが自動的に開始されます。ファイルをマシン上の任意の場所に保存します。

ステップ 4 必要に応じて、[導入ガイドを開く（Open Deployment guide）] をクリックして導入ガイドの新しいバージョンがあるかどうかを確認します。

HDS ホストの構成 ISO の作成

Hybrid Data Security のセットアップ プロセスで ISO ファイルが作成されます。作成された ISO を使用して Hybrid Data Security ホストを構成します。

始める前に

- HDS セットアップ ツールは、ローカル マシン上の Docker コンテナとして実行されます。ツールにアクセスするには、そのマシン上で Docker を実行します。このセットアップ プロセスでは、組織の完全な管理者権限を持つ Cisco Webex Control Hub アカウントのクレデンシャルが必要です。
- 生成する ISO コンフィギュレーション ファイルには、PostgreSQL または Microsoft SQL Server のデータベースを暗号化するマスター キーが格納されます。次のような設定の変更には、必ずこのファイルの最新のコピーが必要になります。
  - データベースのクレデンシャル
  - 証明書の更新
  - 認証ポリシーの変更
- データベース接続を暗号化する予定がある場合は、TLS を使用できるように PostgreSQL または SQL Server の導入環境をセットアップします。

手順

ステップ 1 お使いのマシンのコマンド ラインで、`docker login -u sparkhdsreadonly -p AtAideExertAddisDatumFlame` と入力します。

ステップ 2 ログイン後、`docker rmi ciscosparkhds/hds-setup:stable` と入力します。

（注） この手順で、以前の HDS セットアップ ツール イメージがクリーンアップされます。それ以前のイメージがない場合はエラーが返されますが、無視してかまいません。

ステップ 3 `docker pull ciscosparkhds/hds-setup:stable` と入力します。

最新の安定版イメージがダウンロードされます。

ステップ 4 プル操作が完了したら、`docker run -p 8080:8080 --rm -it ciscosparkhds/hds-setup:stable` と入力します。

コンテナが実行中の場合、「Express server listening on port 8080」という出力が表示されます。

ステップ 5 Web ブラウザを使用して、localhost（`http://127.0.0.1:8080`）にアクセスし、プロンプトが表示されたら、Cisco Webex Control Hub の顧客管理者のユーザ名を入力します。

このツールは、初めて入力されたユーザ名を使用して、そのアカウントの適切な環境を設定します。その後で、標準のサインイン プロンプトが表示されます。

ステップ 6 プロンプトが表示されたら、Cisco Webex Control Hub の顧客管理者サインインクレデンシャルを入力してから、[ログイン（Log in）] をクリックし、Hybrid Data Security に必要なサービスにアクセスできるようにします。

ステップ 7 セットアップツールの概要ページで、[開始（Get Started）] をクリックします。

ステップ 8 [ISO インポート（ISO Import）] ページでは、次の オプションを使用できます。

- [いいえ（No）]：HDS ノードを初めて作成する場合、アップロードする ISO ファイルはありません。
- [はい（Yes)]：すでに HDS ノードを作成してある場合、ブラウザで ISO ファイルを選択してアップロードします。

ステップ 9 「X.509 証明書の要件 （11 ページ）」に記載されている要件を X.509 証明書が満たしていることを確認します。

- それ以前に証明書をアップロードしたことがない場合は、X.509証明書をアップロードし、パスワードを入力して、[続行（Continue）] をクリックします。
- 証明書に問題がなければ、[続行（Continue）] をクリックします。
- 証明書が失効している場合、または証明書を置き換える場合は、[以前のISOのHDS証明書チェーンとプライベートキーを引き続き使用しますか?（Continue using HDS certificate chain and private key from previous ISO?）] で [いいえ（No）] を選択します。新しい X.509 証明書をアップロードして、パスワードを入力し、[続行（Continue）] をクリックします。

ステップ 10 キー データストア（PostgreSQL または Microsoft SQL Server）のデータベース情報とログイン情報を入力します。

a) ドロップダウン リストから、該当するデータベース サーバのタイプを選択します。
b) ホストとポートをコロンで区切って入力します。（HDS クラスタのノードから DNS 解決できないホストの場合は、IP アドレスを使用します）。

   例：

   ```
   10.92.43.20:5432
   ```

c) キー ストレージとして使用するデータベースの名前を入力します。

   重要 キー ストレージ用に新しいデータベースを作成します。デフォルトのデータベースは使用しないでください。HDS アプリケーションは、インストール時にデータベース スキーマを作成します。

d) キー ストレージ データベースに対するすべての権限を持つユーザのユーザ名とパスワードを入力します。

ステップ 11 **TLS データベース接続モード**を選択します。

モード	説明
[TLS を優先（Prefer TLS）]（デフォルト オプション）	HDS ノードでは、TLS をデータベース サーバに接続する必要はありません。データベース サーバで TLS を有効にすると、ノードは暗号化接続を試みます。
[TLS を要求（Require TLS）]	HDS ノードは、データベース サーバが TLS をネゴシエートできる場合にのみ接続します。
TLS を要求して証明書の署名者を確認（Require TLS and verify certificate signer）	（注） このモードは、SQL Server データベースには適用されません。 • HDS ノードは、データベース サーバが TLS をネゴシエートできる場合にのみ接続します。 • TLS接続が確立されると、ノードはデータベース サーバから取得した証明書の署名者を**データベースのルート証明書**の認証局に対して照合します。一致しない場合、ノードは接続を切断します。 このオプションでは、ドロップダウンにある[データベースルート証明書（Database root certificate）]コントロールを使用してルート証明書をアップロードします。

モード	説明
TLS を要求して証明書の署名者とホスト名を確認（Require TLS and verify certificate signer and hostname）	• HDS ノードは、データベース サーバが TLS をネゴシエートできる場合にのみ接続します。 • TLS接続が確立されると、ノードはデータベース サーバから取得した証明書の署名者を**データベースのルート証明書**の認証局に対して照合します。一致しない場合、ノードは接続を切断します。 • ノードは、サーバ証明書のホスト名が、[データベースホストおよびポート（Database host and port）] フィールドで指定されたホスト名と一致していることも確認します。名前は完全に一致する必要があります。完全一致でない場合は、ノードが接続を切断します。 このオプションでは、ドロップダウンにある [データベースルート証明書（Database root certificate）] コントロールを使用してルート証明書をアップロードします。

ルート証明書をアップロードするときに、必要な場合は [続行（Continue）] をクリックすると、HDS セットアップ ツールがデータベース サーバとの TLS 接続をテストします。このツールは、証明書の署名者とホスト名も確認します（該当する場合）。テストが失敗した場合、ツールに問題を説明するエラーメッセージが表示されます。エラーを無視してセットアップを続行するかどうかを選択できます。（接続の違いにより、HDS セットアップ ツールのマシンでテストが成功しなくても、HDS ノードは TLS 接続を確立できる場合があります）。

ステップ 12 [システムログ（System Logs）] ページで、次のように Syslogd サーバを構成します。

a) Syslog サーバの URL を入力します。

HDS クラスタのノードから DNS 解決できないサーバの場合は、[URL] に IP アドレスを入力します。

例：

`udp://10.92.43.23:514` は、UDP ポート 514 で Syslog ホスト 10.92.43.23 へのロギングが行われることを意味します。

b) TLS 暗号化を使用するようにサーバを設定した場合は、[syslogサーバはSSL暗号化対応として構成されていますか?（Is your syslog server configured for SSL encryption?）] をオンにします。

このチェックボックスをオンにする場合は、必ず **`tcp://10.92.43.23:514`** などの TCP URL を入力してください。

c) [syslog記録終了を選択（Choose syslog record termination）] ドロップダウンから、使用する ISO ファイルの適切な設定を選択します。選択するか、Graylog および Rsyslog TCP では [改行（Newline）] が使用されます。

- **Null バイト -- \x00**
- **改行 -- \n**：Graylog および Rsyslog TCP ではこちらを選択します。

d) [続行（Continue）]をクリックします。

ステップ 13 （任意） 一部のデータベース接続パラメータについては、[詳細設定（Advanced Settings）] でデフォルト値を変更できます。通常、変更が必要になるのはこのパラメータのみです。

```
app_datasource_connection_pool_maxSize: 10
```

ステップ 14 [サービスアカウントパスワードのリセット（Reset Service Account Passwords）] 画面で、[続行（Continue）] をクリックします。

サービスアカウントのパスワードの有効期間は、9ヶ月です。パスワードの有効期限が近づいている場合、またはパスワードをリセットして以前の ISO ファイルを無効にする場合は、この画面を使用します。

ステップ 15 [ISO ファイルをダウンロード（Download ISO File）] をクリックします。見つけやすい場所にファイルを保存します。

ステップ 16 ISO ファイルのバックアップ コピーをローカル システムに作成します。

このバックアップコピーは安全に保管してください。このファイルには、データベースコンテンツのマスター暗号キーが含まれています。構成変更を行うべき Hybrid Data Security 管理者のみにアクセス権限を制限してください。

ステップ 17 セットアップ ツールをシャット ダウンするには、`CTRL+C` を入力します。

次のタスク

構成 ISO ファイルをバックアップします。このバックアップは、リカバリ用にさらにノードを作成する場合や、構成を変更する場合に必要になります。ISO ファイルのすべてのコピーが失われた場合、マスター キーも失われます。PostgreSQL または Microsoft SQL Server のデータベースからキーを復元することはできません。

重要 このキーのコピーはシスコでは管理していないため、紛失された場合はお役に立てません。

関連トピック

ノード構成の変更 （42 ページ）

HDS ホスト OVA のインストール

OVA ファイルを使用して仮想マシンを作成するには、次の手順に従います。

手順

ステップ 1 ローカルマシン上の VMware vSphere クライアントを使用して、ESXi 仮想ホストにログインします。

ステップ 2 [ファイル（File）] > [OVF テンプレートの導入（Deploy OVF Template）] の順に選択します。

ステップ 3 ウィザードで、以前にダウンロードした OVA ファイルの場所を指定し、[**次へ（Next）**] をクリックします。

ステップ 4 [名前とフォルダの選択（Select a name and folder）] ページで、ノードの**仮想マシン名**を入力します (たとえば、「HDS_Node_1」)。仮想マシン ノードの導入先となる場所を選択し、[次へ（Next）] をクリックします。

ステップ 5 [コンピューティングリソースの選択（Select a compute resource）] ページで、宛先コンピューティングリソースを選択し、[次へ（Next）] をクリックします。

検証チェックが実行されます。完了すると、テンプレートの詳細が表示されます。

ステップ 6 テンプレートの詳細を確認して、[次へ（Next）]をクリックします。

ステップ 7 [設定（Configuration）]] ページでリソース設定を選択するように求められた場合は、[4 CPU] をクリックし、[次へ（Next）] をクリックします。

ステップ 8 [ストレージの選択（Select storage）] ページで、[次へ（ Next）] をクリックして、デフォルトのディスク形式と VM ストレージ ポリシーを受け入れます。

ステップ 9 [ネットワークの選択（Select network）] ページで、VM に必要な接続を提供するエントリの一覧からネットワークを選択します。

ステップ 10 [テンプレートのカスタマイズ（Customize template）] ページで、次のネットワーク設定を行います。

- [ホスト名（hostname）] : ノードの FQDN （ホスト名とドメイン） または1つの単語のホスト名を入力します。

  （注）
  - X.509 証明書を取得するために使用したドメインと一致するようにドメインを設定する必要はありません。
  - クラウドに問題なく登録できるように、FQDN またはノードに設定するホスト名は小文字のみを使用します。現時点では、大文字と小文字はサポートされていません。
  - FQDN の長さは、64 文字以下にする必要があります。

- **IP アドレス**：ノードの内部インターフェイスの IP アドレスを入力します。

（注） ノードには、内部 IP アドレスと DNS 名が必要です。DHCP はサポートされていません。

- **マスク**：ドット区切りの 10 進表記でサブネットを入力します。たとえば、*255.255.255.0* と入力します。
- **ゲートウェイ**：ゲートウェイの IP アドレスを入力します。ゲートウェイは、他のネットワークへの入り口として機能するネットワーク ノードを表します。
- [DNS サーバ（DNS Servers）]：ドメイン名を数値 IP アドレスに変換する処理を行う DNS サーバのカンマ区切りのリストを入力します。(最大4つのDNSエントリが許可されます)。
- [NTP サーバ（NTP Servers）]：組織の NTP サーバまたは組織で使用可能な別の外部 NTP サーバを入力します。デフォルトの NTP サーバは、すべての企業に対して機能しない場合があります。また、カンマ区切りリストを使用して複数の NTP サーバを入力することもできます。
- すべてのノードを同じサブネットまたは VLAN 上に展開します。これにより、クラスタ内のすべてのノードは、管理目的でネットワーク内のクライアントから到達可能になります。

必要に応じて、ネットワーク設定を省略して、「Hybrid Data Security VM のセットアップ （27 ページ）」の手順に従ってノード コンソールから設定を行います。

（注） OVA 導入時にネットワーク設定を設定するためのオプションは、ESXi 6.5 を使用してテストされています。このオプションは、以前のバージョンでは使用できない場合があります。

ステップ 11 ノードの VM を右クリックして、**[電源（Power）] > [電源オン（Power On）]** を選択します。

Hybrid Media Service ソフトウェアは、ゲストとして VM ホストにインストールされます。これで、コンソールにサインインしてノードを設定する準備が整いました。

トラブルシューティングのヒント

ノードコンテナが起動するまでに、数分の遅延が発生する可能性があります。最初の起動時にコンソールにブリッジファイアウォールのメッセージが表示されます。このとき、サインインはできません。

Hybrid Data Security VM のセットアップ

この手順に従って、Hybrid Data Security ノード VM コンソールに初回サインインし、サインイン認証情報を設定します。また、OVA の導入時に設定していない場合は、コンソールを使用してノードのネットワーク設定を構成することもできます。

手順

ステップ 1 VMware vSphere クライアントで、Hybrid Data Security ノード VM を選択し、[コンソール（Console）]]タブを選択します。
VM が起動してログインプロンプトが表示されます。ログインプロンプトが表示されない場合は、**Enter** キーを押します。

ステップ 2 次のデフォルトのログインとパスワードを使用してサインインし、クレデンシャルを変更します。

a) ログイン：**admin**

b) パスワード：**cisco**

VM にサインインするのはこれが初めてなので、管理者パスワードを変更する必要があります。

ステップ 3 「HDS ホスト OVA のインストール （26 ページ）」でネットワーク設定をすでに設定している場合は、この手順の残りの部分をスキップします。そうでない場合は、メインメニューで、**[構成の編集（Edit Configuration）]** オプションを選択します。

ステップ 4 IP アドレス、マスク、ゲートウェイ、および DNS 情報を使用して静的構成をセットアップします。ノードには、内部 IP アドレスと DNS 名が必要です。DHCP はサポートされていません。

ステップ 5 （省略可能）ホスト名、ドメイン、または NTP サーバをネットワーク ポリシーと一致させる必要がある場合は、これらを変更します。

X.509 証明書を取得するために使用したドメインと一致するようにドメインを設定する必要はありません。

ステップ 6 ネットワーク構成を保存し、VM を再起動して変更を適用します。

HDS 構成 ISO のアップロードとマウント

HDS セットアップ ツールで作成した ISO ファイルから仮想マシンを設定するには、次の手順を使用します。

始める前に

ISO ファイルにはマスターキーが保持されるため、Hybrid Data Security VM とこのファイルに変更を加えなければならない可能性のある管理者だけがアクセスできるよう、必要な場合に限って公開する必要があります。これらの管理者だけがデータストアにアクセスできるようにしてください。

手順

ステップ 1 ご使用のコンピュータから ISO をアップロードします。

a) VMware vSphere クライアントの左側のナビゲーション ウィンドウで、ESXi サーバをクリックします。
b) [構成（Configuration）] タブの [ハードウェア（Hardware）] リストで、[ストレージ（Storage）] をクリックします。
c) [データストア（Datastores）] リストで、VM のデータストアを右クリックし、[Browse Datastore（データベースを参照）] をクリックします。
d) [ファイルのアップロード（Upload Files）]アイコンをクリックし、[ファイルのアップロード（Upload Files）] をクリックします。
e) コンピュータ上の ISO ファイルをダウンロードした場所を参照して、[開く（Open）] をクリックします。
f) アップロード/ダウンロード操作の警告に同意するため [はい（Yes）] をクリックし、データストア ダイアログを閉じます。

ステップ 2 ISO ファイルをマウントします。

a) VMware vSphere クライアントの左側のナビゲーション ウィンドウで、VM を右クリックして [設定の編集（Edit Settings）] をクリックします。
b) [OK] をクリックして、編集オプションの制限に関する警告を受け入れます。
c) [CD/DVD ドライブ 1（CD/DVD Drive 1）] をクリックし、データストア ISO ファイルからマウントするオプションを選択して、構成 ISO ファイルをアップロードした場所を参照します。
d) [接続済み（Connected）] および [電源投入時に接続（Connect at power on）] をオンにします。
e) 変更を保存して仮想マシンを再起動します。

プロキシ統合のための HDS ノードの構成

ネットワーク環境にプロキシが必要な場合は、次の手順に従って Hybrid Data Security に統合するプロキシのタイプを指定します。透過的な検査プロキシまたは明示的な HTTPS プロキシを選択した場合は、ノードのインターフェイスを使用してルート証明書のアップロードとインストールを行うことができます。また、インターフェイスからプロキシ接続を確認し、潜在的な問題をトラブルシューティングすることもできます。

始める前に

- サポートされているプロキシオプションの概要については、「プロキシ サポート （8 ページ）」を参照してください。
- プロキシ サーバの要件 （15 ページ）

手順

ステップ 1 Web ブラウザに HDS ノードのセットアップ URL `https://[HDS ノード IP または FQDN]/setup` を入力し、ノードにセットアップした管理者クレデンシャルを入力してから [サインイン（Sign In）] をクリックします。

ステップ 2 [信頼ストアとプロキシ（Trust Store & Proxy）] に移動して、次のオプションを選択します。

- [プロキシなし（No proxy）]：プロキシを統合する前のデフォルトオプション。証明書の更新は必要ありません。
- [透過的な非検査プロキシ（Transparent Non-Inspecting Proxy）]：ノードは特定のプロキシサーバアドレスを使用するように構成されないため、非検査プロキシと連動するための変更は必要ありません。証明書の更新は必要ありません。
- [透過的な検査プロキシ（Transparent Inspecting Proxy）：ノードは特定のプロキシサーバアドレスを使用するように構成されません。Hybrid Data Security 導入環境で HTTPS 構成を変更する必要はありませんが、HDS ノードがプロキシを信頼するように、HDS ノードにルート証明書が必要です。通常、IT は検査プロキシを使用して、アクセス可能な Web サイトおよび許可されないコンテンツのタイプに関するポリシーを適用します。このタイプのプロキシは、すべてのトラフィックを（HTTPS も）復号化します。
- [明示的なプロキシ（Explicit Proxy）]：明示的なプロキシを使用する場合、プロキシサーバが使用するクライアント（HDS ノード）を指定します。このオプションは複数の認証タイプをサポートします。このオプションを選択した場合、以下の情報を入力する必要があります。

  1. [プロキシ IP/FQDN（Proxy IP/FQDN）]：プロキシ マシンに到達可能なアドレス。
  2. [プロキシポート（Proxy Port）]：プロキシがプロキシ経由のトラフィックをリッスンするために使用するポート番号。
  3. [プロキシプロトコル（Proxy Protocol）]：[http]（クライアントから受信したすべての要求を表示および制御）または [https]（サーバへのチャネルを提供し、クライアントがサーバの証明書を受信して検証）を選択します。プロキシサーバのサポート対象に応じてオプションを選択します。
  4. [認証タイプ（Authentication Type）]：次の認証タイプの中から選択します。
     - [なし（None）]：これ以上の認証は必要ありません。

       HTTP または HTTPS プロキシで使用できます。
     - [基本（Basic）]：要求を行うときにユーザ名とパスワードを入力する HTTP ユーザエージェントに対して使用されます。Base64 エンコーディングを使用します。

       HTTP または HTTPS プロキシで使用できます。

       このオプションを選択した場合は、ユーザ名とパスワードも入力する必要があります。

- [ダイジェスト（Digest）]：機密情報を送信する前にアカウントを確認するために使用されます。ネットワーク経由で送信する前に、ユーザ名とパスワードにハッシュ関数を適用します。

  HTTPS プロキシでのみ使用できます。

  このオプションを選択した場合は、ユーザ名とパスワードも入力する必要があります。

透過的な検査プロキシ、基本認証を使用した明示的なHTTPプロキシ、または明示的なHTTPSプロキシの場合は、次の手順に従います。

ステップ 3 [ルート証明書またはエンドエンティティ証明書のアップロード（Upload a Root Certificate or End Entity Certificate）] をクリックし、プロキシのルート証明書に移動して選択します。

証明書はアップロードされますが、インストールはまだ行われません。証明書をインストールするには、ノードを再起動する必要があるためです。証明書の詳細を取得するには、証明書発行者名の山矢印をクリックします。または、誤りがあったために証明書を再アップロードする場合は、[削除（Delete）] をクリックします。

ステップ 4 [プロキシ接続の確認（Check Proxy Connection）] をクリックして、ノードとプロキシ間のネットワーク接続をテストします。

接続テストが失敗した場合は、失敗した理由とその問題を解決する方法を説明するエラーメッセージが表示されます。

外部 DNS 解決が成功しなかったことを伝えるメッセージが表示された場合、ノードは DNS サーバに到達できませんでした。この条件は、多くの明示的なプロキシ設定で想定されています。セットアップを続行できます。ノードは、ブロックされた外部 DNS 解決モードで機能します。これがエラーであると思われる場合は、これらのステップを完了してから、「ブロックされた外部 DNS 解決モードをオフにする （44 ページ）」を参照してください。

ステップ 5 明示的な HTTPS プロキシの場合のみ、接続テストが成功した後、トグルを [このノードからポート 443/444 へのすべての HTTPS 要求を明示的なプロキシ経由でルーティングする（Route all port 443/444 https requests from this node through the explicit proxy）] に切り替えます。この設定は適用されるまでに 15 秒かかります。

ステップ 6 [すべての証明書を信頼ストアにインストール（Install All Certificates to The Trust Store）]（明示的な HTTPS プロキシまたは透過的な検査プロキシの場合）または [Reboot（再起動）]（明示的な HTTP プロキシの場合）をクリックし、プロンプトを読み、準備ができたら [インストール（Install）] をクリックします。

ノードは数分以内に再起動します。

ステップ 7 ノードが再起動したら、必要に応じて再度サインインして [概要（Overview）] ページを開き、接続チェックのステータスがすべて緑色になっていることを確認します。

プロキシ接続チェックでは、webex.com のサブドメインだけがテストされます。接続の問題がある場合、一般的な原因は、インストール手順に記載されているクラウドドメインの一部がプロキシでブロックされていることです。

クラスタ内の最初のノードの登録

このタスクでは、「Hybrid Data Security VM のセットアップ （27 ページ）」で作成した汎用ノードを Cisco Webex クラウドに登録して Hybrid Data Security ノードに変換します。

最初のノードを登録するときに、ノードを割り当てるクラスタを作成します。クラスタには、冗長性を確保するために導入した 1 つ以上のノードを含めます。

始める前に

- ノードの登録を開始したら、60 分以内に登録を完了する必要があります。そうでないと、最初からやり直さなければなりません。
- ブラウザのポップアップブロッカーが無効になっていること、または admin.webex.com の例外が許可されていることを確認します。

手順

ステップ 1 https://admin.webex.com にログインします。

ステップ 2 画面左側のメニューから、[サービス（Services）] を選択します。

ステップ 3 [ハイブリッドサービス（Hybrid Services）] セクションで、Hybrid Data Security を見つけて [セットアップ（Set up）] をクリックします。
[Hybrid Data Security ノードの登録（Register Hybrid Data Security Node）] ページが表示されます。

ステップ 4 [はい（Yes）] を選択してノードをセットアップして登録する準備ができたことを示し、[次へ（Next）] をクリックします。

ステップ 5 最初のフィールドに、Hybrid Data Security ノードを割り当てるクラスタの名前を入力します。

クラスタには、クラスタのノードの地理的な配置場所に応じた名前を付けることを推奨します。例：San Francisco、New York、Dallas

ステップ 6 2 番目のフィールドに、ノードの内部 IP アドレスまたは完全修飾ドメイン名（FQDN）を入力し、[次へ（Next）] をクリックします。

この IP アドレスまたは FQDN は、「Hybrid Data Security VM のセットアップ （27 ページ）」で使用した IP アドレスまたはホスト名およびドメインと一致している必要があります。

ノードを Cisco Webex に登録できることを通知するメッセージが表示されます。

ステップ 7 [ノードに進む（Go to Node）] をクリックします

ステップ 8 警告メッセージで [続行（Continue）] をクリックします。
しばらくすると、Cisco Webex サービスのノード接続テストにリダイレクトされます。すべてのテストが成功すると、[Hybrid Data Security ノードへのアクセスの許可（Allow Access to Hybrid Data Security Node）] ページが表示されます。このページで、Cisco Webex 組織にノードに対するアクセス権限を付与することを確認します。

ステップ 9 [Hybrid Data Security ノードへのアクセスを許可する（Allow Access to Your Hybrid Data Security Node）] チェックボックスをオンにして、[続行（Continue）] をクリックします。
アカウントが検証され、ノードが Cisco Webex クラウドに登録されたことを示す「登録完了（Registration Complete）」メッセージが表示されます。

ステップ 10 リンクをクリックするか、タブを閉じて Cisco Webex Control Hub Hybrid Data Security ページに戻ります。
[Hybrid Data Security] ページに、登録したノードを含む新しいクラスタが表示されます。ノードは自動的にクラウドから最新のソフトウェアをダウンロードします。

追加ノードの作成と登録

クラスタにノードを追加するには、追加の VM を作成し、同じ構成 ISO ファイルをマウントしてからノードを登録すればよいだけです。少なくとも 3 つのノードを使用することを推奨します。クラスタには最大 5 つのノードを含めることができます。

（注） この時点では、「Hybrid Data Security の前提条件への対応 （16 ページ）」で作成したバックアップ VM はスタンバイ ホストであり、ディザスタリカバリの発生時にのみ使用されます。それまでは、これらの VM はシステムに登録されません。詳細については、「ディザスタ リカバリ後のクラスタの再構築 （46 ページ）」を参照してください。

始める前に

- ノードの登録を開始したら、60 分以内に登録を完了する必要があります。そうでないと、最初からやり直さなければなりません。
- ブラウザのポップアップ ブロッカーが無効になっていること、または admin.webex.com の例外が許可されていることを確認します。

手順

ステップ 1 「HDS ホスト OVA のインストール （26 ページ）」で説明している手順を繰り返して、OVA から新しい仮想マシンを作成します。

ステップ 2 「Hybrid Data Security VM のセットアップ （27 ページ）」で説明している手順を繰り返して、新しい VM に初期構成をセットアップします。

ステップ 3 新しい VM で、「HDS 構成 ISO のアップロードとマウント （28 ページ）」で説明している手順を繰り返します。

ステップ 4 導入環境にプロキシをセットアップする場合は、必要に応じて新しいノードに対して「プロキシ統合のための HDS ノードの構成 （29 ページ）」の手順を繰り返します。

ステップ 5 ノードを登録します。

a) https://admin.webex.com で、画面左側のメニューから [サービス（Services）] を選択します。

b) [ハイブリッドサービス（Hybrid Services）] セクションで、Hybrid Data Security カードを見つけて [リソース（Resources）] をクリックします。
[Hybrid Data Security リソース（Hybrid Data Security Resources ）] ページが表示されます。

c) [リソースの追加（Add Resource）] をクリックします。

d) 最初のフィールドで、既存のクラスタの名前を選択します。

e) 2 番目のフィールドに、ノードの内部 IP アドレスまたは完全修飾ドメイン名（FQDN）を入力し、[次へ（Next）] をクリックします。
ノードを Cisco Webex に登録できることを通知するメッセージが表示されます。

f) [ノードに進む（Go to Node）] をクリックします
しばらくすると、Cisco Webex サービスのノード接続テストにリダイレクトされます。すべてのテストが成功すると、[Hybrid Data Security ノードへのアクセスの許可（Allow Access to Hybrid Data Security Node）] ページが表示されます。このページで、組織にノードに対するアクセス権限を付与することを確認します。

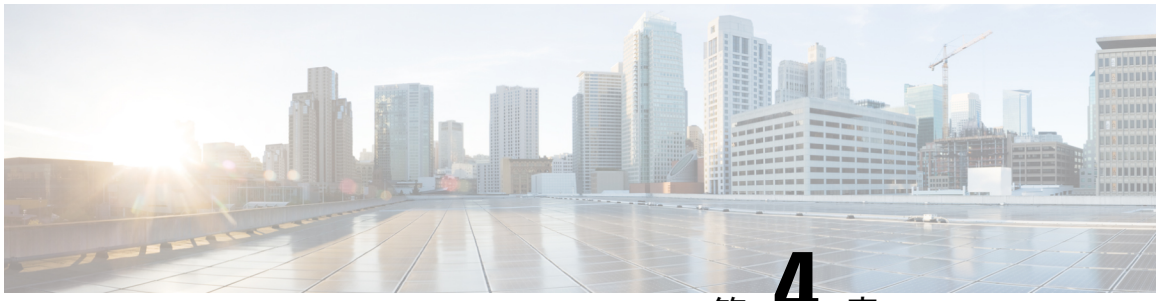
g) [Hybrid Data Security ノードへのアクセスを許可する（Allow Access to Your Hybrid Data Security Node）] チェックボックスをオンにして、[続行（Continue）] をクリックします。
アカウントが検証され、ノードが Cisco Webex クラウドに登録されたことを示す「登録完了（Registration Complete）」メッセージが表示されます。

h) リンクをクリックするか、タブを閉じて Cisco Webex Control Hub Hybrid Data Security ページに戻ります。

ノードが登録されています。トライアルを開始するまでは、ノードでサービスがアクティブ化されていないことを通知するアラームが生成されます。

次のタスク

トライアルの実施と実稼働への移行 （35 ページ） （次の章）



第 4 章

トライアルの実施と実稼働への移行

トライアルから実稼働への移行タスク フロー

Hybrid Data Security クラスタのセットアップが完了したら、パイロットを開始できます。パイロットにユーザを追加し、それを使用して、本稼働に移行する準備として導入環境のテストと検証を行うことができます。

始める前に

Hybrid Data Security クラスタのセットアップ （19 ページ）

手順

	コマンドまたはアクション	目的
ステップ 1	該当する場合は、`HdsTrialGroup` グループ オブジェクトを同期します。	組織でユーザのディレクトリ同期を使用している場合、トライアルを開始する前に、クラウドとの同期に使用する `HdsTrialGroup` グループ オブジェクトを選択する必要があります。手順については、『Cisco Directory Connector 導入ガイド』を参照してください。
ステップ 2	トライアルのアクティブ化 （36 ページ）	トライアルを開始します。このタスクを完了するまでは、ノードでサービスがア

	コマンドまたはアクション	目的
		クティブ化されていないことを通知するアラームが生成されます。
ステップ 3	Hybrid Data Security 導入環境のテスト（37 ページ）	キー要求が Hybrid Data Security 導入環境に渡されていることを確認します。
ステップ 4	Hybrid Data Security のヘルス モニタリング （38 ページ）	ステータスを確認し、アラームの電子メール通知をセットアップします。
ステップ 5	トライアル ユーザの追加または削除 （38 ページ）	
ステップ 6	次のいずれかのアクションによってトライアル フェーズを完了します。 • トライアルから実稼働への移行 （39 ページ） • 実稼働に移行せずにトライアルを終了する （40 ページ）	

トライアルのアクティブ化

始める前に

組織でユーザのディレクトリ同期を使用する場合は、組織のトライアルを開始する前に、クラウドとの同期に使用する `HdsTrialGroup` グループ オブジェクトを選択する必要があります。手順については、『Cisco Directory Connector 導入ガイド』を参照してください。

手順

ステップ 1 https://admin.webex.com にサインインして、[サービス（Services）] を選択します。

ステップ 2 Hybrid Data Security で、[設定（Settings）] をクリックします。

ステップ 3 [サービスステータス（Service Status）] セクションで、[トライアルの開始（Start Trial）] をクリックします。
サービス ステータスがトライアル モードに変わります。

ステップ 4 [ユーザの追加（Add Users）] をクリックし、Hybrid Data Security ノードを使用して暗号化およびインデックス サービスを試用する 1 人以上のユーザの電子メール アドレスを入力します。

（組織でディレクトリ同期を使用している場合は、Active Directory を使用してトライアル グループ `HdsTrialGroup` を管理します。）

Hybrid Data Security 導入環境のテスト

以下の手順に従って、Hybrid Data Security 暗号化のシナリオをテストします。

始める前に

- Hybrid Data Security 導入環境をセットアップします。
- トライアルをアクティブ化し、複数のトライアル ユーザを追加します。
- キー要求が Hybrid Data Security 導入環境に渡されていることを確認するために、Syslog にアクセスできることを確認します。

手順

ステップ 1 所定のスペースのキーは、そのスペースの作成者によって設定されます。パイロットユーザの 1 人として Cisco Webex Teams アプリ にサインインした後、スペースを作成し、少なくとも 1 人のパイロット ユーザと 1 人の非パイロット ユーザを招待します。

注意 Hybrid Data Security 導入環境を非アクティブ化する場合、クライアントがキャッシュした暗号キーのコピーが置き換えられた後は、パイロットユーザによって作成されたスペース内のコンテンツにアクセスできなくなります。

ステップ 2 新しく作成したスペースにメッセージを送信します。

ステップ 3 Syslog 出力を調べて、キー要求が Hybrid Data Security 導入環境に渡されていることを確認します。

a) KMS とのセキュアチャネルを最初に確立したユーザを調べるには、**method: create, type: EPHEMERAL_KEY_COLLECTION** でフィルタリングします。
次のようなエントリが見つかるはずです（読みやすくするために、識別子は短縮されています）。

```
kms2 | 2017-03-17 21:22:38.791 (+0000) INFO  KMS [pool-11-thread-14] - [REQUEST]
(id:8[~]9) received, requestId: 1[~]a, deviceId:
https://ciscospark.com/webhookDevices/5[~]3, method: create, type:
EPHEMERAL_KEY_COLLECTION, URI: kms://hds1.example.com/ecdhe, userId: e[~]0, ecdheKid:
 kms://hds1.example.com/statickeys/3[~]5 (EncryptionKmsMessageHandler.java:178)
```

b) KMS に既存のキーを要求したユーザを調べるには、**method: retrieve, type: KEY** でフィルタリングします。
次のようなエントリが見つかるはずです。

```
kms2 | 2017-03-17 21:22:39.208 (+0000) INFO  KMS [pool-11-thread-15] - [REQUEST]
(id:2[~]4) received, requestId: 4[~]8, deviceId:
https://ciscospark.com/webhookDevices/5[~]3, method: retrieve, type: KEY, URI:
kms://hds2.example.com/keys/c[~]7, userId: c[~]b, ecdheKid:
kms://hds1.example.com/ecdhe/e[~]b (EncryptionKmsMessageHandler.java:178)
```

c) 新しい KMS キーの作成を要求したユーザを調べるには、**method: create, type: KEY_COLLECTION** でフィルタリングします。

次のようなエントリが見つかるはずです。

```
kms2 | 2017-03-17 21:22:36.759 (+0000) INFO KMS [pool-10-thread-30] - [REQUEST]
(id:26) received, requestId: 8[~]8, deviceId:
https://wdm-integration.wbx2.com/wdm/api/v1/devices/e[~]7, method: create, type:
KEY_COLLECTION, URI: /keys, userId: 65c058bb-0e01-4ec1-8a14-037655d9587b, ecdheKid:
 kms://hds2.example.com/ecdhe/326c9b5a-8b73-4ba0-8074-44a057bcdeda
(EncryptionKmsMessageHandler.java:178)
```

d) スペースまたはその他の保護されたリソースの作成時に新しい KMS リソースオブジェクト（KRO）の作成を要求したユーザを調べるには、**method: create, type: RESOURCE_COLLECTION** でフィルタリングします。
次のようなエントリが見つかるはずです。

```
kms2 | 2017-03-17 21:21:30.738 (+0000) INFO KMS [pool-11-thread-8] - [REQUEST]
(id:8[~]1) received, requestId: e[~]b, deviceId:
https://wdm-integration.wbx2.com/wdm/api/v1/devices/a[~]5, method: create, type:
RESOURCE_COLLECTION, URI: /resources, userId: 7[~]4, ecdheKid:
kms://hds2.example.com/ecdhe/4[~]a (EncryptionKmsMessageHandler.java:178)
```

Hybrid Data Security のヘルス モニタリング

Cisco Webex Control Hub 内のステータス インジケータは、Hybrid Data Security 導入環境ですべてが正常に機能しているかどうかを示します。よりプロアクティブにアラートを受け取るには、電子メール通知に登録します。サービスに影響するアラームが発生した場合、またはソフトウェアのアップグレードが利用可能になると、電子メールで通知されます。

手順

ステップ 1 Cisco Webex Control Hub で、画面左側のメニューから [サービス（Services）] を選択します。

ステップ 2 [ハイブリッドサービス（Hybrid Services）] セクションで、Hybrid Data Security を見つけて [設定（Settings）] をクリックします。
[Hybrid Data Security の設定（Hybrid Data Security Settings）] ページが表示されます。

ステップ 3 [電子メール通知（Email Notification）] セクションで、1 つ以上の電子メール アドレスをカンマで区切って入力し、**Enter** キーを押します。

トライアル ユーザの追加または削除

トライアルをアクティブ化して最初のトライアル ユーザを追加した後は、トライアルがアクティブである限り、いつでもトライアルのメンバーを追加または削除できます。

トライアルからユーザを削除する場合は、ユーザのクライアントが KMS ではなくクラウド KMS からキーとキーの作成を要求します。クライアントが KMS に格納されているキーを必要とする場合は、クラウド KMS がユーザの代わりにそのキーを取得します。

組織でディレクトリ同期を使用する場合は、（この手順の代わりに）Active Directory を使用してトライアル グループ `HdsTrialGroup` を管理します。Cisco Webex Control Hub ではグループのメンバーを表示できますが、メンバーの追加や削除はできません。

手順

ステップ 1 Cisco Webex Control Hub にサインインして、[サービス（Services）] を選択します。

ステップ 2 Hybrid Data Security で、[設定（Settings）] をクリックします。

ステップ 3 [サービスステータス（Service Status）] 領域の [トライアルモード（Trial Mode）] セクションで、[ユーザの追加（Add Users）] をクリックしてトライアルにユーザを追加するか、[表示と編集（view and edit）] をクリックしてトライアルからユーザを削除します。

ステップ 4 追加する 1 人以上のユーザの電子メール アドレスを入力するか、ユーザ ID の横にある [X] をクリックしてトライアルからユーザを削除します。次に [保存（Save）] をクリックします。

トライアルから実稼働への移行

導入がトライアルユーザに対して適切に機能していることを確認したら、実稼働に移行できます。実稼働に移行すると、組織内のすべてのユーザが暗号キーやその他のセキュリティ レルム サービスに関してオンプレミスの Hybrid Data Security ドメインを使用します。ディザスタ リカバリの一部としてサービスを非アクティブ化する場合を除き、実稼働からトライアル モードに戻ることはできません。サービスを再アクティブ化するには、新しいトライアルをセットアップする必要があります。

手順

ステップ 1 Cisco Webex Control Hub にサインインして、[サービス（Services）] を選択します。

ステップ 2 Hybrid Data Security で、[設定（Settings）] をクリックします。

ステップ 3 [サービスステータス（Service Status）] セクションで、[実稼働への移行（Move to Production）] をクリックします。

ステップ 4 すべてのユーザを実稼働に移行することを確認します。

実稼働に移行せずにトライアルを終了する

トライアル期間中に、Hybrid Data Security 導入を進めないことにした場合、Hybrid Data Security を非アクティブ化できます。これにより、トライアルが終了し、トライアルユーザはクラウドデータセキュリティ サービスに戻されます。トライアル ユーザは、トライアル中に暗号化されたデータにアクセスできなくなります。

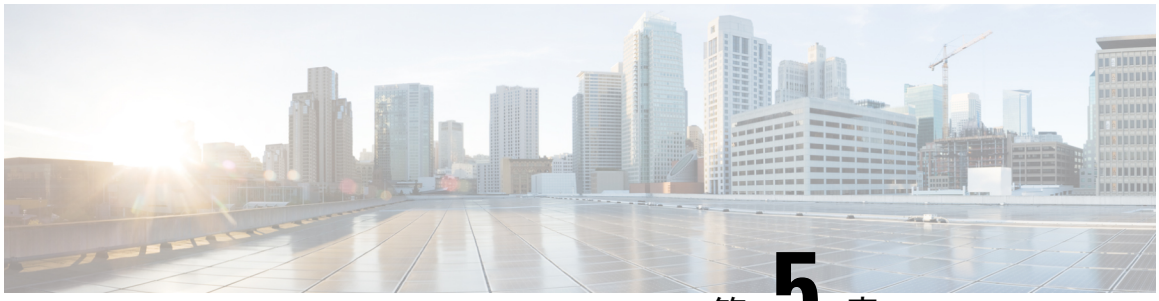
手順

ステップ 1 Cisco Webex Control Hub にサインインして、[サービス（Services）] を選択します。

ステップ 2 Hybrid Data Security で、[設定（Settings）] をクリックします。

ステップ 3 [非アクティブ化（Deactivate）] セクションで、[非アクティブ化（Deactivate）] をクリックします。

ステップ 4 サービスを非アクティブ化してトライアルを終了することを確認します。



第 5 章

HDS 導入環境の管理

Hybrid Data Security 導入を管理するには、ここで説明するタスクを使用します。

クラスタアップグレード スケジュールの設定

Hybrid Data Security のソフトウェア アップグレードはクラスタ レベルで自動的に行われるため、すべてのノードが常に同じソフトウェアバージョンを実行していることが保証されます。アップグレードは、クラスタのアップグレードスケジュールに従って行われます。ソフトウェアアップグレードが利用可能になった時点で、スケジュールされたアップグレード時間よりも前に手動でクラスタをアップグレードすることもできます。特定のアップグレードスケジュールを設定することも、デフォルトのスケジュール（米国：アメリカ/ロサンゼルス時間の毎日午前3:00）を適用することもできます。必要に応じて、予定されているアップグレードを延期することもできます。

アップグレードスケジュールを設定するには、次の手順に従います。

手順

ステップ 1 Cisco Webex Control Hub にログインします。

ステップ 2 概要ページの [ハイブリッドサービス（Hybrid Services）] で、[Hybrid Data Security] を選択します。

ステップ 3 [Hybrid Data Security リソース（Hybrid Data Security Resources）] ページで、クラスタを選択します。

ステップ 4 右側の [概要（Overview）] パネルの [クラスタ設定（Cluster Settings）] で、クラスタ名を選択します。

ステップ 5 [設定（Settings）] ページの [アップグレード（Upgrade）] で、アップグレード スケジュールの時間とタイムゾーンを選択します。

注：選択したタイムゾーンで次に使用可能なアップグレードの日時が表示されます。必要に応じて、[延期（Postpone）] をクリックして、アップグレードを翌日に延期できます。

ノード構成の変更

次のような場合には、Hybrid Data Security ノードの構成を変更しなければならないことがあります。

- 有効期限切れなどの理由により、x.509 証明書を変更する場合。

（注） 証明書の CN ドメイン名の変更はサポートされていません。ドメインは、クラスタの登録に使用された元のドメインと一致している必要があります。

- データベース設定の更新により PostgreSQL または Microsoft SQL Server データベースのレプリカが変更される場合。

（注） PostgreSQL から Microsoft SQL Server へのデータの移行、またはその逆の移行はサポートされていません。データベース環境を切り替えるには、Hybrid Data Security の新しい導入環境を起動する必要があります。

- 新しいデータ センターを準備するために新しい構成を作成する場合。

また、セキュリティ上の理由から、Hybrid Data Security は、有効期間が 9 ヶ月に設定されたサービス アカウント パスワードを使用します。HDS セットアップ ツールによってこれらのパスワードが生成されたら、ISO コンフィギュレーション ファイルに含まれる各 HDS ノードにパスワードを導入します。組織のパスワードの有効期限が近づくと、お使いのマシン アカウントのパスワードをリセットするよう求める通知が Cisco Webex チームから通知が送られます。（この電子メールには、「マシン アカウント API を使用してパスワードを更新してください（Use the machine account API to update the password）」というテキストが含まれています）。パスワードの有効期限がまだ切れていない場合は、次の 2 つのオプションが提示されます。

- **ソフト リセット**：古いパスワードと新しいパスワードの両方を最大10日間使用できます。この期間を利用して、ノード上の ISO ファイルを順次置き換えることができます。
- **ハード リセット**：古いパスワードはただちに使用できなくなります。

パスワードをリセットしないまま期限切れになると HDS サービスが影響を受けます。この場合、即座にハード リセットを実行し、すべてのノード上の ISO ファイルを置き換える必要があります。

新しい構成 ISO ファイルを生成してクラスタに適用するには、次の手順を使用します。

始める前に

- HDS セットアップ ツールは、ローカル マシン上の Docker コンテナとして実行されます。Docker にアクセスするには、Docker がマシン上で実行されている必要があり、さらに組織の Cisco Webex Control Hub 管理者のサインイン資格情報が必要です。
- 新しい構成を生成するには、現在の構成 ISO ファイルのコピーが必要です。この ISO には、PostgreSQL または Microsoft SQL Server のデータベースを暗号化するマスター キーが格納されます。データベースのクレデンシャルの変更、証明書の更新、認証ポリシーの変更を含め、構成を変更するときは必ず、この ISO が必要になります。

手順

ステップ 1 ローカル マシン上の Docker を使用して、HDS セットアップ ツールを実行します。

a) マシンのコマンドラインで、「`docker login -u sparkhdsreadonly -p AtAideExertAddisDatumFlame`」と入力して **Enter** を押します。

b) ログイン後、「`docker rmi ciscosparkhds/hds-setup:stable`」と入力して、**Enter** キーを押します。

（注） この手順で、以前の HDS セットアップ ツール イメージがクリーンアップされます。イメージがない場合はエラーが返されますが、無視してかまいません。

c) 「`docker pull ciscosparkhds/hds-setup:stable`」と入力して、**Enter** キーを押します。

この手順では、必ず最新のセットアップ ツールをプルしてください。2018 年 2 月 22 日より前に作成されたツールのバージョンには、パスワードのリセット画面がありません。

d) プルが完了したら、次のコマンドを入力して **Enter** キーを押します。

```
docker run -p 8080:8080 --rm -it ciscosparkhds/hds-setup:stable
```

e) ブラウザを使用して localhost（http://127.0.0.1:8080）に接続します。

f) プロンプトが表示されたら、Cisco Webex Control Hub ユーザのサインイン資格情報を入力して [同意する（Accept）] をクリックします。

g) 現在の構成 ISO ファイルをインポートします。

h) プロンプトの指示に従ってツールを完了し、更新されたファイルをダウンロードします。

セットアップ ツールをシャット ダウンするには、`CTRL+C` を押します。

i) 別のデータ センターで、更新されたファイルのバックアップ コピーを作成します。

ステップ 2 **実行中の HDS ノードが 1 つしかない**場合は、新しい Hybrid Data Security ノード VM を作成し、新しい構成 ISO ファイルを使ってそれを登録します。詳細な手順については、「追加ノードの作成と登録 （33 ページ）」を参照してください。

a) HDS ホストの OVA をインストールします。
b) HDS VM をセットアップします。
c) 更新された構成ファイルをマウントします。
d) 新しいノードを Cisco Webex Control Hub に登録します。

ステップ 3 古いコンフィギュレーション ファイルを実行している既存の HDS ノードの場合は、ISO ファイルをマウントします。次の手順を各ノードで順番に実行し、次のノードの電源をオフにする前に各ノードを更新します。

a) 仮想マシンの電源をオフにします。
b) VMware vSphere クライアントの左側のナビゲーション ウィンドウで、VM を右クリックして [設定の編集（Edit Settings）] をクリックします。
c) [CD/DVD ドライブ 1（CD/DVD Drive 1）] をクリックし、ISO ファイルからマウントするオプションを選択して、新しい構成 ISO ファイルをダウンロードした場所を参照します。
d) [電源投入時に接続（Connect at power on）] をオンにします。
e) 変更を保存し、仮想マシンの電源をオンにします。

ステップ 4 古い構成ファイルを実行している残りのノードごとに、ステップ 3 を繰り返して構成を置き換えます。

ブロックされた外部 DNS 解決モードをオフにする

ノードを登録するか、ノードのプロキシ設定を確認すると、プロセスは、Cisco Webex クラウドへの DNS ルックアップと接続をテストします。ノードの DNS サーバがパブリック DNS 名を解決できない場合、ノードはブロックされた外部 DNS 解決モードに自動的に進みます。

ノードが内部 DNS サーバを介してパブリック DNS 名を解決できる場合は、各ノードでプロキシ接続テストを再実行することによって、このモードをオフにすることができます。

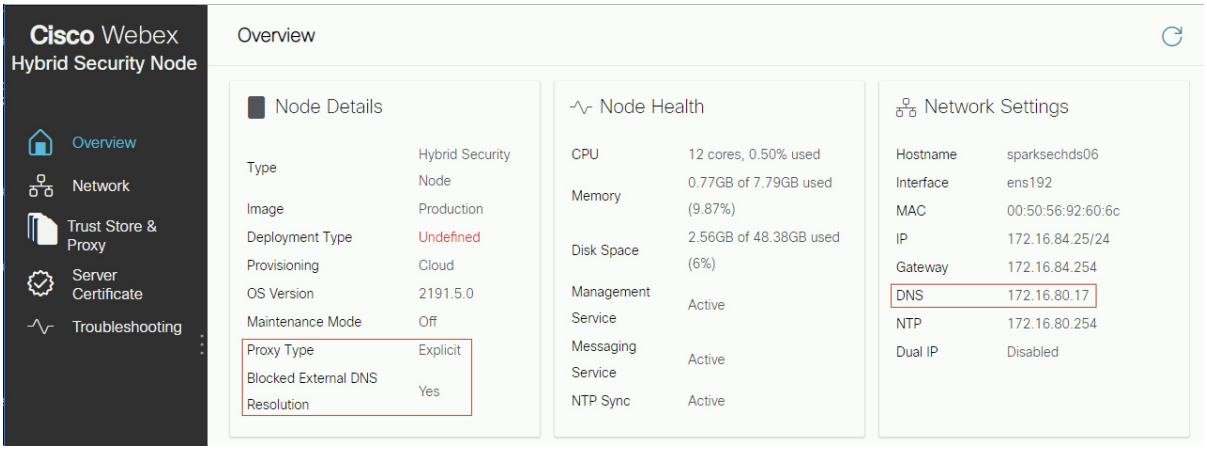
始める前に

内部 DNS サーバがパブリック DNS 名を解決できること、およびノードがパブリック DNS 名と通信できることを確認します。

手順

ステップ 1 Web ブラウザで、Hybrid Data Security ノードインターフェイス（たとえば https://192.0.2.0/setup などの IP address/setup）を開き、ノード用にセットアップした管理者の資格情報を入力し、[サインイン（Sign In）] をクリックします。

ステップ 2 [概要（Overview）]（デフォルトのページ）に移動します。



有効にすると、[ブロックされた外部DNS解決（Blocked External DNS Resolution）]が [はい（Yes）] に設定されます。

ステップ 3 [信頼ストアおよびプロキシ（Trust Store & Proxy）] ページに移動します。

ステップ 4 [プロキシ接続の確認（Check Proxy Connection）] をクリックします。

外部 DNS 解決が成功しなかったというメッセージが表示された場合、ノードは DNS サーバにアクセスできなかったため、ノードはこのモードのままになります。それ以外の場合は、ノードを再起動して、[概要（Overview）] ページに戻ってから、[ブロックされた外部DNS解決（Blocked External DNS Resolution）] を [いいえ （No）] に設定する必要があります。

次のタスク

Hybrid Data Security クラスタ内の各ノードのプロキシ接続を再度テストします。

ノードの削除

Cisco Webex クラウドから Hybrid Data Security ノードを削除するには、次の手順に従います。クラスタからノードを削除した後で、仮想マシンを削除して、セキュリティデータにそれ以降アクセスできないようにします。

手順

ステップ 1 ローカルマシン上の VMware vSphere クライアントを使用して ESXi 仮想ホストにログインし、仮想マシンの電源をオフにします。

ステップ 2 次のようにしてノードを削除します。

a) Cisco Webex Control Hub にサインインして、[サービス（Services）] を選択します。

b) Hybrid Data Security カードで、[すべて表示（View All）] をクリックして Hybrid Data Security リソース ページを表示します。

c) クラスタを選択すると、[概要（Overview）] パネルが表示されます。
d) [ノードリストを開く（Open nodes list）] をクリックし ます。
e) [ノード（Nodes）] タブで、削除するノードを選択します。
f) **[アクション（Actions）] > [ノードを登録解除（Deregister node）]** をクリックします。

ステップ 3 VSphere クライアントで、VM を削除します。（左側のナビゲーションウィンドウで、VM を右クリックし、[削除（Delete）] をクリックします）。

VM を削除しない場合は、ISO コンフィギュレーション ファイルをマウント解除するのを忘れないでください。ISO ファイルがなければ、VM を使用してセキュリティ データにアクセスすることはできません。

ディザスタ リカバリ後のクラスタの再構築

Hybrid Data Security クラスタが提供する最も重要なサービスは、Cisco Webex クラウドに保存されるメッセージやその他のコンテンツを暗号化するために使用するキーの作成と保管です。Hybrid Data Security に割り当てられる組織内の各ユーザについて、新しいキーの作成要求がクラスタにルーティングされます。クラスタはまた、キーの取得が許可されたユーザ（たとえば、会話スペースのメンバー）に、作成したキーを返す役割も担います。

クラスタはこれらのキーを提供するという重要な役割を果たすため、クラスタが稼働中の状態を維持すること、および適切なバックアップが維持されることが不可欠です。Hybrid Data Securityデータベースが失われたり、スキーマに使用されている構成ISOが失われたりすると、顧客のコンテンツが回復不能になります。このような損失を防ぐには、次の慣例が必須となります。

- 構成 ISO ファイルをバックアップし、クラスタとは異なるデータ センターにバックアップを保存します。
- PostgreSQL または Microsoft SQL Server データベースのバックアップを継続的に作成し、別のデータ センターに保管します。
- VM の実稼働環境とバックアップ PostgreSQL または Microsoft SQL Server データベースをミラーリングするバックアップ データ センターを保守します。たとえば、実稼働環境に HDS ノードを実行する 3 つの VM がある場合、バックアップ環境にも 3 つの VM が必要です。（このフェールオーバー モデルの概要については、「ディザスタ リカバリのためのスタンバイ データ センター （6 ページ）」を参照してください）。

障害によってプライマリ データ センターの HDS 導入環境が使用できなくなった場合は、次の手順に従って手動でスタンバイ データ センターにフェールオーバーします。

手順

ステップ 1 Cisco Webex Control Hub から、元のデータ センターの HDS ノードを削除します。（この手順で、これらのノードを登録解除します）。「ノードの削除 （45 ページ）」を参照してください。

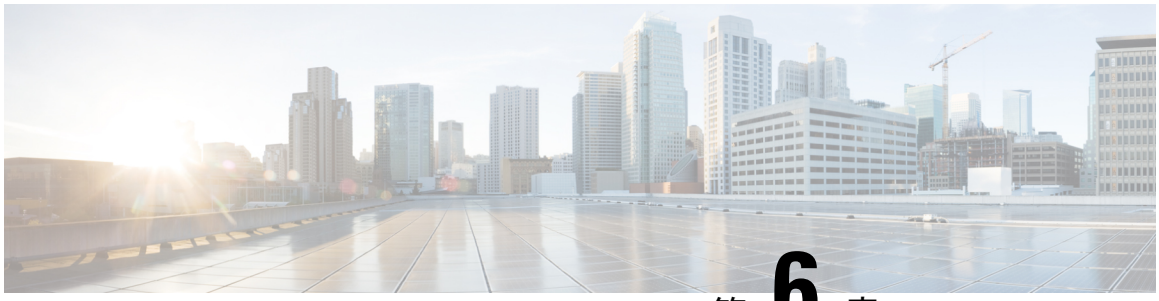
ステップ 2 スタンバイ データ センターの PostgreSQL または Microsoft SQL サーバ データベースをアクティブ（プライマリまたはマスター）データベースにします。元のデータベースが使用可能な場合は、パッシブ（スタンバイ）データベースにします。

ステップ 3 スタンバイ データ センターのデータベース ログイン情報が元のログイン情報と異なる場合は、HDS セットアップ ツールを実行し、元のファイルを使用して新しい構成ファイルを作成します。「ノード構成の変更 （42 ページ）」を参照してください。

ステップ 4 スタンバイ データ センターのバックアップ VM を使用して、各 VM に ISO ファイルをマウントし、ノードを登録して新しいクラスタ内に Hybrid Data Security ノードを作成します。

この手順は、初めてノードをインストールする場合とほぼ同じですが、ノードがまだ登録されていて、サービスを非アクティブ化していない限り、トライアル フェーズはありません。

ステップ 5 できるだけ早く、ISO 構成ファイルのバックアップ コピーを安全な場所に保存し、データベースを起動して新しいアクティブ データベースのスタンバイとして実行するようにしてください。



第 6 章

アラートの表示とトラブルシューティング

クラスタ内のすべてのノードが到達不可能になるか、クラスタの動作速度が低下して要求がタイムアウトした場合、Hybrid Data Security 導入環境は利用不可能と見なされます。ユーザが Hybrid Data Security クラスタに到達できない場合、次の現象が発生します。

- 新しいスペースを作成できない（新しいキーを作成できない）
- 次のユーザに対して、メッセージとスペース タイトルの復号化が失敗する
  - スペースに追加された新しいユーザ（キーを取得できません）
  - 新しいクライアントを使用するスペース内の既存のユーザ（キーを取得できません）
- クライアントに暗号化キーのキャッシュがある限り、スペース内の既存のユーザは正常に動作し続けます。

サービスの中断を回避するためには、Hybrid Data Security クラスタを適切にモニタリングして、アラートに迅速に対処することが重要となります。

- アラート （49 ページ）
- Hybrid Data Security のトラブルシューティング （51 ページ）

アラート

Hybrid Data Security のセットアップで問題が発生すると、Cisco Webex Control Hub で組織管理者に対するアラートが表示され、設定されている電子メール アドレスにメールが送信されます。これらのアラートは、一般的なシナリオの多くをカバーしています。

表 *3:* 一般的な問題とその解決手順

アラート	アクション
ローカル データベースへのアクセスに失敗しました。（Local database access failure.）	データベースのエラーまたはローカル ネットワークの問題を確認します。

アラート	アクション
ローカル データベースへの接続に失敗しました。（Local database connection failure.）	データベース サーバが利用可能であり、ノード構成で適切なサービス アカウント資格情報が使用されたことを確認します。
クラウド サービスへのアクセスに失敗しました。（Cloud service access failure.）	「外部接続の要件（14ページ）」で指定されている Cisco Webex サーバにノードがアクセスできることを確認します。
クラウド サービスの登録を更新しています。（Renewing cloud service registration.）	クラウドサービスへの登録が削除されました。登録の更新が進行中です。
クラウド サービスの登録が削除されました。（Cloud service registration dropped.）	クラウド サービスへの登録が終了しました。サービスがシャット ダウンされます。
サービスがまだアクティブ化されていません。（Service not yet activated.）	トライアルをアクティブ化するか、トライアルから実稼働への移行を完了します。
設定されているドメインがサーバ証明書と一致しません。（Configured domain does not match server certificate.）	サーバ証明書が設定されているサービス アクティベーション ドメインと一致することを確認します。 最も可能性の高い原因は、証明書の CN が最近変更され、初期セットアップ時に使用された CN とは異なっていることです。
クラウド サービスへの認証に失敗しました。（Failed to authenticate to cloud services.）	サービス アカウントの資格情報が正しいかどうか、および期限切れでないかどうかを確認します。
ローカル キーストア ファイルを開くことができませんでした。（Failed to open local keystore file.）	ローカル キーストア ファイルの整合性とパスワードが正しいかどうかをチェックします。
ローカル サーバ証明書が無効です。（Local server certificate is invalid.）	サーバ証明書の有効期限を確認し、信頼できる認証局によって発行されたことを確認します。
メトリックをポストできません。（Unable to post metrics.）	外部クラウド サービスへのローカル ネットワーク アクセスを確認します。
/media/configdrive/hds ディレクトリが存在しません。（/media/configdrive/hds directory does not exist.）	仮想ホスト上の ISO マウント構成を確認します。ISO ファイルが存在すること、再起動時に ISO ファイルをマウントするように設定されていること、および ISO ファイルが正常にマウントされていることを確認します。

Hybrid Data Security のトラブルシューティング

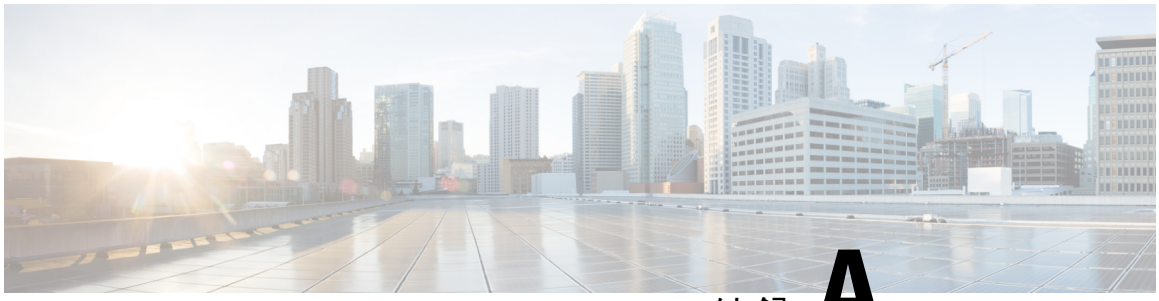
Hybrid Data Security での問題をトラブルシューティングする際は、次の一般的なガイドラインを参考にしてください。

手順

ステップ 1 Cisco Webex Control Hub でアラートの有無を確認し、アラートが見つかった場合はその問題を修正します。

ステップ 2 Syslog サーバの出力で、Hybrid Data Security 導入環境でのアクティビティを確認します。

ステップ 3 シスコサポートに連絡します。



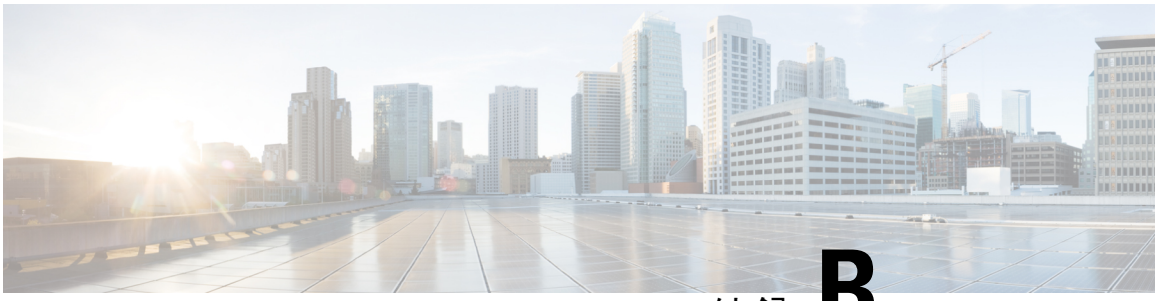
付録 A

Hybrid Data Security に関する既知の問題

- (Hybrid Data Security でクラスタを削除するか、すべてのノードをシャットダウンして）Cisco Webex Control Hub クラスタをシャットダウンした場合、構成 ISO ファイルが失われた場合、またはキーストア データベースにアクセスできなくなった場合、Cisco Webex Teams ユーザは、KMS でキーを使用して作成された [ユーザ（People）] リストに含まれるスペースを使用できなくなります。これは、トライアルと実稼働の両方の導入に当てはまります。現在この問題の回避策や修正方法はないため、アクティブなユーザ アカウントを処理した後で HDS サービスをシャット ダウンしないことを強くお勧めします。
- すでに ECDH で KMS に接続しているクライアントは、一定期間（1 時間程度）その接続を保持します。ユーザが Hybrid Data Security トライアルのメンバーになると、そのユーザのクライアントは既存の ECDH 接続をタイムアウトするまで使用し続けます。または、ユーザは Cisco Webex Teams アプリからサインアウトしてから再びサインインすることで、場所を更新し、アプリが暗号キーを照会できるようにすることもできます。

  組織のトライアルを実稼働に移行したときも、同じ現象が発生します。以前のデータ セキュリティ サービスに対する既存の ECDH 接続を使用するすべての非トライアル ユーザは、（タイムアウトまたはサインアウトと再サインインによって）ECDH 接続が再ネゴシエートされるまで、これらのサービスを使用し続けます。

Hybrid Data Security に関する既知の問題



付録 B

OpenSSL を使用した PKCS12 ファイルの生成

始める前に

- OpenSSL は、HDS セットアップ ツールでの読み込みに適した形式で PKCS12 ファイルを作成するために使用できるツールの 1 つです。他にも使用できる手段はありますが、いずれかの手段をサポートまたは優先することはありません。
- OpenSSL を使用する場合は、「X.509 証明書の要件 （11 ページ）」で説明している x.509 証明書の要件を満たすファイルを作成できるよう、ガイドラインとして以下の手順に従ってください。ファイルを作成する前に、適用される要件を理解する必要があります。
- サポートされている環境に OpenSSL をインストールします。ソフトウェアおよびドキュメントについては、https://www.openssl.orgを参照してください。
- 秘密キーを作成します。
- 認証局（CA）からサーバ証明書を受け取った後、以下の手順に従います。

手順

ステップ 1 CA からサーバ証明書を受け取ったら、`hdsnode. pem` として保存します。

ステップ 2 証明書をテキストとして表示し、詳細を確認します。

```
openssl x509 -text -noout -in hdsnode.pem
```

ステップ 3 テキスト エディタを使用して、`hdsnode-bundle.pem` という名前の証明書バンドル ファイルを作成します。バンドルファイルには、サーバ証明書、中間 CA 証明書、およびルート CA 証明書が次の形式で含まれている必要があります。

```
-----BEGIN CERTIFICATE-----
### Server certificate. ###
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
###  Intermediate CA certificate. ###
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
```

OpenSSL を使用した PKCS12 ファイルの生成

```
###  Root CA certificate. ###
-----END CERTIFICATE-----
```

ステップ 4 フレンドリ名 `kms-private-key` を使用して .p12 ファイルを作成します。

```
openssl pkcs12 -export -inkey hdsnode.key -in hdsnode-bundle.pem -name kms-private-key
-caname kms-private-key -out hdsnode.p12
```

ステップ 5 サーバ証明書の詳細を確認します。

a) `openssl pkcs12 -in hdsnode.p12`

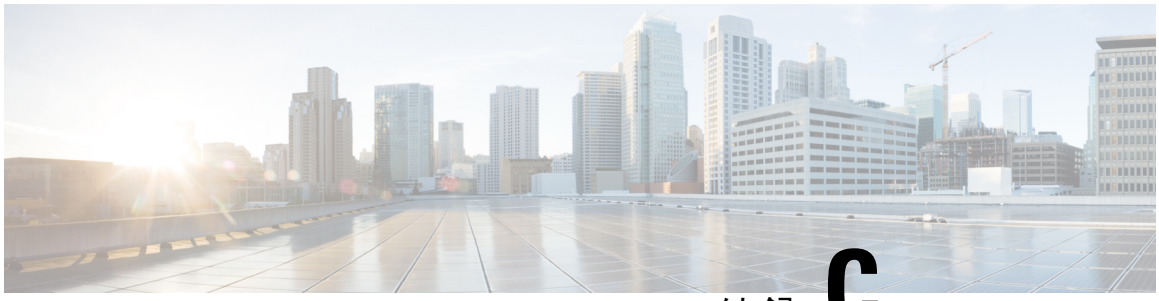
b) プロンプトが表示されたらパスワードを入力して秘密キーを暗号化し、暗号化された状態で出力されるようにします。次に、秘密キーと最初の証明書に **`friendlyName: kms-private-key`** という行が含まれていることを確認します。

例：

```
bash$ openssl pkcs12 -in hdsnode.p12
Enter Import Password:
MAC verified OK
Bag Attributes
    friendlyName: kms-private-key
    localKeyID: 54 69 6D 65 20 31 34 39 30 37 33 32 35 30 39 33 31 34
Key Attributes: <No Attributes>
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----BEGIN ENCRYPTED PRIVATE KEY-----
<redacted>
-----END ENCRYPTED PRIVATE KEY-----
Bag Attributes
    friendlyName: kms-private-key
    localKeyID: 54 69 6D 65 20 31 34 39 30 37 33 32 35 30 39 33 31 34
subject=/CN=hds1.org6.portun.us
issuer=/C=US/O=Let's Encrypt/CN=Let's Encrypt Authority X3
-----BEGIN CERTIFICATE-----
<redacted>
-----END CERTIFICATE-----
Bag Attributes
    friendlyName: CN=Let's Encrypt Authority X3,O=Let's Encrypt,C=US
subject=/C=US/O=Let's Encrypt/CN=Let's Encrypt Authority X3
issuer=/O=Digital Signature Trust Co./CN=DST Root CA X3
-----BEGIN CERTIFICATE-----
<redacted>
-----END CERTIFICATE-----
```

次のタスク

「Hybrid Data Security の前提条件への対応 （16 ページ）」に戻ります。「HDS ホストの構成 ISO の作成 （21 ページ）」では、この `hdsnode.p12` ファイルと、このファイルに設定したパスワードを使用します。



付録 C

HDS ノードとクラウド間のトラフィック

メトリック収集のアウトバウンド トラフィック

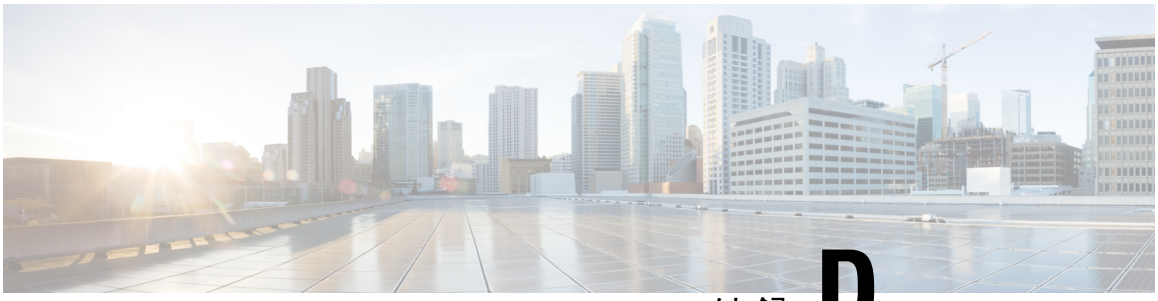
Hybrid Data Security ノードは特定のメトリックを Cisco Webex クラウドに送信します。これには、最大ヒープ、使用ヒープ、CPU 負荷、スレッド カウントに関するシステム メトリック、同期および非同期スレッドのメトリック、暗号化接続、遅延、または要求キュー長のしきい値に関するアラートのメトリック、データストアのメトリック、および暗号化接続のメトリックが含まれます。ノードは、アウトオブバンド（要求とは別の）チャネルを介して暗号化されたキー マテリアルを送信します。

インバウンド トラフィック

Hybrid Data Security ノードは、Cisco Webex クラウドから次のタイプのインバウンド トラフィックを受信します。

- 暗号化サービスによってルーティングされるクライアントからの暗号化要求
- ノード ソフトウェアのアップグレード

HDS ノードとクラウド間のトラフィック



付録 D

Hybrid Data Security の Squid プロキシの構成

HTTPS トラフィックを検査する Squid プロキシは、Hybrid Data Security に必要な WebSocket（wss:）接続の確立に干渉する場合があります。ここでは、サービスが適切に動作するよう、さまざまなバージョンの Squid で wss: トラフィックを無視するように構成する方法を説明します。

Squid 4 および 5

squid.conf に on_unsupported_protocol ディレクティブを追加します。

```
on_unsupported_protocol tunnel all
```

Squid 3.5.27

次のルールを squid.conf に追加して Hybrid Data Security をテストした結果、正しく動作することが確認されています。新しく開発された機能で Webex クラウドが更新されると、これらのルールが変更される可能性があります。

```
acl wssMercuryConnection ssl::server_name_regex mercury-connection

ssl_bump splice wssMercuryConnection

acl step1 at_step SslBump1
acl step2 at_step SslBump2
acl step3 at_step SslBump3
ssl_bump peek step1 all
ssl_bump stare step2 all
ssl_bump bump step3 all
```

Hybrid Data Security の Squid プロキシの構成