# HDS 導入の管理



## HDS 導入環境の管理

ハイブリッドデータ セキュリティ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

ハイブリッドデータ セキュリティ 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** 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（ハイブリッド データ セキュリティ 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、ハイブリッド データ セキュリティ 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、ハイブリッド データ セキュリティ 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 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。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 Control Hub アカウントのクレデンシャルが必要です。

  HDSセットアップツールが環境内のプロキシの背後で実行されている場合は、Dockerコンテナを起動するときにDocker環境変数を使用してプロキシ設定（サーバ、ポート、クレデンシャル）を指定します。1.e （4 ページ）次の表に、考えられる環境変数を示します。

| 説明 | 変数 |
|---|---|
| 認証なしのHTTPプロキシ | `GLOBAL_AGENT_HTTP_PROXY = http : // SERVER_IP : PORT` |
| 認証なしのHTTPSプロキシ | `GLOBAL_AGENT_HTTPS_PROXY = http : // SERVER_IP : PORT` |
| 認証を使用した HTTP プロキシ | `GLOBAL_AGENT_HTTP_PROXY = http : // USERNAME : PASSWORD @ SERVER_IP : PORT` |
| 認証付きHTTPSプロキシ | `GLOBAL_AGENT_HTTPS_PROXY = http : // USERNAME : PASSWORD @ SERVER_IP : PORT` |

- 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、環境に適したコマンドを入力します。

通常の環境：

```
docker rmi ciscocitg/hds-setup:stable
```

FedRAMP環境の場合：

```
docker rmi ciscocitg/hds-setup-fedramp:stable
```

（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。

b) Dockerイメージレジストリにサインインするには、次のように入力します。

```
docker login -u hdscustomersro
```

c) パスワードプロンプトで、次のハッシュを入力します。

```
dckr_pat_aDP6V4KkrvpBwaQf6m6ROkvKUIo
```

d) 環境に合わせて最新の安定したイメージをダウンロードします。

通常の環境：

```
docker pull ciscocitg/hds-setup:stable
```

FedRAMP環境の場合：

```
docker pull ciscocitg/hds-setup-fedramp:stable
```

（注） 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。

e) プルが完了したら、環境に適したコマンドを入力します。

- プロキシのない通常の環境：

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

- HTTP プロキシを使用する通常の環境：

  ```
  docker run -p 8080:8080 --rm -it -e GLOBAL_AGENT_HTTP_PROXY=http://SERVER_IP:PORT
   ciscocitg/hds-setup:stable
  ```

- HTTPS プロキシを使用する通常の環境：

  ```
  docker run -p 8080:8080 --rm -it -e
  GLOBAL_AGENT_HTTPS_PROXY=http://SERVER_IP:PORT ciscocitg/hds-setup:stable
  ```

- プロキシのない FedRAMP 環境の場合：

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

- HTTP プロキシを使用する FedRAMP 環境の場合：

  ```
  docker run -p 8080:8080 --rm -it -e GLOBAL_AGENT_HTTP_PROXY=http://SERVER_IP:PORT
   ciscocitg/hds-setup-fedramp:stable
  ```

- HTTPS プロキシを使用する FedRAMP 環境の場合：

  ```
  docker run -p 8080:8080 --rm -it -e
  GLOBAL_AGENT_HTTPS_PROXY=http://SERVER_IP:PORT ciscocitg/hds-setup-fedramp: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。

f) ブラウザを使用して、ローカルホスト `http://127.0.0.1:8080` に接続します。
g) プロンプトが表示されたら、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。
h) 現在の構成 ISO ファイルをインポートします。
i) 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。

j) 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 ハイブリッド データ セキュリティ 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」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 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。

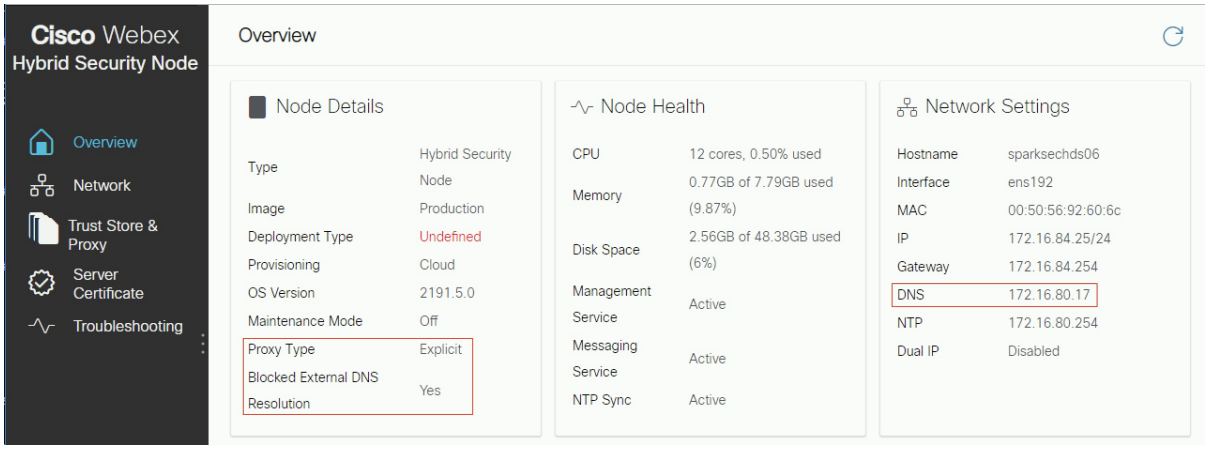
### 始める前に

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

Webex クラウドから ハイブリッド データ セキュリティ 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) Control Hub にサインインして、[サービス（Services）] を選択します。
b) ハイブリッド データ セキュリティ カードで、[すべて表示（View All）] をクリックしてハイブリッド データ セキュリティ 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

ハイブリッド データ セキュリティ クラスタが提供する最も重要なサービスは、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。ハイブリッド データ セキュリティ 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。ハイブリッド データ セキュリティ 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」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** 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 （6 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 （2 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 ハイブリッド データ セキュリティ 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。

# （オプション）HDS 構成後に ISO をマウント解除する

標準の HDS 設定は、ISO をマウントして実行されます。ただし、ISO ファイルをマウントしたままにしないことを希望するお客様もいます。すべての HDS ノードが新しい設定を取得した後、ISO ファイルをマウント解除できます。

引き続き ISO ファイルを使用して設定を変更します。新しい ISO を作成するか、セットアップ ツールを使用して ISO を更新する場合は、すべての HDS ノードに更新された ISO をマウントする必要があります。すべてのノードが設定変更を取得したら、この手順で ISO を再度マウント解除できます。

### 始める前に

すべての HDS ノードをバージョン 2021.01.22.4720 以降にアップグレードします。

### 手順

**ステップ 1** HDS ノードの 1 つをシャットダウンします。

**ステップ 2** vCenter Server Appliance で、HDS ノードを選択します。

**ステップ 3** **[Edit Settings** > **CD / DVD drive]** を選択し、**[Datastore ISO File]** をオフにします。

**ステップ 4** HDS ノードの電源をオンにし、少なくとも 20 分間アラームがないことを確認します。

**ステップ 5** 各 HD ノードに対して順番に繰り返します。

### 関連トピック

HDS 構成 ISO のアップロードとマウント

（オプション）HDS 構成後に ISO をマウント解除する

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。