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

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 （2 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（3 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 （4 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 （5 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 （5 ページ） • 実稼働に移行せずにトライアルを終了する （6 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 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 導入を非アクティブ化する場合、クライアントによってキャッシュされた暗号キーのコピーを置き換えると、パイロットユーザによって作成されたスペース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) ユーザが最初に KMS へのセキュリティで保護されたチャネルを確立しているかどうかを確認するには、**kms.data.method=create** および **kms.data.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）。

```
2020-07-21 17:35:34.562 (+0000) INFO  KMS [pool-14-thread-1] - [KMS:REQUEST] received,

deviceId: https://wdm-a.wbx2.com/wdm/api/v1/devices/0[~]9 ecdheKid:
kms://hds2.org5.portun.us/statickeys/3[~]0
(EncryptionKmsMessageHandler.java:312) WEBEX_TRACKINGID=HdsIntTest_d[~]0,
kms.data.method=create,
kms.merc.id=8[~]a, kms.merc.sync=false, kms.data.uriHost=hds2.org5.portun.us,
kms.data.type=EPHEMERAL_KEY_COLLECTION,
kms.data.requestId=9[~]6, kms.data.uri=kms://hds2.org5.portun.us/ecdhe,
kms.data.userId=0[~]2
```

b) KMSから既存のキーを要求したユーザをチェックするため、**kms.data.method=retrieve** と **kms.data.type=KEY** を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。

```
2020-07-21 17:44:19.889 (+0000) INFO  KMS [pool-14-thread-31] - [KMS:REQUEST] received,
```

```
deviceId: https://wdm-a.wbx2.com/wdm/api/v1/devices/f[~]f ecdheKid:
kms://hds2.org5.portun.us/ecdhe/5[~]1
(EncryptionKmsMessageHandler.java:312) WEBEX_TRACKINGID=HdsIntTest_f[~]0,
kms.data.method=retrieve,
kms.merc.id=c[~]7, kms.merc.sync=false, kms.data.uriHost=ciscospark.com,
kms.data.type=KEY,
kms.data.requestId=9[~]3, kms.data.uri=kms://ciscospark.com/keys/d[~]2,
kms.data.userId=1[~]b
```

c) 新しいKMSキーの作成を要求したユーザをチェックするため、**kms.data.method=create** および **kms.data.type=KEY_COLLECTION** を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。

```
2020-07-21 17:44:21.975 (+0000) INFO  KMS [pool-14-thread-33] - [KMS:REQUEST] received,

deviceId: https://wdm-a.wbx2.com/wdm/api/v1/devices/f[~]f ecdheKid:
kms://hds2.org5.portun.us/ecdhe/5[~]1
(EncryptionKmsMessageHandler.java:312) WEBEX_TRACKINGID=HdsIntTest_4[~]0,
kms.data.method=create,
kms.merc.id=6[~]e, kms.merc.sync=false, kms.data.uriHost=null,
kms.data.type=KEY_COLLECTION,
kms.data.requestId=6[~]4, kms.data.uri=/keys, kms.data.userId=1[~]b
```

d) スペースまたは他の保護対象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チェックするため 、**kms.data.method=create** および **kms.data.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。

```
2020-07-21 17:44:22.808 (+0000) INFO  KMS [pool-15-thread-1] - [KMS:REQUEST] received,

deviceId: https://wdm-a.wbx2.com/wdm/api/v1/devices/f[~]f ecdheKid:
kms://hds2.org5.portun.us/ecdhe/5[~]1
(EncryptionKmsMessageHandler.java:312) WEBEX_TRACKINGID=HdsIntTest_d[~]0,
kms.data.method=create,
kms.merc.id=5[~]3, kms.merc.sync=true, kms.data.uriHost=null,
kms.data.type=RESOURCE_COLLECTION,
kms.data.requestId=d[~]e, kms.data.uri=/resources, kms.data.userId=1[~]b
```

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、ハイブリッドデータ セキュリティ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、ハイブリッドデータ セキュリティを見つけて [設定（Settings）] をクリックします。

[Hybrid Data Security の設定（ハイブリッドデータ セキュリティ 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。