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

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。

	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 （9 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 （11 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 （12 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 （13 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 （15 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 （16 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 （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（ハイブリッド データ セキュリティ 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、ハイブリッド データ セキュリティ 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、ハイブリッド データ セキュリティ 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。

（注） また、**[設定（Settings）]**ページの **[ヘルプ（Help）]** セクションからいつでも OVA をダウンロードできます。ハイブリッドデータ セキュリティカードで **[設定の編集（Edit settings）]** をクリックしてページを開きます。次に、**[ヘルプ（Help）]** セクションの **[Hybrid Data Security ソフトウェアのダウンロード（Download Hybrid Data Security software）]** をクリックします。

ステップ 3 ノードのセットアップがまだ完了していないことを示すために **[いいえ（No）]** を選択し、**[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

ハイブリッド データ セキュリティ 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 ハイブリッド データ セキュリティ 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 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。ステップ 5 （5 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`

説明	変数
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`

- 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 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。

ステップ 2 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
```

ステップ 3 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
```

ステップ 4 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
```

ステップ 5 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。

ステップ 6 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、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 7 プロンプトが表示されたら、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、ハイブリッド データ セキュリティ 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 8 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 9 **[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 10 「X.509 証明書の要件」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 11 HDS のデータベースアドレスとアカウントを入力して、キーデータストアにアクセスします。

a) **データベースの種類**（*PostgreSQL* または *Microsoft SQL Server*）を選択します。

Microsoft SQL Server を選択すると、認証タイプフィールドが表示されます。

b) （*Microsoft SQL Server* のみ）**認証タイプ**を選択します。

- ベーシック認証：**[ユーザー名（Username）]** フィールドにローカル SQL Server アカウント名が必要です。
- *Windows* 認証：`username@DOMAIN` の形式の Windows アカウントが **[ユーザー名（Username）]** フィールドに必要です。

c) フォームにデータベースサーバのアドレスを入力します：`<hostname>:<port>` または `<IP-address>:<port>`。

例：

`dbhost.example.org:1433` または `198.51.100.17:1433`

ホスト名を解決するために、ノードが DNS を使用できない場合は、基本認証に IP アドレスを使用できます。

Windows 認証を使用している場合は、完全修飾ドメイン名を d`bhost.example.org:1433` の形式で入力する必要があります。

d) **データベース名**を入力します。

e) 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 12 **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。

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）	（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。
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 13 [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 14 （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 15 [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 16 [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 17 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 ハイブリッド データ セキュリティ 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 18 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

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。

Procedure

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。

  Note
  - 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。

  Note 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 サーバー（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 サーバー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 サーバー（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 サーバーを入力します。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, on page 11」の手順に従ってノード コンソールから設定を行います。

Note 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。

Troubleshooting Tips

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、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、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 「HDS ホスト OVA のインストール （9 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、ハイブリッド データ セキュリティ 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。

次のタスク

IT ポリシーで必要な場合は、必要に応じて、すべてのノードが設定変更を取得した後に ISO ファイルをマウント解除できます。詳細については、（オプション）HDS 構成後に ISO をマウント解除するを参照してください。

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（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」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 [再起動（**Reboot**）]（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 （11 ページ）」で作成した汎用ノードを Webex クラウドに登録してハイブリッドデータ セキュリティ 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、ハイブリッド データ セキュリティを見つけて [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、ハイブリッド データ セキュリティ 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 （11 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 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、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、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 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 Control Hub ハイブリッド データ セキュリティ 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。

（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 （9 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 （11 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 （12 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 （13 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、ハイブリッド データ セキュリティ 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（ハイブリッド データ セキュリティ 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 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、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 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 Control Hub ハイブリッド データ セキュリティ 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 （次の章）

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。