Hybrid Data Security クラスタのセットアップ

Hybrid Data Security 導入タスクのフロー

始める前に

#unique_8

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 （2 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 （3 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。
ステップ 3	HDS ホスト OVA のインストール （6 ページ）	OVA ファイルを使用して仮想マシンを作成します。

	コマンドまたはアクション	目的
ステップ 4	Hybrid Data Security VM のセットアップ（7 ページ）	VM コンソールにサインインし、サインインクレデンシャルを設定して、ネットワーク設定を構成します。
ステップ 5	HDS 構成 ISO のアップロードとマウント （8 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 （9 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 （11 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 （12 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	トライアルの実行と実稼働への移行 （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（ノードとしてセットアップする Hybrid Data Security ノードではなく）ローカルマシンにダウンロードします。このファイルは、後でインストールプロセスに従うときに使用します。

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。

カードが無効になっている場合や見つからない場合は、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。このツール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ます。また、組織の完全な管理者権限が割り当てられたアカウントの Cisco Webex Control Hub クレデンシャルも必要です。
- このタスクで生成する構成 ISO ファイルには、PostgreSQL または Microsoft SQL サーバ データベースを暗号化するマスターキーが含まれています。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、このファイルの最新のコピーを使用する必要があります。
- PostgreSQL データベースサーバを使用していて、データベース接続を暗号化する予定の場合は、TLS 用の PostgreSQL 導入環境をセットアップします。

手順

ステップ 1 ローカルマシンのコマンドラインで、`docker login -u sparkhdsreadonly -p AtAideExertAddisDatumFlame` と入力して、**Enter** キーを押します。

ステップ 2 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。

ステップ 3 `docker pull ciscosparkhds/hds-setup:stable` と入力して、**Enter** キーを押します。
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
```

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、ローカルホスト http://127.0.0.1:8080 に移動します。

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 X.509 証明書が X.509 証明書の要件 に記載されているすべての要件を満たしていることを確認します。X.509 証明書をアップロードし、パスワードを入力してから [続行（Continue）] をクリックします。

ステップ 9 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クレデンシャルを入力します。

a) ドロップダウンメニューから、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 クラスタを構成するノードから 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。

このデータベースを作成することは必須です。デフォルトのデータベースは使用しないでください。データベーススキーマは、HDS アプリケーションのインストール時に作成されます。

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 10 データベースタイプとして PostgreSQL を選択した場合は、[TLS データベース接続モード（TLS Database Connection Mode）] 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 が有効になっている場合、ノードは暗号化された接続を試行します。
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。

モード	説明
TLS を要求して証明書の署名者を確認（Require TLS and verify certificate signer）	• 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**データベースルート証明書**の認証局に照合します。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。
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**データベースルート証明書**の認証局に照合します。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）] フィールドで指定し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して（必要な場合）、[続行（Continue）] をクリックすると、HDS セットアップツールは即時にデータベースサーバへの 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マシンが接続を正常にテストできなくても、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 11 [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 クラスタを構成するノードから 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) サーバが TLS 暗号化をサポートしていて、これを使用するようにセットアップされている場合は、[Syslog サーバは SSL 暗号化対応として構成されている（Is your syslog server configured for SSL encryption?）] の横にあるチェックボックスをオンにします。

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) [続行（Continue）]をクリックします。

ステップ 12 キーアクセスレベルとして[サービスアカウントと選択されたクラウドによるアクセス（Service Account and Select Cloud Access）] を選択し、次の画面に進みます。これは現在サポートされている唯一のアクセスレベルです。

ステップ 13 [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 14 [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 15 ISO ファイルを見つけて、ローカルシステム上にコピーを作成します。

このコピーを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。アクセスできるのは、構成を変更しなければならない場合がある Hybrid Data Security 管理者だけに制限してください。

ステップ 16 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。

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、リカバリ用の追加ノードを作成したり、構成を変更したり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ると、マスターキーも失われます。その場合、シスコはこのキーのコピーを保持していないため、PostgreSQL または Microsoft SQL Server データベースに保管されているキーを回復することは不可能です。

関連トピック

ノード構成の変更

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ます。

ステップ 4 仮想マシンの名前を指定します。

ステップ 5 ディスクのフォーマットとして、デフォルトの [シックプロビジョニング Lazy Zeroed（Thick Provision Lazy Zeroed）] を選択します。

ステップ 6 [導入後に電源をオンにする（Power on after deployment）] をオフにします。

ステップ 7 設定を確認したら [終了（Finish）] をクリックします。
OVA の導入が完了すると、VM のリストにノード仮想マシンが表示されます。

Hybrid Data Security VM のセットアップ

以下の手順に従って、ハイブリッド データセキュリティ ノード VM コンソールにサインインし、サインインクレデンシャルを設定して、ネットワーク設定を構成します。

手順

ステップ 1 VMware vSphere クライアントで、ハイブリッドデータセキュリティ 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 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。

ステップ 5 （省略可）ネットワークポリシーに一致させる必要がある場合は、ホスト名、ドメイン、または NTP サーバを変更します。

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

以下の手順に従って、HDS セットアップツールで作成した ISO ファイルを使用して仮想マシンを構成します。

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 ローカルマシンから ISO ファイル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) ISO ファイルをダウンロードしたローカルマシン上の場所を参照し、[開く（Open）] をクリックします。
f) [はい（Yes）] をクリックしてアップロード/ダウンロード操作に関する警告を受け入れ、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、[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 ハイブリッド データセキュリティ 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、プロキシサポートを参照してください。
- プロキシサーバの要件

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 ノート 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。ハイブリッド データセキュリティ 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復号します（HTTPS も例外ではありません）。
- [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。

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 （7 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 （7 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 （6 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 （7 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 （8 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 （9 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

トライアルの実行と実稼働への移行 （次の章）